

Hypertrucages et cyberrésilience des personnes âgées : enjeux et perspectives



CHERCHEUSE PRINCIPALE

Nadia Naffi

CO-CHERCHEUSE ET CO-CHERCHEUR

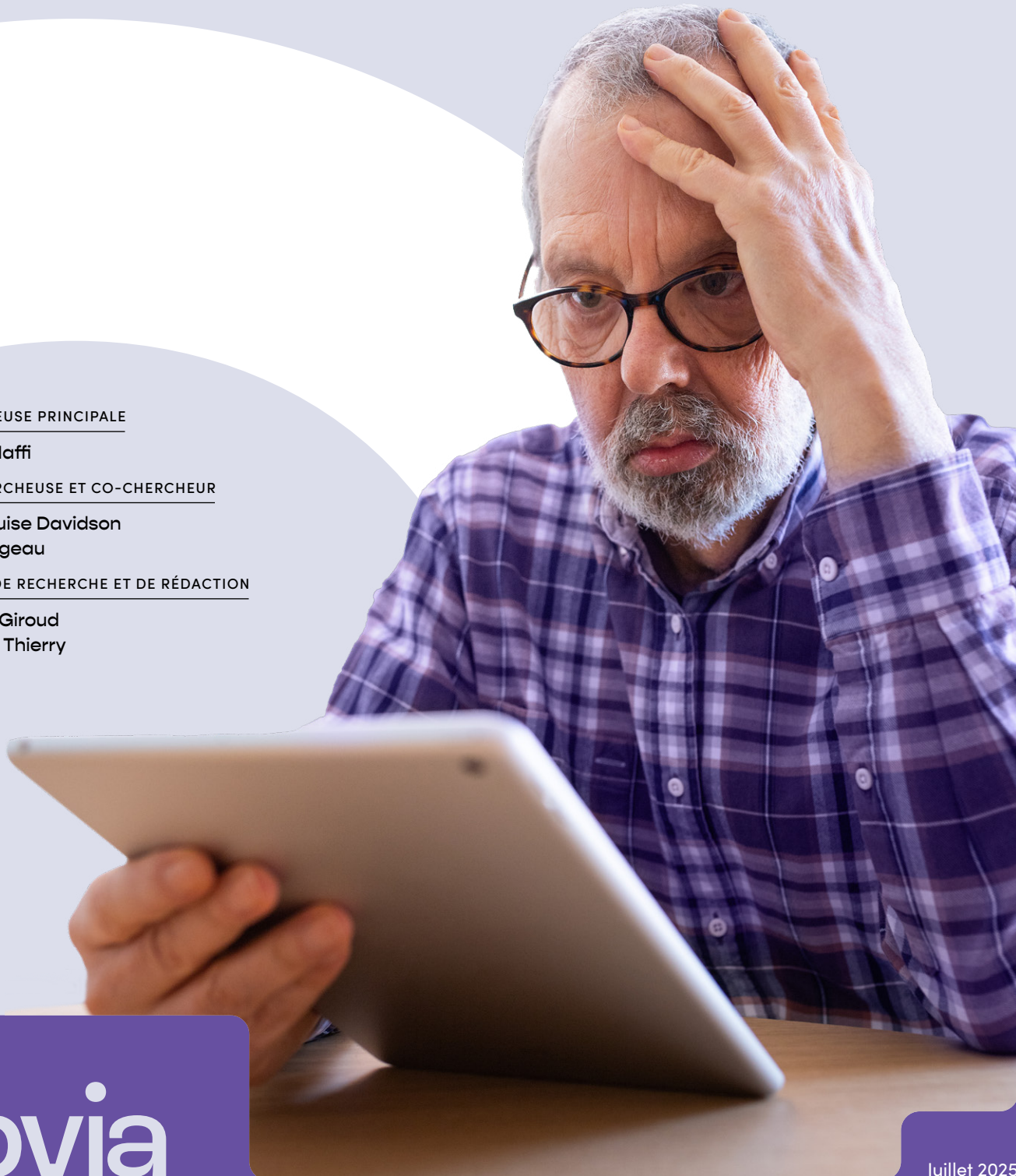
Ann-Louise Davidson

Félix Pageau

ÉQUIPE DE RECHERCHE ET DE RÉDACTION

Nancie Giroud

Tatiana Thierry



Chercheuse principale

- Nadia Naffi, chercheuse co-responsable de l'axe Éducation et capacitation à l'Obvia, et professeure agrégée à la faculté des sciences de l'éducation, Université Laval

Co-chercheuse et co-chercheur

- Ann-Louise Davidson, professeure titulaire, Université Concordia
- Félix Pageau, professeur adjoint enseignant médecin sous-octroi, Université Laval

Équipe de recherche et de rédaction

- Nancie Giroud, professionnelle de recherche à l'Université Laval
- Tatiana Thierry, professionnelle de recherche à l'Université Laval

Personnes collaboratrices des instances partenaires – équipe de révision

- Simon Deslauriers, pht, Ph. D., chef de service aux affaires administratives et scientifiques de la recherche, VITAM – Centre de recherche en santé durable, CIUSSS de la Capitale-Nationale
- Bertrand Gignac, directeur général Conférence des Tables régionales de concertation des aînés du Québec (CTRCAQ)
- Marie-Anik Robitaille, conseillère en développement de la recherche, en liaison et en rayonnement, VITAM – Centre de recherche en santé durable, Centre intégré universitaire de santé et de services sociaux de la Capitale-Nationale
- Amélie Doucet, conseillère en programmes sociaux, Réseau Fédération de l'Âge d'Or du Québec (FADOQ)

Personnes collaboratrices des instances partenaires

- André Tourigny, responsable de l'Initiative et co-directeur de l'Institut sur le vieillissement et la participation sociale des aînés de l'Université Laval (IVPSA)
- Line D'Amours, Coordinatrice Centre d'excellence sur le vieillissement de Québec (CEVQ), Centre intégré universitaire de santé et de services sociaux de la Capitale-Nationale (CIUSSSCN)
- Mireille Fortier, coordinatrice, Institut sur le vieillissement et la participation sociale des aînés de l'Université Laval (IVPSA)

Ce projet a été rendu possible grâce au financement des Chantiers d'interventions thématiques de l'Obvia (2024).

Nous remercions également chaleureusement nos personnes collaboratrices des instances partenaires pour leur soutien et leurs précieux conseils : VITAM – Centre de recherche en santé durable (CIUSSS de la Capitale-Nationale), le Centre d'excellence sur le vieillissement de Québec (CEVQ), l'Institut sur le vieillissement et la participation sociale des aînés de l'Université Laval (IVPSA), la Conférence des Tables régionales de concertation des aînés du Québec (CTRCAQ) et le Réseau Fédération de l'Âge d'Or du Québec (FADOQ).

Enfin, nous remercions tous celles et ceux qui ont partagé leurs connaissances, leurs réflexions et leurs expériences, ainsi que l'ensemble des contributeurs et contributrices pour leur participation active.

Produit avec le soutien financier du Fonds de recherche du Québec



ISBN : 978-2-925138-99-0
DOI : 10.61737/YTQH9064

Pour citer ce document : Naffi, N., Davidson, A.-L., Pageau, F., Giroud, N., Thierry, T., Deslauriers, S., Gignac, B., Robitaille, M.-A. et Doucet, A. (2025). *Hypertrucages et cyberrésilience des personnes aînées : enjeux et perspectives*. Obvia.
<https://doi.org/10.61737/YTQH9064>

Tables des matières

Lexique	4
Résumé exécutif	6
Introduction	7
Contexte et problématique	8
Usages malveillants des hypertrucages (deepfakes) et risques sociétaux	8
Impacts sur la démocratie et l'intégrité de l'information : un enjeu crucial pour l'électorat aîné	9
La vulnérabilité particulière des aînés	9
La fracture numérique et les défis spécifiques	10
Impacts psychologiques et financiers des fraudes par hypertrucages (deepfakes)	10
La triple fracture numérique : obstacles d'accès, d'usage et d'adaptation	11
L'urgence d'une réponse adaptée	11
Objectifs et méthodologie du livre blanc	13
Méthodologie	14
Résultats	19
Résultats de la recension littéraire	20
Résultats de la recension des interventions terrain	33
Discussion	42
Les limites structurelles des approches actuelles	43
La tension fondamentale entre protection et autonomisation	50
L'émergence de pratiques porteuses d'espoir	50
Les enjeux éthiques et sociétaux sous-jacents	50
Conclusion	51
Principaux constats	52
Recommandations	53
Vision pour l'avenir	54
Appel à l'action	54
Bibliographie	55

Lexique

Personne aînée/âgée :

« Personne qui se situe dans les dernières des grandes périodes de la vie et généralement âgée de 65 ans et plus* »

* Bien que ce concept fasse l'objet d'observations, d'analyses, de statistiques, il ne semble pas exister de consensus scientifique qui puisse déterminer le début de l'âge qui lui correspond. Par exemple, l'Organisation mondiale de la santé, en 2017, établit l'âge d'une personne âgée à 60 ans ou plus, tandis que d'autres organisations l'établissent à 65 ans. Cet âge est également tributaire de la société où cette personne vit » ([Office québécois de la langue française, 2023b](#)).

Personne retraitée :

« Situation d'une personne qui a cessé son activité professionnelle et qui a droit à une prestation de retraite » ([Office québécois de la langue française, 2008b](#)).

Baby boomer :

« Personne née pendant le baby-boom qui a suivi la Seconde Guerre mondiale, dans les années 1946 à 1965 » ([Office québécois de la langue française, 2016a](#)).

Génération silencieuse :

« Génération des personnes nées entre 1925 et 1945 approximativement, qui ont atteint l'âge adulte au début de la période d'après-guerre » ([Office québécois de la langue française, 2016b](#)).

Organisation :

« Groupement, régi ou non par des institutions, qui se propose des buts déterminés. * »

* Le terme institution, qui figure dans la définition, désigne une structure socialement sanctionnée, qui a valeur officielle, telles les institutions politiques, sociales et religieuses.

Un organisme, une entreprise ou toute communauté humaine structurée (syndicat, mouvement, association) sont des organisations » ([Office québécois de la langue française, 2005](#)).

Organisme :

« Ensemble organisé de services et de bureaux administratifs chargés de remplir une fonction déterminée * » ([Office québécois de la langue française, 2008a](#)).

* Le terme organisation a une valeur plus large et plus abstraite que le terme organisme, et a le sens très général de « groupement, association qui se propose des buts déterminés » (par exemple, Organisation de coopération et de développement économiques). Le terme organe désigne quant à lui une institution chargée de faire fonctionner des services, de représenter des individus (par exemple, les organes du pouvoir) » ([Office québécois de la langue française, 2008a](#)).

Organisme communautaire :

« Organisme sans but lucratif dont l'objectif est de proposer des services d'aide ou de mieux-être dans une communauté » ([Office québécois de la langue française, 2023a](#)). Un organisme communautaire est en plus d'être sans but lucratif et est issu d'une volonté de la communauté.

Maltraitance :

« Fait de négliger ou d'infliger de mauvais traitements à une personne vulnérable [...] qu'on a sous son autorité ou sous sa garde » ([Office québécois de la langue française, 2006](#)).

Table de concertation :

« Groupe de personnes qu'on réunit dans le but de les informer ou de les consulter sur un problème politique, économique ou social en vue d'une prise de décision en commun » ([Office québécois de la langue française, 2002](#)).

Désinformation :

« Information erronée ou déformant la réalité, qui est transmise au moyen des médias de masse ou des médias sociaux, dans le but de manipuler l'opinion publique » ([Office québécois de la langue française, 2019](#)).

Mésinformation :

« Information fausse ou inexacte. Contrairement à la désinformation, la personne qui partage une mésinformation ne le fait pas de manière malveillante : elle n'a pas l'intention de nuire ou de tromper les autres » ([Obvia, s. d.](#)).

Malinformation :

« Diffusion d'information qui se base sur un fait qui est exagéré pour manipuler » ([Centre canadien pour la cybersécurité, 2024](#)).

Fraude :

« Faute qui est l'acte matériel ou juridique accompli de mauvaise foi et sans droit et qui vise à obtenir illégitimement quelque chose, à nuire à autrui ou à violer le droit » ([Office québécois de la langue française, 2018c](#)).

Cyberfraude/ Escroquerie en ligne :

« Délit qui consiste à gagner la confiance des gens par l'intermédiaire d'Internet afin de leur extorquer de l'argent ».

* À l'origine, l'escroquerie en ligne se résumait à l'envoi de courriels par des escrocs, puis il s'est étendu notamment à l'hameçonnage, au détournement de clic, ainsi qu'à l'utilisation de faux logiciels antivirus, de pourriels, de logiciels espions, de logiciels de rançon.

Quoique fraude ait un sens plus général qu'escroquerie et arnaque, il est très souvent employé comme synonyme : par exemple, dans fraude en ligne (online fraud) et cyberfraude (cyberfraude).

On rencontre aussi arnaque sur Internet, arnaque par Internet, escroquerie sur Internet, escroquerie par Internet, fraude sur Internet, fraude par Internet » ([Office québécois de la langue française, 2018b](#)).

Cybercriminalité :

« Ensemble des délits et des actes criminels commis dans le cyberspace » ([Office québécois de la langue française, 2018a](#)).

Cyberrésilience :

« Capacité d'un système d'information à résister aux cyberattaques et aux pannes accidentelles, puis à revenir à un état de fonctionnement et de sécurité satisfaisant » ([Office québécois de la langue française, 2017](#)).

Hypertrucage (Deepfake) :

« Appelé en anglais « deepfake », l'hypertrucage consiste en l'utilisation de l'IA pour créer des images, vidéos ou enregistrements audio de toutes pièces. Par l'hypertrucage, des personnes peuvent avoir participé à des événements qui n'ont jamais eu lieu ou dit des paroles qui n'ont jamais été prononcées » ([Obvia, s. d.](#)).

Cheapfake :

« Un cheap fake est le même type de trucage qu'un deepfake, mais au lieu d'utiliser l'IA pour créer le contenu indésirable, celui-ci est créé par la main de l'homme et par le biais de capacités d'édition de basse technologie non liées à l'IA » ([Forbes, 2024](#), traduction libre).

Résumé exécutif

L'essor rapide de l'intelligence artificielle générative a introduit des menaces informationnelles d'une complexité inédite, au premier rang desquelles figurent les hypertrucages (*deepfakes*). Ces manipulations audiovisuelles sophistiquées posent un risque disproportionné pour les personnes âgées, une population dont la vulnérabilité est accentuée par une combinaison de facteurs financiers, sociaux, cognitifs et technologiques. Face à ce défi grandissant, ce livre blanc brosse un portrait exhaustif de la situation en s'appuyant sur une approche méthodologique mixte : une revue systématique de la littérature scientifique et grise post-ChatGPT (2023-2025) et une recension terrain exhaustive des initiatives éducatives au Québec, au Canada et à l'international. Cette double démarche a permis d'obtenir une compréhension holistique des enjeux et de formuler des recommandations fondées sur des données probantes.

Notre analyse révèle un décalage préoccupant entre l'ampleur de la menace et les réponses actuellement déployées. Alors que la littérature documente abondamment la vulnérabilité des aînés, les interventions spécifiquement conçues pour les outiller contre les hypertrucages demeurent exceptionnellement rares. La majorité des initiatives existantes se concentrent sur la fraude en général ou la littératie numérique, laissant la menace spécifique des hypertrucages dans un angle mort. Cette situation est aggravée par une fragmentation des initiatives où chaque secteur (bancaire, communautaire, gouvernemental) agit souvent de manière isolée, créant une « cacophonie institutionnelle » qui peut semer la confusion.

Malgré ce constat, des pratiques porteuses d'espoir émergent. Notre recherche identifie une tension fondamentale entre les approches purement protectrices, qui risquent de tomber dans un paternalisme âgiste, et les approches capacitanes, qui visent l'autonomisation. Les interventions les plus prometteuses sont celles qui naviguent dans cette tension avec nuance. Parmi celles-ci figurent les stratégies d'inoculation psychologique, notamment via la ludification, qui préparent l'esprit à résister à la manipulation, les initiatives intergénérationnelles qui favorisent un apprentissage mutuel, et les programmes communautaires ancrés localement qui misent sur des réseaux de confiance.

Ce livre blanc conclut que la cyberrésilience ne peut reposer sur la seule responsabilité individuelle. Elle exige une approche écosystémique, coordonnée et multidimensionnelle. Pour ce faire, des recommandations concrètes et ciblées sont formulées pour chaque partie prenante :

- **Pour les décideurs politiques :** Développer un cadre réglementaire adapté, investir dans des programmes nationaux d'éducation et soutenir la recherche sur des outils de détection accessibles.
- **Pour les organismes communautaires :** Intégrer la sensibilisation aux hypertrucages dans les programmes existants, développer l'apprentissage par les pairs et créer des espaces sécuritaires pour l'apprentissage.
- **Pour les institutions financières et technologiques :** Adopter des principes de conception inclusive (*privacy by design*), concevoir des systèmes de vérification simples et investir dans des outils de détection automatique.
- **Pour les chercheurs et éducateurs :** Développer et évaluer des interventions basées sur des données probantes, documenter les meilleures pratiques et créer des ponts entre la recherche et les besoins du terrain.

L'objectif ultime transcende la simple protection contre une technologie. La vision portée par ce document est celle d'une société numérique véritablement inclusive où les personnes âgées peuvent naviguer avec confiance et autonomie. La protection de nos aînés face aux hypertrucages n'est pas qu'un défi technique : c'est un test de notre capacité à construire une société qui n'abandonne personne face aux bouleversements technologiques, en préservant la confiance sociale et la dignité humaine qui constituent le socle de notre vivre-ensemble. Il est maintenant temps de transformer cette vision en une action collective et concertée.



Introduction

Introduction

Contexte et problématique

L'essor des technologies d'intelligence artificielle générative a révolutionné la création et la diffusion de contenus numériques, engendrant simultanément de nouvelles menaces pour la sécurité informationnelle. Parmi ces innovations technologiques, les hypertrucages (deep-fakes en anglais) – ces contenus audiovisuels ou textuels manipulés par l'intelligence artificielle – représentent un défi majeur pour la société contemporaine (Service canadien du renseignement de sécurité, 2023). La montée en puissance des hypertrucages et leurs usages malveillants, notamment pour la désinformation, les fraudes et les manipulations, soulève des préoccupations croissantes dans nos sociétés hyper connectées (Makhortykh, 2024).

Un nombre croissant de systèmes d'IA génèrent désormais du contenu audio et visuel. Par exemple, Midjourney, Adobe Firefly et Dall-E d'OpenAI créent des images; Runway, Sora d'OpenAI et Veo3 de Google utilisent l'IA pour créer des vidéos. L'audio synthétique -- son généré artificiellement -- a également émergé comme un type de contenu génératif potentiellement robuste et percutant. Ces systèmes peuvent être utilisés à des fins de divertissement, pour produire du contenu créatif pour les médias sociaux, mais ils ont également été utilisés pour diffuser du contenu trompeur, y compris des hypertrucages malveillants susceptibles de manipuler l'opinion publique sur des faits à fort enjeu (Makhortykh, 2024).

L'humanité se trouve à l'aube d'une nouvelle étape de l'évolution humaine qui aura un effet profond sur la société et sur la démocratie, que l'on pourrait qualifier d'« ère de l'intelligence artificielle (IA) générative ». Dans ce contexte de transformation numérique accélérée, trouver des repères face aux possibilités et aux risques qu'elle engendre constitue l'un des plus grands défis du siècle pour la démocratie et la société (Service canadien du renseignement de sécurité, 2023).

La montée en puissance des hypertrucages et leurs usages malveillants, notamment pour la désinformation, les fraudes et les manipulations, soulève des préoccupations croissantes dans nos sociétés hyper connectées (Makhortykh, 2024).

Dans ce contexte de transformation numérique accélérée, trouver des repères face aux possibilités et aux risques qu'elle engendre constitue l'un des plus grands défis du siècle pour la démocratie et la société (Service canadien du renseignement de sécurité, 2023).

Bien que les algorithmes d'IA puissent détecter les hypertrucages, ils ne sont pas facilement accessibles au public. Ainsi, ils ne protègent pas les personnes lorsqu'elles sont confrontées à des hypertrucages sur Internet, dans la publicité mensongère, la pornographie par usurpation d'identité, la propagande politique, la désinformation et les articles académiques frauduleux (Caldwell et al., 2020; Campbell et al., 2021; Fink, 2019; Hamed et al., 2023; Ibrahim et al., 2023; Keya et al., 2023, cités dans Diel et al., 2024).

Usages malveillants des hypertrucages (deepfakes) et risques sociétaux

Les hypertrucages peuvent fournir des voies d'accès à des acteurs malveillants qui pourraient détourner la technologie à des fins sinistres, comme le chantage et l'altération du cours des processus démocratiques (Tang et al., 2024). Des vidéos deepfakes de l'actrice Emma Watson lisant le Mein Kampf d'Hitler ont circulé sur 4chan et se sont répandues sur d'autres médias sociaux, utilisant la technologie d'ElevenLabs qui permet aux utilisateurs d'entendre des textes répétés avec la voix d'une personne (Makhortykh, 2024).

Europol (2022) a signalé que les hypertrucages pouvaient être utilisés pour harceler et humilier les gens en ligne, pratiquer l'extorsion et la fraude, falsifier des identités en ligne et tromper les mécanismes d'identification des clients (Service canadien du renseignement de sécurité, 2023). Les auteurs de cybermenaces malveillants recourent de plus en plus aux technologies fondées sur l'IA générative pour constituer et enrichir leurs troupes à outils de cyberintervention, facilitant la propagation de désinformation en ligne et la manipulation des publics cibles (Service canadien du renseignement de sécurité, 2024).

Il existe cependant des risques sociaux potentiels aggravés par l'IA générative, dont la désinformation, la perte de contrôle sur la confidentialité des données, les menaces pour l'intégrité des élections, la surveillance, le manque de fiabilité des sources, la discrimination notamment fondée sur le genre et les stéréotypes raciaux, et les violations des droits d'auteur (Frau-Meigs, 2024).

La désinformation -- la diffusion ciblée d'informations trompeuses -- a été considérée comme une menace clé pour la démocratie. La désinformation peut, entre autres, accroître la polarisation, renforcer le cynisme ou cultiver la méfiance et l'incertitude parmi les citoyens (Bennett & Livingston, 2018; Freelon & Wells, 2020, cités dans Hameleers, 2024). Ces préoccupations sont exprimées encore plus fortement pour la désinformation visuelle, et les hypertrucages en particulier (Dan et al., 2021; Westerlund, 2019, cités dans Hameleers, 2024).

Impacts sur la démocratie et l'intégrité de l'information : un enjeu crucial pour l'électorat aîné

Les personnes aînées, qui sont plus susceptibles de voter et de participer activement à la politique que les autres groupes d'âge, sont directement concernées par les menaces que les hypertrucages font peser sur le processus démocratique. Un véritable danger des hypertrucages pourrait résider dans des manipulations plus subtiles qui délégitiment progressivement un acteur (politique) en déformant ou en décontextualisant la vérité (Hameleers et al., 2025). Les hypertrucages ont été associés à des conséquences considérables pour la société et la démocratie (Weikmann & Lecheler, 2023, cités dans Hameleers et al., 2025). En offrant des représentations apparemment réalistes de personnes réelles disant ou faisant des choses, les hypertrucages peuvent entraîner des perceptions erronées chez les destinataires (Hameleers et al., 2025), et ce, de manière particulièrement marquée au sein de l'électorat aîné.

En juin 2024, aux élections du Parlement européen, l'équipe d'Observation de l'environnement à Élections Canada a repéré un réseau prétendu de bots Russes qui utilisait l'IA pour générer une énorme quantité de renseignements faux ou trompeurs sur les élections européennes. La campagne semblait authentique en raison de la variation des messages créés à l'aide des modèles de langage génératifs (Élections Canada, 2024).

La guerre de l'information en pleine évolution que livrent certains États hostiles fait planer une menace de plus en plus grave sur les démocraties libérales, dont le Canada. Elle passe par des opérations faisant appel à un large éventail de techniques, mais son objectif reste fondamentalement le même : modifier les comportements ou les croyances du public visé par la propagation calculée d'informations ciblées (Service canadien du renseignement de sécurité, 2024). Dans ce contexte, le poids électoral des aînés et leur intérêt manifeste pour l'actualité en font une cible stratégique pour quiconque chercherait à influencer l'issue d'un scrutin.

La vulnérabilité particulière des aînés

Dans ce contexte d'insécurité informationnelle, certaines personnes aînées constituent une population particulièrement vulnérable. Alors que les personnes aînées de 65 ans et plus représentaient 18 % de la société québécoise en 2016, cette proportion devrait s'élever à 28 % en 2066 (Institut national de santé publique du Québec, 2023). Cette transformation démographique majeure s'accompagne d'enjeux spécifiques liés à la cybersécurité et à la cyberrésilience de cette population.

Bien que les aînés manifestent un intérêt clair pour l'actualité, ils continuent de privilégier les médias traditionnels (la presse écrite, la radio et la télévision) comme référence (Brashier & Schacter, 2020, cités dans Sádaba et al., 2023). Cette particularité, combinée à un niveau de compétence numérique parfois moins élevé (Papí-Gálvez & La Parra-Casado, 2022, cités dans Sádaba et al., 2023), accentue leur vulnérabilité face aux contenus manipulés. De plus, lorsque l'information parvient aux seniors via des réseaux de deuxième génération comme WhatsApp, ils ont tendance à faire confiance à la personne qui leur envoie le message plutôt qu'au support qui le diffuse (Valera-Ordaz et al., 2022, cités dans Sádaba et al., 2023).

La fracture numérique et les défis spécifiques

Les aînés font face à des défis spécifiques dans l'environnement numérique actuel, caractérisés par une fracture numérique persistante. Des obstacles tels que l'accès limité aux appareils, les disparités de connectivité Internet et les différents niveaux de littératie numérique aggravent l'isolement social et limitent l'accès aux services et informations essentiels (Sheil et al., 2024). La pandémie de COVID-19 a encore aggravé cette fracture (Sheil et al., 2024).

Selon l'Académie de la transformation numérique (2024), en 2023, la génération des 65 ans et plus demeure la moins branchée à Internet, avec seulement 85 % disposant d'une connexion, comparativement à 93 % de l'ensemble des adultes du Québec. En 2023, seulement 30 % des adultes du Québec âgés de 65 ans et plus considèrent avoir des habiletés élevées à utiliser les technologies numériques, tandis que 9 % avouent qu'elles sont basses (Académie de la transformation numérique, 2024).

Les personnes internautes aînées de plus de 75 ans sont les moins nombreuses à considérer qu'elles ont une forte capacité à reconnaître les fausses nouvelles (Académie de la transformation numérique, 2024). Cette situation est particulièrement préoccupante alors que l'intelligence artificielle générative éveille de nombreuses craintes, notamment le risque de propagation des fausses nouvelles (mentionné par 51 % des personnes répondantes), les potentielles conséquences sur les capacités cognitives telles que la pensée critique (49 %) et les enjeux de sécurité des données personnelles (49 %) (Académie de la transformation numérique, 2025).

Impacts psychologiques et financiers des fraudes par hypertrucages (deepfakes)

Bien que la technologie des hypertrucages soit récente, des personnes de tous âges sont susceptibles d'être affectées par son usage dans des escroqueries financières (Napal, 2024), les conséquences de ces fraudes sont souvent particulièrement dévastatrices pour les personnes aînées. La maltraitance envers les personnes aînées, incluant les formes matérielle ou financière, peut être un événement singulier ou répétitif qui se produit dans le cadre d'une relation où il devrait y avoir de la confiance (Beaulieu & St-Martin, 2023). L'exploitation financière peut être dévastatrice pour les personnes aînées qui risquent de perdre une vie d'actifs accumulés avec des possibilités limitées de récupération (Dessin, 2003; James et al., 2014, cités dans Heemskerk et al., 2024).

Les conséquences de la victimisation par fraude sont significatives et dévastatrices pour le bien-être physique et mental des personnes aînées, dont beaucoup sont retraitées et peuvent avoir du mal à s'en remettre financièrement et psychologiquement (Nerenberg, 2000, cité dans Liao et al., 2024).

Être victime de fraude peut exposer les personnes aînées à des pertes financières inattendues et irréparables. Sur le plan psychologique, cela peut engendrer de vives émotions comme la colère, la honte et le remords, et entraîner de lourdes séquelles psychologiques, incluant des symptômes sévères de dépression et d'anxiété, ainsi que des plaintes somatiques fonctionnelles (Chen et al., 2024). Les conséquences de la victimisation par fraude sont significatives et dévastatrices pour le bien-être physique et mental des personnes aînées, dont beaucoup sont retraitées et peuvent avoir du mal à s'en remettre financièrement et psychologiquement (Nerenberg, 2000, cité dans Liao et al., 2024).

La victimisation criminelle en général peut causer de graves dommages psychologiques aux personnes aînées sous forme d'anxiété, de dépression et même de trouble de stress post-traumatique (TSPT) (Havers et al., 2024). Les personnes aînées plus aisées sont plus susceptibles d'être victimes d'escroqueries en ligne et de vol d'identité (Williams et al., 2018, cités dans Azam et al., 2024), ce qui peut entraîner solitude, dépression et autres problèmes de santé mentale (Grigore & Maftei, 2020, cités dans Azam et al., 2024).

Les personnes victimes de fraude sont souvent blâmées pour être trop crédules, confiantes et naïves, et peuvent être rejetées par la police qui les perçoit parfois comme ayant activement contribué à leur propre victimisation. En conséquence, les victimes peuvent se sentir honteuses et se blâmer elles-mêmes, ce qui décourage davantage la recherche d'aide et réduit la confiance dans les questions financières (DeLiema, 2024). Ce sentiment de honte peut même conduire la victime à un déni de sa situation, refusant de reconnaître la fraude malgré les avertissements de ses proches et rendant toute intervention extérieure impossible.

Ce sentiment de honte peut même conduire la victime à un déni de sa situation, refusant de reconnaître la fraude malgré les avertissements de ses proches et rendant toute intervention extérieure impossible.

La triple fracture numérique : obstacles d'accès, d'usage et d'adaptation

Les personnes âgées font face à des défis spécifiques dans l'environnement numérique actuel, caractérisés par une fracture numérique persistante. Des obstacles tels que l'accès limité aux appareils, les disparités de connectivité Internet et les différents niveaux de littératie numérique aggravent l'isolement social et limitent l'accès aux services et informations essentiels. La pandémie de COVID-19 a encore aggravé cette fracture.

D'après l'Académie de la transformation numérique (2024a), les personnes âgées représentent le groupe démographique le moins connecté à Internet au Québec, avec un taux de connexion inférieur à celui de la population adulte générale. La majorité des aînés québécois évaluent leurs compétences numériques comme étant moyennes ou faibles, une minorité seulement se considérant comme ayant des habiletés élevées dans ce domaine. Les plus âgés parmi ce groupe expriment moins de confiance en leur capacité à identifier la désinformation en ligne. Cette vulnérabilité numérique soulève des inquiétudes particulières dans le contexte actuel de l'intelligence artificielle générative, qui génère des préoccupations majeures concernant la diffusion de fausses informations, l'impact sur les fonctions cognitives comme l'esprit critique, ainsi que la protection des renseignements personnels.

Au-delà des questions d'accès, l'usage même des technologies peut être un défi. Des études montrent que les aînés peuvent rencontrer des difficultés d'utilisation avec les technologies conversationnelles et les assistants vocaux, ressentir une pression psychologique face à des interfaces mal conçues comme les bornes interactives, et exprimer des craintes légitimes concernant la confidentialité de leurs données et la surveillance.

De manière plus large, les obstacles les plus documentés dans l'accès et l'usage des technologies numériques sont le manque d'assistance technique pour les utiliser (Cheng, Beauchamp, et al., 2020; Summers-Gabr, 2020, cités dans Institut national de santé publique du Québec, 2024), et le fait que les principes de conception inclusive ne sont pas toujours au point (Arnhold et al., 2014; Cheng, Elsworth, et al., 2020, cités dans Institut national de santé publique du Québec, 2024)

De manière plus large, les obstacles les plus documentés dans l'accès et l'usage des technologies numériques sont le manque d'assistance technique pour les utiliser (Cheng, Beauchamp, et al., 2020; Summers-Gabr, 2020, cités dans Institut national de santé publique du Québec, 2024), et le fait que les principes de conception inclusive ne sont pas toujours au point (Arnhold et al., 2014; Cheng, Elsworth, et al., 2020, cités dans Institut national de santé publique du Québec, 2024)

L'urgence d'une réponse adaptée

Face à ces multiples défis, il devient urgent de développer des stratégies efficaces pour renforcer la cyberrésilience des aînés. Alors que les initiatives visant à promouvoir l'éducation aux médias se sont principalement concentrées sur les jeunes, l'attention doit également être portée sur un autre groupe hautement vulnérable : les seniors (Sádaba et al., 2023).

Des initiatives adaptées se concentrant sur l'accès, l'amélioration des compétences numériques et l'inclusivité sont nécessaires pour améliorer la qualité de vie des personnes âgées dans notre monde numérique (Sheil et al., 2024). Avec les avantages potentiels de l'accès à la technologie, il est important de s'attaquer aux obstacles à l'entrée pour les populations âgées à faible revenu, comme le développement de programmes pour connecter les individus à la formation sur les appareils tout en fournissant un soutien aux utilisateurs et un environnement encourageant pour favoriser l'apprentissage (Han & Nam, 2021, cités dans Ferguson et al., 2024).

Les personnes âgées présentent en effet certaines vulnérabilités numériques, mettant en danger leurs ressources financières et leurs données personnelles, ce qui limite leur indépendance et leur autonomie. Cependant, il est également indéniable que les TIC peuvent aider à promouvoir un vieillissement actif, et avec une formation spécifique, il est possible de réduire la fracture numérique et d'améliorer leur qualité de vie (Rodríguez-Miranda et al., 2025).

Le gouvernement du Canada a reconnu l'urgence de cette problématique. Depuis 2019, l'Initiative de citoyenneté numérique, dotée de 19,4 millions de dollars sur quatre ans, vise à renforcer la résilience des citoyens contre la désinformation en ligne. Le Programme de contribution en matière de citoyenneté numérique (PCCN) a distribué plus de 30 millions de dollars depuis 2020 pour soutenir des projets de recherche et de sensibilisation. En 2023-2024, le cinquième appel du PCCN a alloué plus de 9 millions de dollars à 27 projets, avec un accent particulier sur l'éducation aux médias numériques et l'identification des contenus générés par l'intelligence artificielle (ministère du Patrimoine canadien, 2024). Ces investissements témoignent d'une prise de conscience gouvernementale, mais la question demeure : dans quelle mesure ces initiatives rejoignent-elles spécifiquement les aînés face à la menace émergente des hypertrucages ?

Comme le souligne Cassar (2023), une contribution opportune et pertinente à la compréhension du rôle de la technologie face à la menace actuelle, pouvant servir de fondement à l'endiguement de la diffusion des fausses nouvelles, mérite d'être étudiée. Faire face à un tel problème peut s'avérer une responsabilité intimidante, mais l'ignorer aujourd'hui entraînera une réalité problématique pour la prochaine génération de la société (Cassar, 2023).

Les approches traditionnelles qui s'appuient sur la formation des usagers pour identifier les techniques de tromperie sont insuffisantes, particulièrement dans le cas d'attaques ciblées telles que le harponnage et le whaling (Schmitt et Flechais, 2024).

Face à ces multiples défis, il devient urgent de développer des stratégies efficaces pour renforcer la cyberrésilience des aînés.

Dans ce contexte, les approches traditionnelles qui s'appuient sur la formation des usagers pour identifier les techniques de tromperie sont insuffisantes, particulièrement dans le cas d'attaques ciblées telles que le harponnage et le whaling (Schmitt et Flechais, 2024). L'ampleur potentielle et l'automatisation des attaques malveillantes signifieront que les individus auront besoin de niveaux de sensibilisation constants et presque parfaits pour atteindre un équilibre satisfaisant entre se protéger de la tromperie tout en maintenant la confiance dans les canaux de communication (Schmitt et Flechais, 2024).



2

Objectifs et méthodologie du livre blanc

Objectifs et méthodologie du livre blanc

Face à ces enjeux complexes et multidimensionnels, ce livre blanc vise à :

- 1 Synthétiser l'état des connaissances académiques et empiriques sur les approches mises en place pour capaciter les personnes âgées face aux hypertrucages et développer leur cyberrésilience.
- 2 Recenser les initiatives terrain qui visent à renforcer leur résilience cognitive et médiatique.
- 3 Formuler des recommandations concrètes pour les acteurs de l'éducation aux médias et du numérique.

Méthodologie

Cette étude adopte une approche méthodologique mixte, articulée autour de deux volets complémentaires : une revue systématique de la littérature scientifique et grise récente, ainsi qu'une recension terrain des initiatives éducatives. Cette double démarche vise à développer une compréhension holistique des enjeux et solutions liés à la cyberrésilience des personnes âgées face aux hypertrucages et à la désinformation.

Outils d'assistance à la recherche

Dans le cadre de cette étude, les assistants d'intelligence artificielle Claude Opus 4 (Anthropic, 2025), ChatGPT-4o (OpenAI, 2025) et Copilot (Microsoft, 2025) ont été utilisés comme outils de soutien à la rédaction. Leur utilisation s'est limitée à :

- L'assistance à la synthèse et à l'organisation des données recueillies
- La vérification de la cohérence et de la structure argumentative
- L'aide à la traduction de passages clés de l'anglais vers le français
- Le support à la rédaction pour améliorer la clarté et la fluidité du texte

Il est important de souligner que toutes les analyses, interprétations et conclusions présentées dans ce livre blanc demeurent le fruit du travail intellectuel des auteurs. L'IA a servi d'outil d'assistance et non de source de contenu original.

Note sur les traductions

Sauf indication contraire, toutes les citations provenant de textes originellement publiés en anglais ont été traduites librement par les autrices afin d'en faciliter la lecture et la compréhension. Les traductions visent à préserver le sens et l'intention des auteurs originaux tout en les rendant accessibles au lectorat francophone.

Revue systématique de la littérature

Conception et démarche

La revue systématique de la littérature a été conçue suivant une méthodologie rigoureuse, structurée et reproductible, visant à synthétiser l'état actuel des connaissances sur notre sujet d'étude. Comme le définit la Bibliothèque de l'Université Laval, « la revue systématique est une méthode de synthèse de la connaissance rigoureuse, structurée et reproductible. Elle vise à vérifier si la littérature scientifique réunit des preuves suffisamment solides pour répondre, de façon précise, à une question de recherche. »

Notre question de recherche s'est portée sur l'identification des approches éducatives permettant aux personnes âgées de développer une résilience face aux hypertrucages et la capacité de les contrer, indépendamment du contexte de désinformation.

Identification des concepts et stratégie de recherche

Cinq concepts principaux ont été identifiés pour structurer notre recherche documentaire : Aînés, Éducation, Cybercriminalité, Numérique et Résilience. Pour chacun de ces concepts, nous avons développé une arborescence de mots-clés en français et en anglais, permettant de maximiser la pertinence des résultats.

La stratégie de recherche a fait appel aux opérateurs booléens pour combiner ces concepts et affiner les requêtes. Selon les bases de données consultées, les filtres ont été appliqués aux titres, aux résumés, aux mots-clés des auteurs ou au texte intégral lorsque nécessaire.

Critères de sélection

→ Critères d'inclusion

- Publications parues entre 2023 et 2025, période couvrant les travaux antérieurs et postérieurs à la démocratisation de l'intelligence artificielle générative (post-ChatGPT)
- Publications scientifiques, gouvernementales et institutionnelles
- Documents traitant des hypertrucages (deepfakes), de l'intelligence artificielle générative et de leurs implications pour les personnes aînées
- Publications accessibles en français ou en anglais
- Textes intégraux disponibles en ligne et téléchargeables en format PDF au besoin

→ Critères d'exclusion

- Thèses, mémoires académiques et monographies
- Publications antérieures à 2023
- Documents non accessibles en ligne ou sans version intégrale
- Publications dans des langues autres que le français ou l'anglais
- Études portant spécifiquement sur d'autres groupes d'âge (adolescents, enfants, étudiants, jeunes)

Sources et outils de recherche

La consultation des bases de données a été réalisée principalement via le portail de la Bibliothèque de l'Université Laval. Les disciplines explorées incluaient les Sciences de l'éducation, l'Informatique et Génie logiciel, le Génie informatique, la Criminologie, les Sciences sociales, le Génie électrique, la Médecine sociale et préventive, la Sociologie et le Travail social.

Les bases de données retenues comprenaient :

- EBSCO (Academic Search Premier, AgeLine, Computers & Applied Sciences Complete, Education Source, ERIC et Social Sciences Full Text)
- Compendex
- Inspec
- ACM Digital Library
- Google Scholar

Recherche documentaire complémentaire

En complément de la revue systématique, une recherche documentaire libre a été menée via :

- Le moteur de recherche Google
- Des bases de données de littérature grise (Greysource Index, Web of Conferences, BASE)
- Les fonctions de recherche intégrées aux sites web pertinents
- Des agents conversationnels (ChatGPT, Gemini, Claude, Copilot) pour identifier des sources supplémentaires
- L'exploration des références citées dans les articles clés
- L'analyse des publications d'auteurs spécialisés dans le domaine

Des documents de référence partagés par les organismes contactés lors de la recension terrain ont également enrichi notre corpus documentaire.

Limites méthodologiques de la revue de littérature

Notre revue systématique présente certaines limites qu'il convient de reconnaître :

- Fonctionnalités limitées de certaines bases de données comme Google Scholar pour la recherche avancée
- Prédominance des sources anglophones et rareté des bases de données francophones spécialisées sur les hypertrucages
- Accès restreint à certaines sources scientifiques
- Variations dans la définition de la catégorie « aînés » entre les études (55+, 65+, 70+, 75+)
- Ambiguïté du terme « Aged » générant des résultats hors sujet
- Possible omission de documents pertinents en raison de combinaisons incomplètes de mots-clés

Recension terrain des initiatives éducatives

Conception et démarche

Parallèlement à la revue de littérature, une recension terrain des initiatives éducatives a été réalisée du 24 juin au 15 décembre 2024. Cette démarche exploratoire visait à cartographier les interventions existantes dans la lutte contre la désinformation et la cyberfraude alimentées par l'intelligence artificielle auprès des personnes aînées.

Population cible et parties prenantes

La population cible se compose principalement des personnes aînées de 65 ans et plus, avec une attention secondaire portée aux adultes de 55 à 64 ans qui constituent une population préretraitée potentiellement vulnérable.

Les parties prenantes concernées incluent :

- Les organisations communautaires dédiées aux personnes aînées
- Les institutions financières et bancaires
- Les centres de recherche
- Les institutions académiques
- Les organismes gouvernementaux
- Les entreprises d'économie sociale
- Les tables de concertation des aînés
- Les réseau, regroupement et association pour personnes aînées
- Les résidences pour aînées
- Le réseau des bibliothèques
- Le service de police
- Le gouvernement provincial et fédéral
- Des Organismes sans but lucratif (OSBL) ou (OBNL)

Justification de l'approche exploratoire

Le choix d'une méthodologie exploratoire se justifie par :

- La nouveauté du phénomène étudié nécessitant une approche flexible
- Les contraintes temporelles et les ressources disponibles
- La complexité multidimensionnelle du sujet

Stratégie de recension

La stratégie s'est articulée autour de deux axes principaux :

- **Axe documentaire** : analyse de sites web, de littérature grise, d'articles de presse et de rapports gouvernementaux
- **Axe terrain** : consultations auprès des organisations communautaires, des institutions et des experts du domaine

Critères de sélection des initiatives

→ Critères d'inclusion

- Interventions et initiatives au Québec, au Canada et à l'international (formations, ateliers, conférences, documents explicatifs, ressources en ligne)
- Actions en lien direct avec la sensibilisation et l'éducation aux deepfakes, à l'intelligence artificielle générative et aux fraudes générées par l'IA
- Initiatives accessibles au public, spécifiquement aux personnes âgées
- Ressources disponibles via la programmation d'activités d'organismes, sites web, ou diffusées sur les réseaux sociaux

→ Mots-clés utilisés

Pour élargir la recherche, des termes comme « action », « effort », « formation », « activity », « ressources », « awareness », « campaign », « prevention », « protect », « danger », « victims », « intervention », « training », « AI scam », « deep fake » ont été utilisés en conjonction avec les descripteurs de la population âgée (« elderly », « elder », « senior », « retired person », « older adult »).

Ces combinaisons de mots-clés ont été traduites dans plusieurs langues, notamment l'espagnol, le croate, le tchèque, l'estonien, le turc, le perse, le hongrois, l'islandais, le portugais et le néerlandais.

→ Critères d'exclusion

- Initiatives non accessibles librement
- Ressources non mises à jour depuis 2023

Phases de la recension

La recension s'est déployée en deux phases distinctes :

- **Phase québécoise** : cartographie détaillée des initiatives locales et analyse des programmes existants
- **Phase élargie** : investigation au niveau canadien et international, permettant une analyse comparative et l'identification d'innovations potentiellement transférables au contexte québécois

Limites méthodologiques de la recension terrain

La recension terrain présente certaines limites qu'il convient de reconnaître :

- Impact de la période estivale sur le taux et la vitesse de réponse des organisations contactées
- Difficultés de compréhension des objectifs spécifiques de la recherche par certaines organisations
- Défis de traitement et de classification de l'importante quantité d'informations recueillies
- Absence de définition consensuelle de la notion de « personne âgée » nécessitant l'utilisation de multiples termes de recherche
- Limitations liées à la traduction de certains termes et documents
- Orientation des résultats vers des ressources nord-américaines malgré la recherche d'initiatives internationales
- Omission possible de ressources pertinentes en raison de combinaisons incomplètes de mots-clés
- Difficultés de traduction du terme « deepfake » dans certaines langues

Synthèse méthodologique

Cette approche méthodologique mixte, combinant revue systématique de la littérature et recension terrain, permet une triangulation des données et une compréhension approfondie de la problématique. La complémentarité de ces deux démarches offre une vision à la fois théorique et pratique des enjeux de cyberrésilience des personnes âgées face aux hypertrucages et aux technologies d'IA générative, ainsi que des interventions éducatives qui peuvent être mises en œuvre pour y répondre.

Malgré les limites identifiées, cette méthodologie rigoureuse a permis de constituer un corpus substantiel et pertinent pour répondre aux objectifs du livre blanc et formuler des recommandations fondées sur des données probantes.



Résultats

Résultats de la recension littéraire

Comprendre les hypertrucages et leurs impacts sur les personnes âgées

Qu'est-ce qu'un hypertrucage (deepfake) ?

Définition et évolution technologique

Les hypertrucages représentent une forme sophistiquée de médias synthétiques créés grâce à l'intelligence artificielle, dupliquant « de manière convaincante l'apparence et le discours de personnes réelles, brouillant ainsi la frontière entre réalité et illusion » (Tang et al., 2024, p. 237, traduction libre). Cette technologie permet de créer des vidéos montrant des individus accomplissant des actions fictives ou prononçant des propos qu'ils n'ont jamais tenus, ce qui peut conduire à la propagation de fausses nouvelles, particulièrement ciblant des personnalités publiques.

D'un point de vue technique, les hypertrucages sont générés à l'aide de réseaux antagonistes génératifs (GANs), fonctionnant sur « la base d'une collaboration IA de réseaux neuronaux artificiels » (Hameleers, 2024, p. 2, traduction libre). Entraînés sur des séquences authentiques, ces modèles peuvent produire des contenus synthétiques remarquablement réalistes. Le Service canadien du renseignement de sécurité (2023) les définit comme des manipulations « à l'aide d'outils de pointe faisant appel à l'intelligence artificielle pour modifier ou créer de toutes pièces des images, des voix, des vidéos ou des textes » (p. 15).

Yan et al. (2024) classifient les techniques de deepfake en quatre catégories principales : « l'échange de visage (face-swapping), la réanimation faciale (face-reenactment), la synthèse complète de visage (entire face synthesis) et l'édition faciale (face editing) » (p. 3, traduction libre). Cette diversité technique contribue à la sophistication croissante des médias synthétiques.

Ce qui rend les hypertrucages particulièrement préoccupants est leur potentiel de tromperie élevé. Hameleers et al. (2025) soulignent que « parce que les hypertrucages offrent un lien fort avec la réalité, ils sont associés à une probabilité plus faible de détection de la tromperie que la désinformation textuelle » (p. 180, traduction libre). Les individus sont généralement plus enclins à croire ce qu'ils voient plutôt que des abstractions écrites d'événements ou de phénomènes.

L'évolution rapide des technologies d'hypertrucages a considérablement simplifié leur création. Le Service canadien du renseignement de sécurité (2023) note que « la synthèse d'images à partir d'invites textuelles » constitue une avancée majeure permettant de générer des images uniques à partir de simples mots-clés (p. 16). Malgré le développement de solutions de détection, Ebner et al. (2023) observent que « les hypertrucages sont toujours capables de tromper les humains en contournant les algorithmes de détection basés sur l'intelligence artificielle » (p. 8-9, traduction libre).

Hameleers et al. (2025) soulignent que « parce que les hypertrucages offrent un lien fort avec la réalité, ils sont associés à une probabilité plus faible de détection de la tromperie que la désinformation textuelle »

Types de fraudes utilisant l'IA et les hypertrucages

L'utilisation malveillante des hypertrucages a donné naissance à diverses formes de fraudes exploitant la vulnérabilité des personnes âgées. Ces technologies sont « souvent utilisées à mauvais escient pour manipuler l'identité d'une personne ou contrôler les expressions faciales », ce qui « peut conduire à de graves crimes numériques et saper la confiance sociale » (Yan et al., 2024, p. 2, traduction libre).

Les escrocs exploitent l'IA pour perfectionner leurs stratégies de tromperie. DeLiema (2024) explique comment « l'IA générative permet aux escrocs de rédiger des messages persuasifs avec une grammaire et une ponctuation parfaites » (p. 5, traduction libre). Plus inquiétant encore, la technologie des hypertrucages est utilisée pour « cloner numériquement les voix et les ressemblances des proches des victimes », trompant celles-ci pour qu'elles transfèrent des sommes importantes (p. 5, traduction libre).

Napal (2024) détaille le phénomène de « clonage vocal » dans la production d'appels frauduleux (p. 185). Les technologies génératives utilisent des ensembles de données audio prélevés « à partir d'appels enregistrés ou de contenus publiés sur les médias sociaux » pour générer de nouveaux contenus audio convaincants (p. 186, traduction libre). Cette technique permet aux fraudeurs d'imiter la voix de proches ou de figures d'autorité pour manipuler les victimes.

Le Service canadien du renseignement de sécurité (2023) alerte sur l'intégration des hypertrucages dans « des campagnes de fraude psychologique visant à manipuler des personnes et des organisations ». Par exemple, « une vidéo 'hypertruquée' mettant en scène un être cher qui demande une forte somme d'argent, surtout s'il semble en danger, peut entraîner d'importantes pertes financières pour la cible » (p. 60).

Herrera et al. (2024) proposent une classification détaillée des communications affectées par l'IA générative dans les fraudes, couvrant le texte, les images, les voix et les vidéos. Pour les communications textuelles, l'IA permet de masquer les caractéristiques linguistiques des escrocs. Concernant les images, les technologies actuelles permettent de « fabriquer de nouvelles [images] où les caractéristiques détectables sont minimisées », créant des preuves fictives (p. 3, traduction libre). Les manipulations vocales peuvent modifier accents et inflexions, tandis que les vidéos, traditionnellement considérées comme fiables, peuvent désormais être entièrement falsifiées grâce aux « hypertrucages corporels complets » (p. 4, traduction libre).

Exemples concrets d'hypertrucages utilisés dans la désinformation et la fraude

Des cas documentés illustrent l'utilisation malveillante des hypertrucages ciblant spécifiquement les personnes âgées. Napal (2024) rapporte qu'en 2023, « deux grands-parents en Saskatchewan ont reçu un appel de quelqu'un se présentant comme leur « petit-fils » leur disant qu'il avait besoin d'argent pour sa caution après avoir été emprisonné » (p. 186, traduction libre). L'intervention d'un directeur de banque vigilant a heureusement permis d'éviter cette fraude, révélant qu'il s'agissait d'un clone vocal généré par IA.

Dans un autre cas, « un grand-parent à Terre-Neuve, au Canada, a signalé que son 'petit-fils' avait été arrêté après un accident de voiture et avait besoin de plus de 50 000 CAD pour sa caution » (traduction libre). Contrairement au premier exemple, cette personne et d'autres victimes n'ont pas échappé à l'arnaque, les personnes âgées de cette région ayant perdu « un total combiné de 200 000 USD à cause des arnaques de clonage vocal par IA » (Napal, 2024, p. 186, traduction libre).

Lawson (2023) mentionne également le cas d'un PDG d'une compagnie d'énergie ayant été escroqué de « près de 250 000 USD » après avoir été trompé par un enregistrement généré automatiquement imitant la voix d'un proche (paragr. 17, traduction libre).

Ces exemples illustrent comment les fraudeurs exploitent la technologie des hypertrucages pour cibler les personnes âgées, en s'appuyant sur des liens émotionnels forts et des situations d'urgence fictives pour extorquer des sommes importantes.

Pourquoi les personnes âgées sont une cible privilégiée des manipulations audiovisuelles

Plusieurs facteurs contribuent à faire des personnes âgées des cibles de choix pour les fraudeurs utilisant les hypertrucages. Leur vulnérabilité s'explique par une combinaison de facteurs financiers, sociaux, cognitifs et psychologiques.

La sous-déclaration des fraudes constitue un premier facteur facilitant. Comme le soulignent Deng et al. (2025), « ce qui rend les efforts antifraude plus difficiles est la sous-déclaration parmi les victimes âgées d'escroqueries » (p. 3, traduction libre). Cette réticence à signaler les incidents s'explique par une combinaison de facteurs : la honte et la peur d'être blâmé, comme nous l'avons vu précédemment, le manque d'information sur les moyens de signaler, ou encore la peur de commettre des erreurs en utilisant la technologie pour poser des questions ou signaler des activités suspectes. Cette situation crée non seulement un environnement propice pour les fraudeurs, qui peuvent opérer avec un risque réduit de détection, mais elle complexifie également le déploiement de stratégies d'aide efficaces.

La sous-déclaration des fraudes constitue un premier facteur facilitant. Comme le soulignent Deng et al. (2025), « ce qui rend les efforts antifraude plus difficiles est la sous-déclaration parmi les victimes âgées d'escroqueries » (p. 3, traduction libre). Cette réticence à signaler les incidents s'explique par une combinaison de facteurs : la honte et la peur d'être blâmé, le manque d'information sur les moyens de signaler, ou encore la peur de commettre des erreurs en utilisant la technologie pour poser des questions ou signaler des activités suspectes.

Les ressources financières des personnes âgées représentent une motivation majeure pour les fraudeurs. Après « une vie de gains et d'épargne pour la retraite, les adultes plus âgés ont accumulé plus d'actifs que les jeunes et les adultes d'âge moyen », ce qui « les rend plus attrayants pour les prédateurs financiers » (DeLiema, 2024, p. 9, traduction libre). Cette perception de richesse accumulée fait des personnes âgées des « cibles financièrement attrayantes » (McDonald et Mentis, 2023, p. 5, traduction libre).

Paradoxalement, les personnes âgées disposant de ressources limitées peuvent également être ciblées. Comme l'expliquent Robinson et Edwards (2024), une personne âgée ayant un revenu modeste peut avoir « une motivation plus élevée à prendre un risque pour améliorer sa situation financière », ce qui en fait une « cible viable » pour les fraudeurs (p. 1182, traduction libre). Thomas et al. (2023) notent l'interconnexion entre différents facteurs de vulnérabilité : « le manque d'accès, le manque de confiance, le manque de compétences numériques, le manque d'expérience/connaissances, le revenu et l'occupation plus faible » (p. 335, traduction libre).

Les traits de personnalité comme la compassion sont également exploités. Robinson et Edwards (2024) identifient cette caractéristique comme « un trait ciblé par les escrocs, en particulier dans les escroqueries basées sur la sympathie comme les escroqueries de charité » (p. 1182, traduction libre).

Les liens familiaux constituent un levier puissant pour les fraudeurs. Espinoza (2024) note que « 83 % des personnes âgées de 65 ans et plus aux États-Unis reconnaissent avoir des petits-enfants », ce qui augmente l'efficacité des arnaques où les fraudeurs se font passer « pour un petit-enfant en détresse » (p. 7, traduction libre). Cette stratégie exploite les liens affectifs forts et le désir naturel de porter secours à ses proches.

Facteurs qui font des personnes âgées des cibles vulnérables

→ Facteurs cognitifs et mémoire de travail

Les changements cognitifs liés à l'âge accroissent la vulnérabilité des personnes âgées face aux fraudes sophistiquées. DeLiema (2024) observe que « les déclin du fonctionnement cognitif et, plus spécifiquement, les déclin du fonctionnement exécutif, sont les facteurs de risque les plus cités pour la victimisation par escroquerie chez les adultes plus âgés » (p. 8, traduction libre).

Ebner et al. (2023) expliquent que « la vitesse de traitement, la mémoire de travail et les fonctions exécutives déclinent avec l'âge », impactant directement la façon dont les informations sont traitées (p. 3, traduction libre). Si « la prise de décision intuitive reste relativement préservée en fin de vie », le « traitement systématique de l'information devient moins efficace », entraînant « une plus grande dépendance aux heuristiques par rapport à la délibération » (p. 3, traduction libre). Cette tendance augmente la susceptibilité aux tromperies.

Chen et al. (2025) confirment que les adultes âgés peuvent être « particulièrement vulnérables à la fraude en raison de leur dépendance aux modèles de traitement de l'information heuristique », les amenant à « négliger des signes cruciaux de fraude » (p. 464, traduction libre). Les limitations de la mémoire à court terme constituent également un facteur significatif, affectant « la capacité à gérer les mots de passe et à maintenir la confidentialité en ligne » (Sheil, 2024, p. 1, traduction libre).

Xin et al. (2024) synthétisent les principaux facteurs de risque identifiés dans la littérature : « le déclin des fonctions cognitives et physiques, les traits de crédulité (confiance facile, agréabilité), l'isolement social, la prise de risque et l'analphabétisme financier » (p. 2, traduction libre).

→ Facteurs émotionnels et psychologiques

Les aspects émotionnels jouent un rôle crucial dans la vulnérabilité des personnes âgées. Ebner (2023) observe que « l'affect négatif améliore la détection de la tromperie, tandis que l'affect positif l'altère » (p. 4, traduction libre). Paradoxalement, « un affect positif plus élevé était associé à une capacité réduite à détecter les fausses nouvelles avec un âge chronologique plus élevé chez les adultes plus âgés » (p. 4, traduction libre).

Les fraudeurs exploitent délibérément les réactions émotionnelles de leurs victimes. DeLiema (2024) explique qu'ils « utilisent des tactiques pour susciter de puissantes émotions », tant positives (excitation, surprise) que négatives (colère, peur) (p. 7, traduction libre). Ces « émotions à forte excitation consomment des ressources cognitives et motivent les individus à agir immédiatement par instinct plutôt que par analyse raisonnée » (p. 7, traduction libre).

Le sentiment d'urgence constitue une tactique particulièrement efficace. Les escrocs « exercent une pression intense sur leurs cibles pour qu'elles agissent rapidement », produisant « une réponse émotionnelle qui altère la pensée rationnelle » et réduisant le temps disponible « pour poser des questions critiques et demander un second avis » (DeLiema, 2024, p. 7-8, traduction libre).

La peur de la mort représente un facteur psychologique spécifique exploité par certains fraudeurs, particulièrement dans les escroqueries liées à la santé. Chen et al. (2024) définissent l'anxiété face à la mort comme « une réaction émotionnelle négative provoquée par l'anticipation d'un état dans lequel le soi n'existe pas » (p. 292, traduction libre). Cette émotion est « répandue chez les adultes plus âgés en raison des pertes liées à l'âge », comme la diminution des capacités physiques et les maladies chroniques (p. 292, traduction libre).

→ Facteurs sociaux : respect de l'autorité et isolement

Le respect de l'autorité constitue un levier puissant pour les fraudeurs ciblant les personnes âgées. Logie et Das (2024) observent que « de nombreux fraudeurs privilégiaient l'usurpation d'identité de figures d'autorité » pour manipuler les personnes âgées (p. 25, traduction libre). DeLiema (2024) explique que cette tactique fonctionne car « les gens ont tendance à suivre les conseils d'experts crédibles et compétents » (p. 7, traduction libre). Napal (2024) confirme que « les personnes âgées sont particulièrement vulnérables aux appels d'arnaque – beaucoup font davantage confiance aux personnes qui se présentent comme ayant de l'autorité, du pouvoir ou de l'influence » (p. 185, traduction libre).

L'isolement social représente un autre facteur de vulnérabilité majeur. Ebner et al. (2023) identifient « l'isolement social et la dépendance aux autres pour les activités de la vie quotidienne » parmi les principaux facteurs de risque (p. 2, traduction libre). Les fraudeurs exploitent consciemment cette vulnérabilité, comme le notent Deng et al. (2025) : « les escrocs ont remarqué le rôle potentiellement protecteur des membres de la famille pour contrer la fraude, ils ont donc exploité l'isolement social pour manipuler les cibles afin de cacher des informations aux membres de la famille » (p. 3, traduction libre).

Les transitions de vie majeures augmentent également la vulnérabilité. DeLiema (2024) confirme que « les événements majeurs de la vie tels que la retraite, le veuvage, le divorce et l'apparition d'un handicap peuvent également augmenter le risque de victimisation » (p. 9, traduction libre). Liao et al. (2024) soulignent que « de nombreuses personnes âgées vivent seules », les laissant « sans la surveillance protectrice des membres de la famille » (p. 511, traduction libre).

→ Manque de connaissances technologiques

Le décalage générationnel face aux technologies constitue un facteur de vulnérabilité significatif. Augenbaum (2024) souligne le « manque de sensibilisation » des personnes âgées concernant « les différents types d'escroqueries en ligne et les tactiques sophistiquées utilisées par les cybercriminels » (p. 711, traduction libre). Ce déficit de connaissances technologiques les rend particulièrement vulnérables aux fraudes sophistiquées comme les hypertrucages.

Herrera et al. (2024) identifient parmi les facteurs de risque une « conscience limitée des menaces, une faible littératie numérique, une acceptation lente des nouvelles technologies, et des connexions limitées à d'autres personnes pouvant fournir un soutien compétent » (p. 2, traduction libre). Ces éléments se combinent pour créer un environnement propice à l'exploitation par des acteurs malveillants.

Tang et al. (2024) observent que « les seniors peuvent rencontrer des difficultés à détecter la désinformation et les hypertrucages en raison d'une familiarité technologique limitée » (p. 237, traduction libre). La « prévalence des hypertrucages sur diverses plateformes en ligne aggrave encore ce problème, car les seniors peuvent rencontrer de la désinformation sans les compétences nécessaires pour identifier les manipulations ou les incohérences » (p. 237, traduction libre).

→ Les défis de la détection des hypertrucages

La difficulté à reconnaître les hypertrucages constitue un défi majeur, particulièrement pour les personnes âgées. Comme l'expliquent Tang et al. (2024), « les personnes âgées sont vulnérables en raison d'un manque relatif de connaissances technologiques, combiné à leur difficulté à distinguer le contenu authentique du contenu manipulé » (p. 237, traduction libre). Ce défi est amplifié par la sophistication croissante des technologies de deepfake.

Un biais psychologique fondamental rend les hypertrucages particulièrement difficiles à détecter. Hameleers (2024) explique que « la représentation apparemment plus directe du discours politique des hypertrucages peut contourner le traitement critique des arguments du message plus que les 'cheapfakes', étant donné que l'heuristique 'voir, c'est croire' est invoquée davantage pour les hypertrucages » (p. 3, traduction libre). Cette tendance naturelle à faire confiance à ce que nous voyons rend les médias visuels manipulés particulièrement efficaces pour la désinformation.

Une étude menée par Tang et al. (2024) auprès de personnes âgées de 55 à 70 ans a identifié cinq stratégies principales utilisées par les seniors pour tenter d'identifier les vidéos deepfake :

- 1 **L'apparence du personnage** : analyse des expressions faciales, mouvements des yeux, présence de rides, ainsi que la posture et le langage corporel.
- 2 **Les aspects visuels non humains** : attention portée à la résolution de l'image, aux coupures abruptes dans la vidéo et à la cohérence des objets d'arrière-plan.
- 3 **L'audio** : vérification de la synchronisation labiale, des modulations de voix et de la qualité sonore.
- 4 **Les connaissances personnelles** : utilisation des connaissances préexistantes sur le contenu de la vidéo et les personnes qui y apparaissent.
- 5 **Les sources externes** : consultation d'amis, de famille ou d'experts pour évaluer la crédibilité d'une vidéo.

Malgré certains aspects de succès de quelques-unes de ces stratégies, l'efficacité de détection reste limitée. Chun et al. ont observé que « la précision d'identification pour les hypertrucages était faible (55 %) lors de la première semaine » d'exposition, s'améliorant progressivement pour atteindre « 70 % pour les semaines 2 et 3 » (p. 877, traduction libre).

Une enquête de l'Ifop (2024) révèle que 88 % des Français de 65 ans et plus « ne s'estiment pas du tout capables de discerner une image ou une vidéo générée par une IA » (p. 6, traduction libre). Cette même étude montre également que 38 % des Français de 65 ans et plus « ne savent pas ce que sont les hypertrucages » (p. 18, traduction libre), ce qui constitue un obstacle fondamental à leur détection.

Les résultats de ces études soulignent l'urgence de développer des programmes d'éducation spécifiquement adaptés aux personnes âgées pour renforcer leur capacité à identifier les médias manipulés et à se protéger contre les fraudes utilisant les technologies de deepfake.

Revue des connaissances sur les interventions pour renforcer la cyberrésilience des personnes âgées face aux hypertrucages

Approches éducatives et de sensibilisation

L'éducation et la sensibilisation constituent le principal axe d'intervention pour renforcer la cyberrésilience des personnes âgées face aux hypertrucages et autres formes de désinformation numérique. Comme le soulignent Azam et al. (2024), « l'éducation est essentielle, particulièrement alors que les utilisateurs sont constamment exposés aux cybermenaces, indépendamment du temps ou du lieu » (p. 91, traduction libre). La « sensibilisation à la cybersécurité » fait référence à la compréhension qu'a un individu de la sécurité en ligne, incluant la connaissance des menaces de sécurité actuelles et des meilleures pratiques, ainsi que des risques posés par des comportements dangereux.

Plusieurs modèles d'éducation à la cybersécurité adaptés aux personnes âgées ont été développés. Azam et al. (2024) décrivent notamment le modèle OSICSAM (Organization, Social, and Individual Cyber Security Awareness Model), conçu en Malaisie en intégrant « des modèles existants de cybersécurité avec les préférences d'apprentissage des personnes âgées, [leurs rythmes d'apprentissage et leurs expériences antérieures] incorporant des éléments organisationnels, sociétaux et individuels » (p. 92, traduction libre). Les mêmes auteurs présentent également le Cadre de sensibilisation à la cybersécurité pour les personnes âgées, qui inclut « sept étapes clés pour les utilisateurs âgés afin de protéger leurs informations personnelles en ligne : mettre à jour les logiciels, corriger les appareils, utiliser des mots de passe forts, identifier les menaces et attaques actuelles, améliorer les compétences Internet, établir des systèmes de soutien, et toujours se déconnecter après utilisation » (p. 93, traduction libre).

Pour répondre aux défis spécifiques des personnes âgées, Azam et al. (2024) ont proposé le modèle SCSAM-Elderly (Synergistic Cyber Security Awareness Model for the Elderly), qui offre « une approche sur mesure, moins technique, à l'éducation à la cybersécurité pour les personnes âgées » (p. 93, traduction libre). Ce modèle aborde leurs vulnérabilités spécifiques et s'appuie sur des méthodes accessibles pour améliorer leur sensibilisation et leur compréhension des cybermenaces. Les auteurs suggèrent d'intégrer ce modèle « dans des campagnes de sensibilisation publique, des programmes communautaires et des initiatives d'alphabétisation numérique ciblant la population âgée » (p. 104, traduction libre).

La personnalisation des approches éducatives selon l'âge apparaît comme un facteur clé de succès. Ebner et al. (2023) soulignent « la nécessité d'avertissements adaptés à l'âge (au lieu d'une approche universelle) pour améliorer les tentatives de détection de tromperie car elles varient selon les contextes » (p. 6, traduction libre). Les mêmes auteurs notent que « des formations espacées et multi-sessions peuvent être particulièrement bénéfiques pour les populations vieillissantes, selon les approches réussies issues de la littérature sur l'entraînement cognitif du vieillissement » (p. 7, traduction libre).

Le contenu des programmes éducatifs doit également être adapté aux besoins spécifiques des personnes âgées. Ebner et al. (2023) suggèrent que « les efforts futurs de conception d'interventions pourraient bénéficier de l'incorporation de composantes de formation ciblant la promotion de la littératie financière et sanitaire pour améliorer la prise de décision complexe et réduire la susceptibilité à la fraude chez les adultes âgés » (p. 8, traduction libre). Fatima et al. (2024) soulignent que « l'amélioration de la littératie numérique joue un rôle clé dans l'autonomisation des adultes plus âgés pour naviguer en toute confiance et en sécurité sur les plateformes de rencontres en ligne » (p. 6, traduction libre).

Wang et al. (2025) présentent des résultats contre-intuitifs concernant l'éducation : « les résultats de la régression logistique indiquent que l'éducation est positivement liée aux risques de ciblage et de victimisation de fraude en ligne, contrairement à ce que prédirait la perspective d'inégalité numérique ». Une explication possible est que « l'éducation peut également être liée au niveau de sensibilisation des adultes âgés ou à leur expressivité concernant les expériences de fraude en ligne » (p. 9, traduction libre). Ces résultats suggèrent que la sensibilisation et l'éducation doivent être complétées par d'autres approches.

Sádaba et al. (2023) rappellent que « Spohr (2017) met en garde sur l'importance de sensibiliser les citoyens à la nécessité de rechercher des informations provenant de sources diverses (Bakshy et al., 2015) » et que « l'éducation aux médias a également été identifiée comme essentielle pour combattre la polarisation politique (Gaultney et al., 2022) » (p. 2, traduction libre). Les auteurs notent l'intérêt récent pour « les actions d'éducation aux médias et au numérique visant ce segment de population (Ramírez García et al., 2017) » et, « compte tenu de leur intérêt manifeste pour les actualités, cette étude expérimentale permet d'affirmer la pertinence de concevoir des actions spécifiques destinées à ce segment de population (Tucker et al., 2018) » (p. 8, traduction libre).

Cependant, l'approche éducative traditionnelle présente certaines limites. Schmitt et Flechais (2024) critiquent la logique circulaire selon laquelle « si quelqu'un échoue à un test d'hameçonnage ou devient victime d'ingénierie sociale, cela est généralement interprété comme un signe qu'il n'a pas été suffisamment formé ou qu'il n'a pas prêté assez d'attention, ce qui est ensuite utilisé comme justification pour plus de sensibilisation, de formation et d'éducation » (p. 13, traduction libre). Cette approche peut conduire à blâmer les victimes plutôt qu'à reconnaître les limites inhérentes aux stratégies de protection individuelles face à des menaces sophistiquées comme les hypertrucages.

McDonald et Mentis (2023) proposent une approche différente de l'éducation à la cybersécurité : « Une façon de penser à l'éducation et aux protections de cybersécurité pour n'importe quel groupe, y compris les adultes plus âgés, est de penser, non pas à quel ensemble de faits les gens connaissent, mais à comment ils conceptualisent leur moi numérique et comment ils naviguent et atteignent des personnes pour obtenir du soutien » (p. 4, traduction libre). Ils soulignent que « l'éducation à la cybersécurité devrait mettre l'accent sur l'évitement des communications et des produits que les utilisateurs n'ont pas demandés, comme un colis, des prêts ou des cadeaux » et « ne devrait pas utiliser les mêmes tactiques littéraires que celles utilisées dans les courriels d'hameçonnage » (p. 16, traduction libre).

Formation et développement des compétences numériques

Au-delà de la simple sensibilisation, la formation pratique et le développement des compétences numériques sont essentiels. Sullivan et Kosuth (2024) notent que « pour ces répondants, la technologie est une ressource significative pour rester connectés; cependant, des niveaux modérés à faibles de satisfaction avec les appareils indiquent le besoin de formation supplémentaire pour les adultes plus âgés sur la meilleure et la plus sûre utilisation de ces appareils. Simplement avoir accès à la technologie n'est pas suffisant » (p. 30, traduction libre).

Diel et al. (2024) suggèrent que « la formation par rétroaction peut améliorer les stratégies perceptuelles pour détecter les hypertrucages, et l'efficacité de la formation pourrait être améliorée en fournissant aux utilisateurs des conseils supplémentaires sur la façon de détecter les hypertrucages. La performance peut être encore améliorée en permettant aux utilisateurs formés d'utiliser l'IA » (p. 8, traduction libre).

Rodríguez-Miranda et al. (2025) soulignent que « pour faire face à cette réalité, il est nécessaire de comprendre les concepts de base de la cybersécurité et d'être conscient des tactiques utilisées par les cybercriminels. Les adultes plus âgés peuvent protéger leurs informations personnelles et profiter d'une expérience en ligne plus sûre s'ils sont formés pour le faire » (p. 3, traduction libre). Leurs recherches ont confirmé que l'échelle basée sur le cadre DigComp (Digital Competence Framework for Citizens), un projet mis en place par le Centre commun de recherche pour la Commission européenne, « est un outil valide et fiable pour évaluer les compétences numériques dans la navigation sur Internet et la cybersécurité chez les adultes plus âgés » (p. 7, traduction libre).



Sheil et al. (2024) rapportent que leur suggestion « d'éviter les arnaques en vérifiant les sites web via le site Check My Link s'est avérée très populaire, beaucoup en prenant note », car « certains adultes plus âgés ne savaient pas que le symbole de cadenas dans l'URL ne garantit pas complètement la légitimité d'un site web » (p. 4, traduction libre).

Ferguson et al. (2024) insistent sur l'importance « de s'attaquer aux obstacles à l'entrée pour les populations d'adultes plus âgés à faible revenu, comme le développement de programmes pour connecter les individus à la formation sur les appareils tout en fournissant un soutien aux utilisateurs et un environnement encourageant pour favoriser l'apprentissage » (p. 2, traduction libre).

Approches innovantes et inoculation psychologique

Des approches innovantes émergent pour compléter les méthodes éducatives traditionnelles. L'inoculation psychologique, en particulier, semble prometteuse. Aung et al. (2024) la définissent comme « une approche basée sur la sensibilisation et l'éducation pour développer une résilience cognitive aux tentatives de persuasion » (p. 5, traduction libre). Cette méthode comprend deux éléments : la préemption réfutationnelle et la menace. La préemption réfutationnelle -- ou « pré-bunking » -- implique de fournir aux destinataires les informations nécessaires pour résister à la tentative persuasive, souvent en incluant des arguments ou des preuves qui remettent en question la perspective présentée dans l'attaque.

La ludification apparaît comme un moyen efficace d'appliquer la théorie de l'inoculation. Aung et al. (2024) expliquent que « les approches gamifiées peuvent fournir une inoculation 'active', qui serait plus efficace pour favoriser l'acquisition de compétences et la rétention d'informations que les approches traditionnelles d'inoculation 'passive' (par exemple, les campagnes de lecture) » (p. 5, traduction libre). Les auteurs notent que « les preuves en faveur de l'inoculation gamifiée proviennent principalement d'études récentes sur la lutte contre les fausses nouvelles en ligne » (p. 5, traduction libre) et recommandent « des affinements continus basés sur les retours des utilisateurs et des tests itératifs pour assurer un processus d'apprentissage plus efficace et engageant, soutenant efficacement une résilience à plus long terme chez les adultes plus âgés » (p. 21, traduction libre).

Tang et al. (2024) suggèrent que « les éducateurs et les décideurs politiques peuvent adapter les stratégies pour concevoir des programmes de formation aidant les seniors à identifier les hypertrucages » (p. 242, traduction libre), en s'appuyant sur les cinq stratégies d'identification identifiées dans leur étude (analyse de l'apparence du personnage, des aspects visuels non humains, de l'audio, utilisation des connaissances personnelles et consultation de sources externes).

Ebner et al. (2023) proposent que « des solutions de défense adaptées à l'âge pourraient être développées pour offrir un avertissement immédiat concernant des messages potentiellement trompeurs (par exemple, dans les SMS, les courriels, les plateformes de médias sociaux) en utilisant des algorithmes d'apprentissage automatique basés sur le langage naturel et les images » (p. 9, traduction libre). Cette approche technique compléterait les efforts d'éducation en fournissant une assistance en temps réel.

Systèmes de vérification et aspects techniques

Les interventions techniques constituent un autre axe important pour renforcer la cyberrésilience des personnes âgées. Fatima et al. (2024) recommandent, par exemple, pour les sites de rencontre en ligne, la mise en œuvre de systèmes avancés de vérification d'identité » (p. 6, traduction libre). Ils expliquent que « la vérification vidéo en temps réel lors de la configuration du compte peut réduire considérablement la prévalence des faux profils, répondant particulièrement à la tendance des personnes âgées à se fier aux photos de profil pour établir une confiance initiale » (p. 6, traduction libre).

Les auteurs proposent également « un système de vérification progressif à plusieurs niveaux, où les utilisateurs peuvent vérifier des aspects supplémentaires de leur identité (par exemple, profession, éducation) pour gagner des badges 'de confiance' » (p. 6, traduction libre). Cette approche répond aux préoccupations concernant l'authenticité des informations de profil. Enfin, ils suggèrent « d'afficher de manière proéminente le statut de vérification avec des icônes ou des étiquettes claires et facilement compréhensibles » (p. 6, traduction libre), ce qui répond à la préférence des personnes âgées pour des éléments d'interface simples.

Sheil et al. (2024) rapportent des stratégies pratiques développées par les aînés eux-mêmes : « certains participants ont révélé qu'ils avaient leurs propres stratégies pour faire face aux messages d'arnaque, par exemple en s'assurant que si leurs enfants étaient réellement en danger, ils utilisent un mot de sécurité que seuls eux connaîtraient. De cette façon, ils peuvent vérifier s'il s'agit bien d'eux » (p. 4, traduction libre). Cette approche simple mais efficace peut être intégrée dans les programmes de formation.

Fatima et al. (2024) soulignent également l'importance de « développer des ressources claires et accessibles, telles que des vidéos d'instruction et des guides imprimables [qui] soutiendront les adultes plus âgés dans la maîtrise des interactions en ligne » (p. 6, traduction libre). Ces ressources doivent être conçues spécifiquement pour répondre aux besoins et préférences des aînés.

Horstmann et al. (2023) rappellent que « les nouvelles technologies conçues pour les adultes plus âgés sont souvent liées à un paternalisme bienveillant qui vise à 'protéger' les adultes plus âgés. Cependant, comme cela est perçu par les adultes plus âgés comme très désagréable, les concepteurs devraient donner la priorité aux mesures de protection de la vie privée dès le début, plutôt que de considérer la vie privée comme un complément fastidieux qui ne fait qu'inhiber la collecte de données et la fonctionnalité » (p. 6, traduction libre). Cette observation souligne l'importance de concevoir des technologies qui respectent l'autonomie des aînés tout en les protégeant.

Approches législatives et réglementaires

Les interventions législatives et réglementaires constituent un pilier essentiel pour lutter contre les hypertrucages et protéger les populations vulnérables. Fatima et al. (2024) soulignent que « la législation imposant des audits de sécurité réguliers et une stricte conformité à la protection des données garantira que les plateformes de rencontres répondent à des normes de sécurité élevées, en particulier pour protéger les utilisateurs contre les arnaques en ligne » (p. 7, traduction libre).

Cassar (2023) observe que « les résultats recueillis indiquent clairement que le gouvernement est l'une des entités potentielles plus importantes qui peuvent être un influenceur pour annoncer les contre-mesures nécessaires concernant la propagation des fausses nouvelles » (p. 20, traduction libre). Le Service canadien du renseignement de sécurité (2023) ajoute que « les organismes gouvernementaux ont un rôle essentiel à jouer pour orienter les stratégies nationales de recherche, afin que davantage de ressources soient investies dans l'étude de mesures visant à lutter contre les hypertrucages, mais aussi pour axer les efforts législatifs sur le contrôle du problème » (p. 43).

Lawson (2023) décrit l'approche canadienne en matière de régulation des hypertrucages, qui comprend « une stratégie à trois volets incluant la prévention, la détection et la réponse » (paragr. 21, traduction libre). Pour prévenir la création et la distribution d'hypertrucages, « le gouvernement canadien travaille à sensibiliser le public à la technologie et à développer des technologies de prévention ». Pour détecter les hypertrucages, « le gouvernement a investi dans la recherche et le développement de technologies de détection ». En termes de réponse, « le gouvernement explore une nouvelle législation qui rendrait illégal de créer ou de distribuer des hypertrucages avec une intention malveillante » (paragr. 21, traduction libre). L'auteur ajoute que « les mécanismes de recours, tels que les avis de retrait ou les actions en justice, peuvent répondre aux questions de droits d'auteur et de diffamation » (paragr. 41, traduction libre).

Le Bureau du directeur général des élections du Canada (2024) a formulé plusieurs recommandations spécifiques concernant la lutte contre les hypertrucages dans le contexte électoral :

- La recommandation 1.3 propose de « modifier la disposition de la LEC relative à l'usurpation de qualité (art. 480.1) pour qu'elle s'applique à toute présentation trompeuse des personnes énumérées aux alinéas a) à e), dont la voix ou l'image est manipulée par quelque moyen que ce soit » (p. 15).
- La recommandation 1.4 suggère d'« élargir la portée des articles 480.1 et 481 pour qu'ils s'appliquent également en dehors d'une période électorale » (p. 16).
- La recommandation 1.5 stipule que « toute communication électorale payée et non payée (sous forme d'image, d'audio, de vidéo ou de texte), diffusée pendant une période préélectorale réglementée ou une période électorale, qui a été générée ou manipulée par IA, devrait inclure une marque indiquant clairement le recours à l'IA » (p. 16).
- Enfin, la recommandation 1.6 suggère, pour « s'assurer que les abonnés obtiennent de l'information exacte lorsqu'ils cherchent à savoir où, quand et comment s'inscrire et voter, [d'] obliger les plateformes qui utilisent des agents conversationnels ou des fonctions de recherche générés par IA à indiquer dans leurs réponses où trouver l'information officielle » (p. 16).

Makhortykh (2024) souligne que « la littératie numérique et l'éducation des utilisateurs sont des interventions précieuses, mais les décideurs politiques et les développeurs et implémenteurs d'IA doivent également prendre des mesures et faire des choix de conception qui protègent les informations historiques » (p. 5, traduction libre).

Approches communautaires et participation sociale des aînés

La participation sociale des aînés et les approches communautaires représentent une dimension importante pour renforcer leur résilience. Havers et al. (2024) notent que « la honte entourant la victimisation par cybercriminalité a été attribuée à des attitudes âgistes omniprésentes qui blâment les victimes aînées » (p. 8, traduction libre). Pour contrer cette stigmatisation, ils suggèrent la transmission de « messages clés aux victimes et non-victimes de tous âges qui remettent en question les idées fausses entourant la crédulité des victimes ou l'ineptie technologique » (p. 8, traduction libre).

Les approches communautaires offrent un cadre propice aux interventions. Havers et al. (2024) rapportent que les personnes interrogées « ont discuté de la valeur des sessions de groupe interactives en personne pour les adultes plus âgés dans les espaces communautaires, comme une modalité d'intervention potentielle » (p. 9, traduction libre).

La participation sociale des personnes aînées a été documentée dans diverses sphères de la vie sociale, notamment « sur le plan de la participation politique et des mouvements sociaux » (Charpentier et Quéniart, 2007; Gottlieb et Gillespie, 2008; Serrat et al., 2018, traduction libre, cités dans Marchand et Laau-Laurin, 2024, p. 3), « dans l'action bénévole accomplie au sein d'organismes et d'associations » (Castonguay et al., 2015; Gagnon et al., 2004; Grenier, 2012; Lie et al., 2009; Pavelek, 2013; Sévigny et Vézina, 2007, traduction libre, cités dans Marchand et Laau-Laurin, 2024, p. 3) et « dans la proche aide » (Arriagada, 2020; Lavoie et Guberman, 2009; Saillant et Gagnon, 2001, traduction libre, cités dans Marchand et Laau-Laurin, 2024, p. 3).

Cette participation sociale est définie comme « l'engagement conscient et actif au sein d'activités sociales conduisant à l'interaction et au partage de ressources avec d'autres personnes de la communauté; la personne éprouve une satisfaction personnelle résultant de cet engagement » (Dehi Aroogh et al., traduction libre, cité dans Marchand et Laau-Laurin, 2024, p. 4). Elle apparaît « tributaire des expériences de vie antérieures, et elle est influencée par des déterminants sociaux et environnementaux tels que le support social, la discrimination à l'égard de l'âge (âgisme), l'accès aux transports, aux loisirs et aux services, le sentiment de sécurité, etc. » (Dehi Aroogh et al., 2020, traduction libre, cité dans Marchand et Laau-Laurin, 2024, p. 4).

Marchand et Laau-Laurin (2024) observent que « dans les récits, les personnes aînées agissent souvent comme moteur de l'action collective (en prenant des initiatives, développant des programmes et des services); elles sont partie prenante d'un système d'action local (Klein, 2006; Fontan et Klein, 2020) » (p. 15). « Contrairement aux idées reçues qui les positionnent comme des réceptacles passifs de soin, les résultats montrent que les personnes aînées sont aussi des propulseurs d'innovations socioterritoriales » (p. 15). En effet, « contrairement aux discours âgistes qui posent les personnes aînées comme un poids pour la société, ou encore un 'handicap' pour les territoires ruraux (Gucher, 2013) », leur recherche montre que « ces dernières ont une influence certaine sur l'amélioration des conditions de vie en participant à l'effort collectif pour bâtir des communautés résilientes et vivantes » (p. 15).

Dans des contextes ruraux, « l'entraide mise en relief dans les témoignages se matérialise dans les réseaux de réciprocité et d'échange, qui rythment l'aide qui se transige entre les individus, voire entre les organisations et les citoyen-ne-s. À l'échelle territoriale, les personnes aînées agissent au sein du système local d'action et développent des initiatives permettant l'innovation socioterritoriale afin de répondre à un problème social ou à un besoin de leur communauté » (Marchand et Laau-Laurin, 2024, p. 15).

Cette perspective est particulièrement pertinente dans le contexte de la lutte contre la désinformation et les hypertrucages. Les personnes aînées peuvent jouer un rôle actif dans l'éducation par les pairs et le partage d'expériences, contribuant ainsi au renforcement de la résilience collective face aux manipulations numériques.

Approches multidimensionnelles et personnalisées

La complexité des défis posés par les hypertrucages et autres formes de désinformation numérique nécessite des approches multidimensionnelles et personnalisées. Herrera et al. (2024) proposent des recommandations qui, « contrairement aux approches actuelles qui placent un fardeau significatif de protection sur les victimes potentielles, visent à rediriger ce fardeau ». Ces recommandations sont divisées en « quatre domaines interconnectés : Programmes de formation à la sensibilisation, Législation et politique, Récupération, et Avancées technologiques » (p. 6, traduction libre).

DeLiema (2024) propose trois niveaux de stratégies :

1. **Prévention primaire** : « Améliorer la sensibilisation aux arnaques • réduire l'isolement social et la solitude • activer les comptes en ligne et mobiles • opter pour des fonctionnalités de sécurité de compte • s'engager dans une planification financière préalable • nommer un contact de confiance pour chaque compte de retraite et d'investissement » (p. 11, traduction libre).
2. **Prévention secondaire** : « Enquêter sur les activités et comportements suspects • poser des questions et éduquer les participants au plan sur les risques de fraude • sécuriser les comptes par des blocages temporaires • signaler la fraude aux forces de l'ordre • récupérer les fonds • orienter vers des services de soutien aux victimes » (p. 11, traduction libre).
3. **Prévention tertiaire** : « Contacter la personne de confiance • impliquer les mandataires pour fournir un soutien et une surveillance financière • surveiller les comptes financiers • répondre aux besoins non satisfaits (par exemple, sécurité financière, interaction sociale, sentiment d'utilité) • Orientation vers des services juridiques, financiers et de santé mentale » (p. 11, traduction libre).

Cassar (2023) souligne que « les résultats obtenus de cette recherche (enquête et entretiens) ainsi que des données similaires d'autres études suggèrent qu'il n'y a pas une solution unique qui puisse entièrement contourner la désinformation. Une approche multidisciplinaire provenant de différents corps de pouvoir, entités et individus experts est impérative pour s'attaquer à une telle menace » (p. 20, traduction libre). L'auteur note que « l'implication du gouvernement, avec des spécialistes du domaine, est vitale pour une législation nouvelle et améliorée, en plus d'un programme éducatif révisé à tous les niveaux d'éducation » (p. 20, traduction libre). Cependant, « les résultats indiquent que les gouvernements seuls n'apporteront pas le changement nécessaire. Le secteur privé, les ONG et les institutions académiques et de recherche auront également un rôle crucial à jouer dans l'obtention de la confiance des communautés et l'expression de leurs préoccupations, transformant la question en une responsabilité partagée » (p. 20, traduction libre).

Un aspect important de ces approches multidimensionnelles concerne l'éthique. Cassar (2023) rapporte que « les participants ont collectivement réalisé que la première étape de la longue route à parcourir pour freiner les fausses nouvelles est l'introduction d'initiatives qui doivent être moins axées sur la technologie et plus sur les capacités d'éthique et de confiance » (p. 20, traduction libre). Les participants ont également « convenu que la réforme éducative est également nécessaire non seulement pour sensibiliser le public à la désinformation, mais aussi pour

apprendre des compétences de vie essentielles » (p. 20, traduction libre). Dès le jeune âge, « les gens bénéficieraient d'une telle réforme car ils seraient capables d'apprendre et de pratiquer efficacement des compétences, notamment la recherche, la vérification des informations et, en fin de compte, le discernement entre ce qui est juste et ce qui est faux » (p. 20, traduction libre).

Sádaba et al. (2023) soulignent l'importance d'adapter ces interventions aux caractéristiques spécifiques des différents groupes d'âge : « Compte tenu de l'importance des émotions par rapport aux connaissances objectives dans le contexte idéologique polarisé actuel, il semble pertinent que les actions d'alphabétisation médiatique et numérique prennent également en compte les particularités du public cible » (p. 8, traduction libre). Les auteurs notent que « étant donné que les citoyens plus âgés sont plus susceptibles de voter, de consommer des médias traditionnels et de participer activement à la politique, nous pouvons supposer que diriger les efforts pour renforcer la résilience contre la désinformation vers ce segment de la population peut avoir des effets particulièrement bénéfiques sur le rétablissement global de la confiance du public » (p. 8, traduction libre).

Enfin, l'Institut national de santé publique du Québec (2023) rappelle l'importance de mesures plus larges pour favoriser un vieillissement en santé : « Tout au long du parcours de vie, l'adoption d'un mode de vie physiquement actif peut contribuer à prévenir ou retarder l'apparition des troubles neurocognitifs majeurs, en plus d'avoir plusieurs autres bénéfices pour la santé » (p. 5). L'institut souligne la pertinence de « l'aménagement d'infrastructures de loisir universellement accessibles et proposant des activités attrayantes à coûts réduits ou gratuits » pour favoriser un vieillissement en santé, ainsi que « des stratégies de mobilisation communautaire visant à en maximiser l'utilisation » (p. 5). L'institut recommande également des « politiques et mesures agissant directement sur l'âgeisme [qui] doivent être promues auprès de partenaires de différents secteurs, comme le travail, l'enseignement, les médias et le réseau de la santé et des services sociaux. Il convient aussi de rendre disponibles des lieux publics intérieurs et extérieurs propices aux rapprochements intergénérationnels » (p. 5).

Cette dimension intergénérationnelle est une composante clé des approches multidimensionnelles. Elle se matérialise dans des initiatives concrètes comme le programme de jumelage informatique Générations@branchées, proposé par les bibliothèques publiques du Québec, qui favorise l'entraide et le partage de connaissances entre des adolescents et des aînés. De tels programmes créent des dynamiques d'apprentissage mutuellement enrichissantes où les jeunes, souvent plus au fait des nouvelles technologies comme les hypertrucages, peuvent outiller les aînés, tandis que ces derniers partagent leur expérience de vie et leur esprit critique.



Vers une approche intégrée de la cyberrésilience

Design inclusif et autonomisation

La conception des technologies destinées aux personnes âgées représente un enjeu crucial pour renforcer leur cyberrésilience. Horstmann et al. (2023) soulignent que « lors de la conception et de la mise en œuvre de nouvelles technologies pour les adultes plus âgés, une préoccupation principale doit être qu'elles les aident à maintenir leur autonomie et leur indépendance » (p. 7, traduction libre). Ils mettent en garde contre « le paternalisme bienveillant qui vise à 'protéger' les adultes plus âgés » car il « peut être perçu comme empiétant sur leur liberté ». Leur recommandation est claire : « Au lieu de concevoir ces technologies pour les adultes plus âgés, il devrait y avoir un changement vers la conception avec les adultes plus âgés » (p. 7, traduction libre). La lutte contre l'âgisme, qui est souvent à l'origine de ce paternalisme, représente donc une dimension importante. L'Institut national de santé publique du Québec (2023) recommande que « des politiques et mesures agissant directement sur l'âgisme doivent être promues auprès de partenaires de différents secteurs, comme le travail, l'enseignement, les médias et le réseau de la santé et des services sociaux » (p. 5). Cette approche est cohérente avec les observations de Havers et al. (2024) concernant la stigmatisation des victimes âgées de cybercriminalité, souvent attribuée à des attitudes âgistes.

Les mêmes auteurs identifient « un manque de compétences et des systèmes sociaux et institutionnels limités » comme « des défis pour les adultes plus âgés qui les empêchent d'acquérir des expériences et de se sentir à l'aise avec l'utilisation des technologies » (p. 7, traduction libre). Cette observation souligne l'importance d'adopter une approche holistique qui prend en compte non seulement les aspects techniques mais aussi les dimensions sociales et institutionnelles.

Lee et al. (2024) notent que « certaines études récentes stipulent la nécessité pour les adultes plus âgés d'apprendre sur l'intelligence artificielle (IA) et ses applications pour faciliter leurs tâches quotidiennes » (p. 693, traduction libre). Cette familiarisation avec l'IA pourrait être particulièrement pertinente pour reconnaître et se prémunir contre les hypertrucages.

Face aux risques de victimisation, McDonald et Mentis (2023) proposent une vision alternative : « les recherches futures devraient explorer des outils de cybersécurité qui se concentrent sur la prévention - sur le blocage des préjudices par des interventions techniques - comme le blocage des publicités, le signalement du pourriel et la limitation de son empreinte numérique - qui atténuent le besoin de formation à l'ingénierie sociale en premier lieu » (p. 17, traduction libre). Ils suggèrent que « les travaux futurs devraient explorer des façons de reconceptualiser les utilisateurs adultes plus âgés non pas comme des victimes, mais comme des agents capables de mieux censurer leurs vies » (p. 17, traduction libre).

Ces auteurs critiquent également certaines approches éducatives courantes, notamment celles des organisations comme l'AARP (American Association of Retired Persons) : « Nous soutenons que des publications comme celles de l'AARP mènent les adultes plus âgés dans la mauvaise direction en leur faisant mémoriser une série de règles et particulariser les menaces, plutôt que de les instruire sur l'importance du contexte » (p. 17, traduction libre).

L'importance de la santé cognitive et du bien-être global

Le renforcement de la cyberrésilience des personnes âgées s'inscrit dans une perspective plus large de promotion de la santé cognitive et du bien-être global. À ce titre, le maintien de liens sociaux forts constitue un facteur de protection essentiel, la littérature identifiant l'isolement comme un risque majeur de victimisation. De plus, l'Institut national de santé publique du Québec (2023) rappelle que « tout au long du parcours de vie, l'adoption d'un mode de vie physiquement actif peut contribuer à prévenir ou retarder l'apparition des troubles neurocognitifs majeurs, en plus d'avoir plusieurs autres bénéfices pour la santé » (p. 5).

Cette approche globale de la santé cognitive peut également contribuer à renforcer les capacités de détection de la tromperie. Comme l'ont souligné Ebner et al. (2023), les facteurs cognitifs jouent un rôle crucial dans la vulnérabilité des personnes âgées face aux fraudes sophistiquées. Le maintien des fonctions cognitives à travers l'activité physique, intellectuelle et sociale pourrait donc constituer une stratégie préventive efficace, bien qu'indirecte.

Vers une gouvernance multiacteurs de la désinformation

La complexité du phénomène des hypertrucages et de la désinformation exige une approche de gouvernance impliquant de multiples acteurs. Comme le souligne Cassar (2023), « les résultats indiquent que les gouvernements seuls n'apporteront pas le changement nécessaire. Le secteur privé, les ONG et les institutions académiques et de recherche auront également un rôle crucial à jouer dans l'obtention de la confiance des communautés et l'expression de leurs préoccupations, transformant la question en une responsabilité partagée » (p. 20, traduction libre).

Cette vision est partagée par Yao et Yang (2024), qui recommandent que « le gouvernement devrait intensifier ses programmes d'éducation et d'information des consommateurs pour les personnes âgées ». D'une part, « l'éducation des consommateurs pourrait permettre aux personnes âgées d'agir en tant que consommateurs discriminants, capables de faire un choix éclairé de biens et de services pour prévenir la fraude ciblée des consommateurs ». D'autre part, « de tels programmes enseignent également aux personnes âgées comment faire face aux réactions émotionnelles négatives qui suivent la fraude à la consommation, comment affirmer correctement les droits des consommateurs sans stéréotypes âgistes injustifiés, et conscients de leurs droits et responsabilités dans les activités de litige » (p. 15, traduction libre).

Les mêmes auteurs notent que « si la recherche révèle une forte prévalence d'escroqueries en ligne ciblant les adultes plus âgés, des programmes accrus d'éducation publique et de sensibilisation axées sur la littératie numérique pourraient être déployés de manière proactive » (p. 15, traduction libre). Cette recommandation illustre l'importance d'une approche fondée sur des données probantes pour orienter les politiques et les interventions.

Évaluation et adaptation continue des stratégies

Face à l'évolution rapide des technologies de deep-fake et des stratégies de désinformation, l'évaluation et l'adaptation continue des approches de prévention sont essentielles. Azam et al. (2024) soulignent que « à mesure que les cybermenaces évoluent, le matériel éducatif du modèle doit rester actuel pour protéger efficacement les personnes âgées contre les risques nouveaux et émergents » (p. 104, traduction libre).

Sádaba et al. (2023) suggèrent d'explorer « si les mesures d'éducation aux médias ont un effet comparativement plus positif chez les adultes plus âgés que chez la population plus jeune » (p. 8, traduction libre). Cette question de recherche pourrait orienter le développement d'interventions plus efficaces et adaptées aux besoins spécifiques des différents groupes d'âge.

Wang et al. (2025) concluent que leur étude « soutient l'applicabilité de la théorie de l'activité routinière du mode de vie dans l'étude de la victimisation par la criminalité en ligne » (p. 9, traduction libre). Cette approche théorique pourrait fournir un cadre utile pour comprendre et prévenir la victimisation des personnes âgées dans le contexte numérique.

Résultats de la recension des interventions terrain

Dans le cadre de ce rapport, une intervention ou une initiative désigne toute action éducative, informationnelle, de soutien ou de mobilisation visant à informer, éduquer ou outiller les personnes âgées face à la désinformation, la cyberfraude et l'utilisation non éthique de l'intelligence artificielle, notamment les hypertrucages (deepfakes). Ces actions ont pour objectif de renforcer la résilience et l'autonomie des personnes âgées dans l'environnement numérique.

Afin de recueillir les données, plusieurs échanges ont eu lieu par courriel, par téléphone, via LinkedIn ou par rencontre sur Microsoft Teams. De plus, plusieurs ressources ont été collectées via des sites web où les ressources en ligne sont accessibles et disponibles aux professionnels mais également au grand public. Il est à noter que les ressources partagées avec notre équipe par les organisations sont le plus souvent, et essentiellement au Québec, en lien d'une part avec la réduction de la fracture numérique en favorisant la littératie numérique dans son ensemble et en répondant à un besoin immédiat de sensibiliser et faire de la prévention à la désinformation et aux fraudes sans nécessairement aborder directement les hypertrucages.

Ainsi, afin de faciliter la lecture, plusieurs types d'interventions ont été identifiés, abordant des thématiques majeures et complémentaires. L'ensemble des initiatives classées se regroupent ainsi en trois catégories distinctes :

Les interventions directes

Les interventions directes représentent les initiatives qui abordent les hypertrucages (deepfakes) et qui ont été spécifiquement créées pour les personnes âgées.

Les interventions indirectes

Les interventions indirectes représentent les initiatives qui abordent les hypertrucages (deepfakes) et qui n'ont pas été directement créées pour les personnes âgées mais qui permettent de sensibiliser les acteurs du milieu communautaire, le grand public ou encore les communautés de chercheurs.

Les interventions sous-jacentes

Les interventions sous-jacentes regroupent les initiatives qui, de manière directe ou indirecte, traitent des hypertrucages (deepfakes), notamment à travers des thématiques plus larges telles que : la sensibilisation à l'intelligence artificielle et ses enjeux éthiques, la lutte contre la désinformation, les fausses nouvelles et leurs enjeux liés aux partages d'informations erronées, mensongères, tronquées ou manipulées, la prévention des fraudes et des cybermenaces ciblant par exemple les arnaques aux grands-parents ou encore les arnaques sentimentales, ainsi que la lutte contre la maltraitance des personnes âgées.

Les interventions directes à destination des personnes âgées

Les interventions directes représentent les initiatives qui abordent les hypertrucages (deepfakes) et qui ont été spécifiquement créées pour les personnes âgées.

Formations, ateliers, conférences et Webinaire

AI Frauds and Scams – Protecting Cyber Safety

Elder Abuse Prevention Ontario

Cible : Personnes âgées – Canada

Webinaire abordant les fraudes et les escroqueries utilisant l'IA, destinées aux personnes âgées (Elder Abuse Prevention Ontario, 2023).

Documents de prévention, guide

AI for Older Adults

Senior Planet de l'AARP

Cible : Personnes âgées – États-Unis

Guide explicatif de l'IA, de ses usages et des risques pour les personnes de plus de 50 ans (Senior Planet, 2024).

Guide How to Protect Seniors from AI Scams and Fraud

GPTzero

Cible : Professionnels et personnes âgées – États-Unis

Ce guide *Comment protéger les personnes âgées des escroqueries et des fraudes liées à l'IA* vise à partager des conseils pratiques pour protéger les personnes âgées contre les cyber-fraudes comme les hypertrucages et comment l'intelligence artificielle peut être utilisée comme mesure de protection pour protéger les personnes âgées contre la fraude (GPTzero, s. d.).

Guide : Risques associés à l'intelligence artificielle pour les seniors

Faculté pédagogique de l'Université Palacký d'Olomouc, CEDMO (Observatoire européen central des médias numériques) et Université Charles de Prague

Cible : Personnes âgées – République tchèque

Guide à destination des personnes âgées : *Risques associés à l'intelligence artificielle pour les seniors*, créé dans le cadre du projet [E-Safety](#) de la Faculté pédagogique de l'Université Palacký d'Olomouc, en collaboration avec le CEDMO et l'Université Charles de Prague et le soutien de Google intitulé (Kopecký et al., 2024).

Trousse de prévention de la fraude pour aînés

Association des banquiers canadiens (ABC) et Pensez Cybersécurité (gouvernement du Canada)

Cible : Personnes âgées – Canada

Trousse à destination des personnes âgées pour la protection contre la fraude et les escroqueries (Association des banquiers canadiens, 2025).

Plateforme en ligne, site web et blogue

Artificial Intelligence Scams

Missouri Department of Health and Senior Services

Cible : Personnes âgées – États-Unis

Explication de ce qu'est l'IA, quand la personne doit-elle s'alerter et comment se protéger (Missouri Department of Health and Senior Services, s. d.).

Deepfakes: nepvideo's van verontrustend hoge kwaliteit

SeniorWeb

Cible : Personnes âgées – Pays-Bas

Plateforme, formations, ressources, articles et conseils pratiques à destination des personnes âgées. Exemple de l'article : *Deepfakes : de fausses vidéos d'une qualité inquiétante* (Van Amstel, 2023).

Don't Fall Prey to Artificial Intelligence Scams: Tips for Recognizing and Guarding Against AI Scammers

Senior Service of America

Cible : Personnes âgées – États-Unis

Article présentant différentes stratégies et conseils pratiques sur les fraudes utilisant l'intelligence artificielle auprès des personnes âgées (Senior Service of America, s. d.).

<u>How to spot and avoid AI scams</u> <i>The Bank of Nova Scotia</i> <i>Cible : Personnes âgées – Canada</i>	L'article explique comment l'IA et le deepfake ont renforcé les escroqueries qui visaient déjà les personnes âgées et présente quelques conseils pratiques (The Bank of Nova Scotia, 2024).
<u>The Cybersecurity blog – How Hackers and Scammers Use AI (Artificial Intelligence)</u> <i>Cyber-Seniors</i> <i>Cible : Personnes âgées – Canada</i>	Plateforme en ligne, outils, ressources et formations en littératie numérique destinés aux personnes âgées abordant notamment la cybersécurité et les fraudes liées à l'intelligence artificielle (deepfake) à travers un onglet spécialement dédié à la <u>cybersécurité</u> (Cyber-Seniors, s. d.).
<u>Understanding Deepfakes: What Older Adults Need to Know</u> <i>National council on aging</i> <i>Cible : Personnes âgées – États-Unis</i>	Ressource explicative abordant les différents types de deepfakes, comment les identifier et comment les repérer dans une vidéo, une photo ou un extrait audio (National council on aging, 2024).

Les interventions indirectes à destination des personnes âgées

Les interventions indirectes représentent les initiatives qui abordent les hypertrucages (deepfakes) et qui n'ont pas été directement créées pour les personnes âgées mais pour sensibiliser les acteurs du milieu communautaire, le grand public ou encore les communautés de chercheurs.

Formations, ateliers, conférences et Webinaire

Fraude web : À un clic de la catastrophe

François Charron

Cible : Grand public – Québec, Canada

Conférence sur la prévention de la fraude et les vols d'identité, sur l'évolution des fraudes, les identifier et comment les combattre (Charron, s. d.).

Documents de prévention, guide

Conseils sur la cybersécurité pour les institutions démocratiques : intelligence artificielle

Centre canadien pour la Cybersécurité – gouvernement du Canada

Cible : Grand public – Canada

Document synthétique abordant la notion d'intelligence artificielle, ses enjeux, exemple de contenus faux, comment atténuer la menace de l'IA utilisée de façon non éthique (Centre canadien pour la cybersécurité, 2024).

Théâtre, film, jeu, vidéo

Super Fake Safari

Mediajungle

Cible : grand public – Pays-Bas

Conférences, formations, jeux de société, Mediajungle propose plusieurs outils, formations et ressources pour lutter contre la désinformation dont le jeu Super Fake Safari dont les fausses nouvelles, les deepfakes sont démystifiés. Le jeu a été créé pour les personnes ayant une légère déficience intellectuelle mais est également utilisé auprès des jeunes et des personnes âgées (Mediajungle, s. d.).

Campagne de sensibilisation

Pensez Cybersécurité

Centre canadien pour la cybersécurité, Centre de la sécurité des télécommunications Canada – Gouvernement du Canada la campagne nationale

Cible : grand public – Canada

Pensez Cybersécurité/Get CyberSafe a pour mission d'informer la population canadienne des enjeux liés à la cybersécurité et à leur indiquer des façons simples, des trucs et astuces et une multitude de ressources leur permettant de mieux se protéger en ligne (gouvernement du Canada, 2024).

Plateforme en ligne, site web et blogue

<u>AI-Powered Scams: How AI is Enhancing Existing Scams</u> Royal Bank <i>Cible : grand public – Canada</i>	La Banque Royale du Canada met en garde contre les fraudes améliorées avec l'usage de l'intelligence artificielle. L'institution financière expose une liste de conseils pour aider à mieux se protéger contre les fraudes évoluées de l'IA (Royal Bank of Canada, s. d.).
<u>AI-Powered Scams: What You Need to Know to Help Safeguard Your Aging Loved Ones</u> True Link <i>Cible : Grand public – États-Unis</i>	L'article s'adresse aux proches des personnes âgées (True Link, 2024). Explication des méthodes de fraude les plus fréquentes : « Voice cloning », « AI phishing attacks » et « Deepfake videos ». Aussi, plusieurs ressources pour protéger les personnes plus vulnérables à ces fraudes.
<u>Artificial Intelligence (AI) and Investment Fraud</u> Canadian Investment Regulatory Organization <i>Cible : Grand public – Canada</i>	Article qui explique comment l'Intelligence et artificielle peut être un danger de sécurité et quels sont les types fréquents de fraude. L'un des points se concentre sur les deepfake (Canadian Investment Regulatory Organization, s. d.).
<u>Détecter l'hypertrucage</u> Gouvernement du Québec – Québec, Canada	Ressources en ligne abordant la notion d'hypertrucage et comment les reconnaître (gouvernement du Québec, 2024).
<u>La montée de l'IA : la fraude à l'ère numérique</u> Bureau de la concurrence Canada – gouvernement du Canada <i>Cible : Grand public – Canada</i>	Communiqué du Bureau de la concurrence Canada qui explique les principaux signaux d'une fraude créée par l'IA (Bureau de la concurrence Canada, 2024).
<u>L'hypertrucage (deepfake)</u> Prévention de la fraude – Autorité des marchés financiers <i>Cible : Grand public – Canada</i>	Ressources en ligne abordant la notion d'hypertrucage (deepfake) et comment reconnaître une fraude par hypertrucage (Autorité des marchés financiers, s. d.).
<u>Scammers use AI to enhance their family emergency schemes</u> Federal Trade Commission : Consumer advice <i>Cible : Grand public – États-Unis</i>	Article informatif sur les escroqueries utilisant l'intelligence artificielle. Ressources et brochures disponibles sur les différents types d'escroqueries.

Les interventions sous-jacentes

Les interventions sous-jacentes regroupent les initiatives qui, de manière directe ou indirecte, traitent des hypertrucages (deepfakes), notamment à travers des thématiques plus larges telles que : la sensibilisation à l'intelligence artificielle et ses enjeux éthiques, la lutte contre la désinformation, les fausses nouvelles et leurs enjeux liés aux partages d'informations erronées, mensongères, tronquées ou manipulées, la prévention des fraudes et des cybermenaces ciblant par exemple les arnaques aux grands-parents ou encore les arnaques sentimentales. Ainsi que la lutte contre la maltraitance des personnes âgées.

Formations, ateliers, conférences et Webinaire

<u>Ateliers Fadoq.ca – Activités sociales et éducatives</u> <i>Ateliers FADOQ – FADOQ Région des Laurentides</i> <i>Cible : Personnes âgées – Québec, Canada</i>	Formation abordant la notion de cybersécurité, ses enjeux et les bonnes pratiques à adopter (Fadoq, s. d.).
<u>Formations – Sécurité et le comportement en ligne</u> <i>Insertech</i> <i>Cible : Personnes âgées – Québec, Canada</i>	Atelier de discussion abordant la notion de sécurité et comportement en ligne, navigation sécuritaire et bien protéger son appareil informatique, comment mieux se protéger et développer de bons réflexes (Insertech, s. d.).
<u>PING! est une offre de formation qui vise à améliorer les compétences en informatique et numériques des Québécois et des Québécoises</u> <i>Programme Ping – Communautique</i> <i>Cible : Grand public – Québec, Canada</i>	Module de formation, <i>Recherches sur le Web et sources fiables d'information</i> , abordant comment utiliser son navigateur de façon sécuritaire, comprendre l'interface d'un site web et identifier les sources fiables (Ping, s.d.)
<u>Prévention contre la fraude</u> <i>La Sûreté du Québec</i> <i>Cible : Grand public – Québec, Canada</i>	Prévention contre la fraude, capsule vidéo éducative <u>5 conseils pour prévenir la fraude téléphonique</u> et ateliers dans les bibliothèques, les organismes et les résidences pour personnes âgées (Sûreté du Québec, 2024). Atelier de sensibilisation <i>Décrypter la fraude</i> , partager des stratégies liées à la fraude, identifier des comportements à risque et sécuritaires, informer des différents types de fraudes (également en lien avec l'intelligence artificielle), signaler une fraude et porter plainte. Atelier de sensibilisation <i>Prévenir la fraude, ça débute avec vous!</i> , actualité sur les fraudes, comment se protéger et comment la signaler. Trois fraudes sont abordées (fraude grands-parents, faux conseiller/représentant et fraude amoureuse). <i>Cible : Personne âgée</i> (Sûreté du Québec, s. d.).
<u>Protecting Older Adults from Scams</u> <i>South Carolina Department of Consumer Affairs</i> <i>Cible : Personnes âgées – États-Unis</i>	Webinaire et document de présentation abordant des conseils pratiques à destination des personnes âgées, proposés dans le cadre de la semaine nationale de la protection des consommateurs en mars 2024 (South Carolina Department of Consumer Affairs, 2024).
<u>Réseau Poivre et sel</u> <i>Regroupement de collaborateurs et de partenaires actifs dans la Haute-St-Charles et la MRC de la Jacques Cartier</i> <i>Cible : Personnes âgées – Québec, Canada</i>	Issu du projet intergénérationnel <i>Le Net me branche</i> , le Réseau propose un module de formation sur la sécurité numérique abordant les différentes fraudes, comment s'y préparer et les détecter, quoi faire si vous êtes victime de fraude (Réseau Poivre et Sel, s. d.).

Plateforme en ligne, site web et blog

Alphanumérique

Bibliopresto et partenaires

Cible : Grand public – Québec, Canada

Plateforme d'apprentissage en ligne (littératie numérique) et ressources gratuites pour le grand public et les professionnels. Plusieurs formations disponibles dont : [Introduction aux fausses nouvelles et à leur caractère viral](#) abordant les différentes formes de désinformation, pourquoi partage-t-on de fausses nouvelles ou encore quel est le rôle des médias (Alpha numérique, s. d.) ou encore [les fausses nouvelles : trucs et astuces pour éviter de les partager](#) formation abordant la notion de validité d'une information, comment nos préjugés influencent-ils notre manière de s'informer ou encore comment vérifier l'information (Alpha numérique, s. d.).

Centre de sécurité, centre d'information – BMO

Banque de Montréal (BMO)

Cible : grand public – Canada

Ressource en ligne abordant la cybersécurité, les fraudes, ses enjeux, actualités et outils pour la combattre (BMO, s. d.).

Centre de soutien des aînés – Banque CIBC

Banque CIBC

Cible : Personnes âgées – Canada

Opérations et avantages bancaires pour les personnes âgées, ressources en ligne sur les fraudes (CIBC, s. d.).

Clinique de Cyber-Criminologie

Chaire de recherche en prévention de la cybercriminalité

Cible grand public – Québec, Canada

Plateforme en ligne de ressources sur la fraude et la cyber-fraude, accompagnement, plateforme de partage, signalement de fraude sous forme de forum ([fraudealerte.ca](#)) (Clinique de cybercriminologie, s. d.).

Comment combattre la désinformation – Robot conversationnel

Les Décrypteurs –Radio-Canada

Cible : grand public – Québec, Canada

Articles de blog, émissions, ressources et agent conversationnel abordant plusieurs thématiques en lien avec la désinformation afin de sensibiliser et outiller les citoyens contre les fausses nouvelles (Décrypteurs, s. d.).

Espace aîné – Insertech

Insertech

Cible : Personnes âgées– Québec, Canada

Plateforme d'apprentissage en ligne (littératie numérique), ateliers thématiques de discussions, accompagnement et ressources gratuites pour les personnes âgées (Insertech, s. d.).

Odil, la plateforme francophone des initiatives de lutte contre la désinformation

Odil

Cible : Grand public – France et pays francophones

Dans le cadre du projet « [Lutte contre les désordres de l'information](#) », la plateforme Odil a été créée et propose des outils et ressources, des listes d'initiatives de lutte contre la désinformation dans la Francophonie, et une cartographie des mesures de politiques publiques pour lutter contre la désinformation. (Odil, s. d.).

Options aînés

Option consommateur

Cible : Personnes âgées – Québec

Conférences sur les vols d'identités et la fraude, la gestion financière, ressources en ligne et ligne téléphonique de soutien (Option consommateurs, s. d.). Exemple : [Guide Vos finances en toute sécurité](#); [Gestion des finances et maltraitance financière \(Fascicule à l'intention des aînés isolés\)](#); [Gestion des finances et maltraitance financière \(Fascicule à l'intention des personnes proches aidantes\)](#)

Personnes âgées : petit guide pour vous y retrouver

Éducaloi

Cible : Personnes âgées – Québec, Canada

Dossier comportant des ressources en ligne diverses dont contre les fraudes et abus financiers envers les personnes âgées (Éducaloi, s. d.).

<u>Préoccupations concernant la mésinformation en ligne, 2023</u> Statistique Canada (20/12/2023) – gouvernement du Canada Cible : Grand public – Canada	Communiqué abordant les préoccupations en lien avec la mésinformation selon l'influence de l'âge, les revenus ou encore la santé mentale (Statistiques Canada, 2023).
<u>Prévenir et reconnaître la maltraitance et la fraude</u> JuridiQC – gouvernement du Québec – Québec, Canada	Ressource en ligne de prévention contre la fraude et la maltraitance des personnes âgées (JuridiQC, s. d.).
<u>Prévenir la fraude financière envers les aînés</u> Prévention de la fraude – Autorité des marchés financiers Cible : Personnes âgées – Canada	Ressources en ligne de prévention contre les fraudes, les différents types de fraudes, comment se protéger (L'autorité des marchés financiers, s. d.).
<u>Protéger nos clients de 60 ans et plus</u> Banque Nationale Cible : Personnes âgées – Canada	Ressources en ligne de prévention contre les fraudes, l'exploitation et les abus financiers (Banque Nationale, s. d.).
<u>Reconnaître et prévenir l'exploitation financière</u> Caisse Desjardins Cible : Personnes âgées – Québec, Canada	Ressource en ligne et capsules vidéo sur les fraudes, les abus financiers et les arnaques (Desjardins, s. d.).
<u>Votre argent aînés</u> Association des banquiers canadiens Cible : Personnes âgées – Canada	Programme de littératie financière, ressources en ligne, séminaires, de prévention contre les fraudes, arnaque des grands-parents, les abus financiers (Canadian Bankers Association, s. d.).
<u>What is Misinformation and Disinformation?</u> Toronto Public Library Cible : Grand public – Canada	Ressource en ligne sur la désinformation, la mésinformation et les fausses informations qui se présentent sous diverses formes comme les deepfakes. (Toronto Public Library, s.d.).
Documents de prévention, guide	
<u>Intelligence artificielle</u> Centre canadien pour la Cybersécurité – gouvernement du Canada Cible : Grand public – Canada	Document synthétique abordant la notion d'intelligence artificielle et de ses enjeux (Centre canadien pour la cybersécurité, 2023).
<u>La Fraude en 3D</u> La Sûreté du Québec en collaboration avec la Banque du Canada, l'Autorité des marchés financiers et plusieurs autres partenaires du Forum de la prévention de la fraude, co-présidé par le Centre antifraude du Canada (CAFC), la Gendarmerie royale du Canada et le Bureau de la concurrence Cible : Grand public – Canada	Rapport abordant les différents types de fraudes, ses enjeux et comment s'en protéger (Banque du Canada et Sûreté du Québec, 2024).
<u>L'intelligence artificielle générative</u> Centre canadien pour la Cybersécurité – gouvernement du Canada Cible : Grand public – Canada	Document synthétique abordant la notion d'intelligence artificielle générative, ses enjeux, comment est-elle utilisée et quelles sont les risques (Centre canadien pour la cybersécurité, 2023).

<u>Plateforme d'accompagnement dans le vieillissement actif – Zone AVA</u> <i>Initiative du Cégep de Drummondville, Centre collégial d'expertise en gérontologie</i> <i>Cible : Personnes âgées – Québec, Canada</i>	La plateforme Zone AVA – Accompagner dans un Vieillessement Actif a été développée pour et avec les personnes âgées, afin de mieux répondre à leurs besoins, à leurs aspirations et à leurs intérêts diversifiés en matière de vieillissement actif (Zone AVA, s. d.).
<u>Trousse de cybersécurité</u> <i>Association des banquiers canadiens (ABC) et Pensez Cybersécurité (gouvernement du Canada)</i> <i>Cible : Grand public – Canada</i>	Trousse à destination du grand public de sensibilisation à la cybersécurité (Association des banquiers canadiens, s. d.).
Projets et programmes	
<u>AlphabéTICaction – Projets 50 ans et plus</u> <i>La puce, ressource informatique</i> <i>Cible : Personnes âgées – Québec, Canada</i>	Projet d'initiation à la littératie numérique pour les 50 ans et plus. Plusieurs formations sont disponibles comme les essentiels de la cybersécurité abordant la notion d'arnaque, de navigation sécuritaire, protéger son appareil informatique, créer des mots de passe robustes mais également la notion de cybersécurité, ses enjeux et les bonnes pratiques à adopter (La puce, s. d.).
<u>BOSS (Be Online and Stay Safe)</u> <i>Leeds Older People's Forum</i> <i>Cible : Personnes âgées – Angleterre</i>	Plusieurs outils et ressources disponibles afin de développer les compétences en éducation aux médias et pour protéger de la désinformation des personnes âgées (Leeds Older People's Forum, 2022). Exemple, capsules vidéo sur l'utilisation de ChatGPT et A guide to supporting older people to keep safe online through building digital media literacy skills.
<u>Programmes et services pour les aînés</u> <i>Gouvernement du Québec</i> <i>Cible : Personnes âgées – Québec, Canada</i>	Guide destiné aux personnes âgées, répertoriant les ressources, les programmes et services gouvernementaux qui leur sont destinés (gouvernement du Québec, 2024).
<u>Programme Québec ami des aînés</u> <i>Secrétariat aux aînés – ministère de la Santé et des Services sociaux – gouvernement du Québec</i> <i>f- Québec, Canada</i>	Le programme encourage la participation des personnes âgées au développement social, économique et culturel de leur communauté à travers le financement de projets réalisés par des organismes (gouvernement du Québec, 2024).
<u>The poynter Institute : MediaWise for Seniors</u> <i>MediaWise for Senior – The Poynter Institute</i> <i>Cible : Personnes âgées – États-Unis</i>	Ce programme propose une plateforme et des cours en ligne visant à améliorer l'éducation aux médias des personnes âgées et d'apprendre à vérifier les faits et à lutter contre les fausses nouvelles et la désinformation (The Poynter Institute, 2024).
Avant 2023	
<u>Nouveau système de signalement des incidents de cybercriminalité et de fraude</u> <i>Centre national de coordination en cybercriminalité – Gendarmerie royale du Canada – Centre antifraude du Canada – gouvernement du Canada – Canada</i>	Mise en place d'un système de signalement, afin de faciliter le processus de signalement des cybercrimes et des fraudes pour les particuliers et les entreprises au pays (Gendarmerie royale du Canada, 2022).

Campagne de sensibilisation	
<u>Campagne « N’hésitez pas, raccrochez ! »</u> <i>Prévention Suisse de la Criminalité</i> <i>Cible : Grand public – Suisse</i>	Campagne de sensibilisation, ressources et conseils pratiques sur les escroqueries par téléphone utilisant ou non l’IA pour des « appels chocs ». (Prévention Suisse de la Criminalité, s. d.).
<u>European Cybersecurity Month</u> <i>European Union Agency for Cybersecurity</i> <i>Cible : Grand public – Europe</i>	Campagne de sensibilisation organisée pour promouvoir la cybersécurité auprès des citoyens de l’Union européenne et des organisations (European Union Agency for Cybersecurity, s. d.).
<u>Journée internationale des personnes âgées</u> <i>Nations Unies</i> <i>Cible : Grand public</i>	La Journée internationale des personnes âgées, le 1 ^{er} octobre, met en avant les droits, le bien-être et la contribution des personnes âgées dans la société. Elle sensibilise aussi aux défis liés au vieillissement global (Nations Unies, s. d.-a).
<u>Journée mondiale de sensibilisation à la maltraitance des personnes âgées</u> <i>Nations Unies</i> <i>Cible : Grand public</i>	La Journée mondiale de sensibilisation à la maltraitance des personnes âgées, le 15 juin, vise à dénoncer les abus subis par les personnes âgées et encourage la protection des droits et de la dignité des personnes âgées à travers le monde (Nations Unies, s. d.-b).
<u>Journées des partenaires pour contrer la maltraitance envers les personnes âgées</u> <i>Ministère de la Santé et des Services sociaux – gouvernement du Québec – Québec, Canada</i>	Plan d’action gouvernemental pour contrer la maltraitance envers les personnes âgées (ministère de la Santé et des Services sociaux, 2023).
<u>Le Mois de la prévention de la fraude</u> <i>La Sûreté du Québec en collaboration avec la Banque du Canada, l’Autorité des marchés financiers et plusieurs autres partenaires du Forum de la prévention de la fraude, co-présidé par le Centre antifraude du Canada (CAFC), la Gendarmerie royale du Canada et le Bureau de la concurrence</i> <i>Cible : Grand public – Québec, Canada</i>	Le Mois de la prévention de la fraude est une campagne de sensibilisation offerte au Grand public afin de le sensibiliser et le maintenir informé de l’actualité en lien avec la fraude. Ce peut-être sous forme de plusieurs interventions comme des conférences, des publicités ou encore des ateliers (Sûreté du Québec, s. d.).
Théâtre, film, jeu, vidéo	
<u>Parlez-moi d’amour</u> <i>La FADOQ de Montréal en collaboration avec la SPVM, Info-Crime Montréal et le Secrétariat aux aînés (Direction régionale de la santé publique)</i> <i>Cible : Personnes âgées – Québec, Canada</i>	Ce projet a été réalisé dans le cadre de la Journée mondiale de lutte contre la maltraitance envers les personnes âgées. Cette pièce de théâtre documentaire a été créée et présentée à près de 250 personnes âgées de l’île de Montréal. Cette pièce de théâtre d’impact est une œuvre originale, écrite à partir de témoignages réels de personnes âgées et d’intervenants ayant vécu ou vu des situations d’exploitation financière par des proches ou des situations de fraudes amoureuses, suivi d’une discussion avec un agent sociocommunautaire du SPVM et autres collaborateurs (Théâtre Déchaînés, 2024).



Discussion

Discussion

Cette recension des connaissances et des interventions terrain révèle un décalage préoccupant : alors que la littérature scientifique documente abondamment la vulnérabilité des personnes âgées face aux hypertrucages, les interventions spécifiquement conçues pour les outiller contre ces technologies demeurent exceptionnellement rares. Notre analyse des initiatives existantes confirme que la majorité d'entre elles traitent de la fraude au sens large, laissant la menace spécifique des hypertrucages dans un angle mort. Cette invisibilité soulève des questions fondamentales : s'agit-il d'un simple retard de la prise de conscience collective face à une technologie émergente, ou d'une difficulté structurelle des intervenants, qui se forment souvent de manière autonome, à aborder des sujets d'une telle complexité technique ? Les hypertrucages, démocratisés seulement depuis 2022, représentent effectivement un phénomène relativement nouveau. Ou bien la complexité technique de ces technologies constitue-t-elle un obstacle insurmontable pour les différents acteurs qui, comme le révèle notre enquête, se forment principalement de manière autonome et ne possèdent pas nécessairement d'expertise technique approfondie ? Cette réalité du terrain pourrait expliquer une certaine réticence à aborder des concepts technologiques perçus comme inaccessibles.

Les limites structurelles des approches actuelles

L'analyse approfondie des interventions met en lumière des limites qui dépassent la simple méconnaissance technologique. La fragmentation des initiatives constitue un premier obstacle majeur. Chaque secteur – bancaire, communautaire, gouvernemental, policier – développe ses propres outils sans coordination apparente. Certes, il existe des exemples de collaboration réussie, comme le document « La Fraude en 3D », fruit d'un partenariat entre la Sûreté du Québec, la Banque du Canada, l'Autorité des marchés financiers et plusieurs autres partenaires du Forum de la prévention de la fraude, co-présidé par le Centre antifraude du Canada (CAFC), la Gendarmerie royale du Canada et le Bureau de la concurrence. Ce document est largement utilisé et partagé par différents acteurs, et les services de police locaux s'appuient principalement sur le matériel produit par la Sûreté du Québec. Cependant, ces exemples de coordination demeurent l'exception plutôt que la règle. Pour la majorité des acteurs, les formations et ateliers proposés restent distincts les uns des autres et n'utilisent pas systématiquement les outils développés par la police, le gouvernement ou d'autres institutions.

Cette recension des connaissances et des interventions terrain révèle un décalage préoccupant : alors que la littérature scientifique documente abondamment la vulnérabilité des personnes âgées face aux hypertrucages, les interventions spécifiquement conçues pour les outiller contre ces technologies demeurent exceptionnellement rares.

Cette situation entraîne une duplication des efforts et une dilution des messages. Cette cacophonie institutionnelle devient source de confusion pour les personnes âgées qui doivent naviguer entre de multiples sources d'information parfois contradictoires.

L'inadéquation entre les besoins spécifiques des personnes âgées et les réponses génériques offertes constitue une deuxième limite importante. Alors que la littérature scientifique identifie clairement les facteurs de vulnérabilité propres à cette population – déclin des fonctions exécutives, respect de l'autorité, isolement social – la plupart des interventions adoptent une approche universelle. Les formations actuelles répondent principalement aux besoins immédiats selon une logique réactive « problématique = solution », sans développer les compétences d'analyse critique nécessaires face aux manipulations sophistiquées des hypertrucages.

Les barrières à l'accessibilité représentent un troisième défi majeur. Notre recension elle-même s'est heurtée à des obstacles révélateurs : le terme « deepfake » ne se traduit pas dans toutes les langues, créant un biais systématique vers les ressources anglophones. Les moteurs de recherche privilégient les résultats régionaux, limitant l'accès aux initiatives internationales. Ces barrières méthodologiques reflètent celles auxquelles font face quotidiennement les personnes âgées dans leur recherche d'information et de protection.

L'absence d'une terminologie francophone établie aggrave ces difficultés. Alors qu'aux États-Unis, les termes « AI Scam » ou « AI phishing scams » sont entrés dans le vocabulaire courant, aucun équivalent francophone n'a émergé au Québec. Cette lacune linguistique n'est pas anodine : elle reflète et perpétue le retard dans la prise de conscience collective de cette menace, rendant difficile toute communication efficace sur le sujet.

Pour surmonter cette fragmentation, il est essentiel de définir clairement le rôle et la contribution de chaque acteur. Une approche écosystémique requiert une action coordonnée où chaque partie prenante assume ses responsabilités.

Définir la contribution des parties prenantes : une réponse à la fragmentation

La construction d'un environnement propice à la cyber-résilience des personnes âgées face aux hypertrucages nécessite l'implication coordonnée de multiples parties prenantes. Cette section examine les rôles et contributions spécifiques que peuvent apporter différents acteurs, des individus aux organisations, en passant par les instances gouvernementales.

Rôle des créateurs d'outils et plateformes numériques

Les concepteurs et développeurs d'outils d'intelligence artificielle portent une responsabilité particulière dans la prévention des risques liés aux hypertrucages. Comme le souligne Makhortykh (2024), « les apprenants utilisent de plus en plus l'IA générative pour compléter des devoirs et trouver des informations, ce qui signifie que les entreprises et les individus concevant ces systèmes doivent adopter le même type de processus décisionnel concernant le contenu, la formation de récits et la fiabilité que les historiens et éducateurs de l'Holocauste » (p. 6, traduction libre). L'auteur insiste sur le fait que « le rôle de ceux qui développent et déploient des systèmes et outils d'IA doit être central dans les considérations sur la façon de gouverner la technologie au service de la préservation historique et de la vérité » (p. 6, traduction libre).

Les contenus générés par l'IA, particulièrement les hypertrucages audio et visuels, sont particulièrement préoccupants pour leurs représentations émotionnellement évocatrices et potentiellement trompeuses. Makhortykh (2024) note que « l'IA pourrait être utilisée pour modifier ou générer des images, des sons ou des vidéos, pour faire apparaître des figures historiques ou des survivants disant ou faisant des choses qu'ils n'ont pas faites » (p. 10, traduction libre). Face à ces risques, « il est essentiel d'introduire des garde-fous, limitant l'abus potentiel de l'IA pour générer de fausses preuves [...], ou mettre en évidence pour les utilisateurs que les preuves sont générées par l'IA » (p. 10, traduction libre).

Horstmann et al. (2023) rappellent que les concepteurs de technologies destinées aux personnes âgées devraient « donner la priorité aux mesures de protection de la vie privée dès le début, plutôt que de considérer la vie privée comme un complément fastidieux qui ne fait qu'inhiber la collecte de données et la fonctionnalité » (p. 6, traduction libre). Cette approche de « privacy by design » est particulièrement importante dans le contexte des technologies capables de générer des hypertrucages.

Rôle de la famille et des proches

Le cercle familial et les proches constituent un levier fondamental pour renforcer la cyber-résilience des personnes âgées. Le Service canadien du renseignement de sécurité (2023) note qu'« une personne est plus facilement convaincue et corrigée par quelqu'un qu'elle connaît. Par conséquent, il faut amener les normes et le discours sociétaux sur les hypertrucages à changer pour instaurer un climat dans lequel les gens sont non seulement sceptiques face à ce qu'ils voient, mais sont encouragés à remettre en question les informations provenant de leurs pairs » (p. 32).

Xu et al. (2024) soulignent que « l'encouragement et le soutien des membres de la famille, des pairs et des organisations communautaires peuvent être une grande motivation pour les adultes plus âgés dans leur parcours de littératie numérique » (p. 693, traduction libre). Ils précisent que « lorsque les adultes plus âgés reçoivent de l'assistance et du soutien technique de leurs proches et des membres de la communauté, cela leur inculque un sentiment de confiance et de motivation pour explorer et apprendre de nouvelles compétences numériques » (p. 693, traduction libre).

Des recherches antérieures suggèrent que « les systèmes de soutien social tels que la famille et les amis, des espaces d'apprentissage sûrs qui sont aussi libres que possible des stéréotypes liés à l'âge et au genre, et la mise en évidence des avantages de pouvoir comprendre et utiliser la technologie peuvent aider à atténuer la réticence des adultes plus âgés concernant l'utilisation des (nouvelles) technologies » (Horstmann et al., 2023, p. 7, traduction libre).

L'Institut national de santé publique du Québec (2023) confirme que « les proches, les amis et les groupes de pairs sont une source importante d'encouragement pour s'initier aux technologies numériques, et leur soutien peut s'avérer un déterminant majeur de leur utilisation » (p. 17). Cette observation souligne l'importance des relations sociales dans le développement de la littératie numérique des personnes âgées.

Cependant, Sullivan et Kosuth (2024) mettent en garde contre une dépendance excessive à ce soutien familial : « Considérant l'omniprésence des cybercriminels ciblant les adultes plus âgés, compter sur la famille, les amis ou eux-mêmes pour acquérir les connaissances et les outils nécessaires à la protection est au mieux une stratégie fragile » (p. 30, traduction libre). Cette observation suggère la nécessité de compléter le soutien familial par des approches plus structurées et institutionnalisées.

Stratégies pratiques à mettre en place au niveau individuel et familial

Napal (2024) propose plusieurs stratégies concrètes pour les personnes âgées et leurs proches face aux risques de fraude par hypertrucages :

- « Prendre du recul et réfléchir avant d'agir – envisager d'essayer d'appeler votre proche sur son numéro de contact connu, ou appeler un autre membre de la famille ou un ami proche pour leur faire savoir ce qui s'est passé et demander leur soutien.
- Signaler toute arnaque à votre prestataire de services financiers et à votre membre du Congrès – cela peut aider à sensibiliser sur la question, et à traiter les arnaques qui ont particulièrement ciblé votre communauté locale.
- Établir un 'mot de code' ou une phrase secrète avec votre famille proche, vos amis ou votre communauté – un clone vocal IA pourrait être capable d'imiter votre être cher, mais pourrait ne pas connaître quelque chose de spécifique à votre vie ou aux relations que vous avez. Vous pourriez établir une question secrète, une phrase ou un mot, comme connaître la bonne réponse à 'dans quelle rue ai-je grandi' ou un mot spécifique que vous pouvez leur demander s'ils sont vraiment en danger » (p. 187, traduction libre).

Ces stratégies pragmatiques constituent des moyens simples mais efficaces de contrer les tentatives de fraude utilisant des hypertrucages, en s'appuyant sur des connaissances partagées qui ne peuvent être facilement reproduites par l'intelligence artificielle.

Rôle des organismes communautaires et œuvres de bienfaisance

Les organismes communautaires et les œuvres de bienfaisance jouent un rôle crucial dans le renforcement de la cyberrésilience des personnes âgées. Havers et al. (2024) notent que « plusieurs parties prenantes professionnelles ont mentionné l'importance de tiers neutres et dignes de confiance, tels que les travailleurs d'œuvres de bienfaisance ou les 'défenseurs' des soins de santé et sociaux (c'est-à-dire des individus séparés du FJN ou des autorités), qui peuvent guider et soutenir les victimes tout au long du processus de signalement » (p. 8, traduction libre).

McDonald et Mentis (2023) observent que « CSCW (Computer-Supported Cooperative Work) s'intéresse de plus en plus aux études sur la vie privée et la sécurité parmi les populations âgées qui sont perçues comme ayant des besoins uniques en matière de vie privée. Nicholson et al. constatent que les adultes plus âgés ont tendance à privilégier les ressources sociales et accessibles plutôt que les ressources expertes et sont plus enclins à prêter attention aux sources médiatiques non Internet » (p. 5, traduction libre). Ils ajoutent que « Kropczynski et al. ont découvert que les adultes plus âgés ont tendance à graviter vers ceux de leur communauté ayant une expertise similaire » (p. 5, traduction libre).

L'Institut national de santé publique du Québec (2023) souligne qu'« il peut s'avérer bénéfique de proposer des ateliers de groupe dans la communauté pour diminuer la sédentarité chez les personnes de 50 ans et plus » (p. 9). L'Institut ajoute que « les personnes présentant un cumul de facteurs de risques associés aux troubles neurocognitifs majeurs, comme l'isolement social et une faible scolarisation, pourraient tirer le plus grand bénéfice de tels ateliers » (p. 9).

L'Institut décrit également le rôle de différents acteurs communautaires : « Les centres d'action bénévole et différents organismes communautaires des secteurs sportifs et de loisirs peuvent apporter une contribution positive pour les composantes touchantes, par exemple, la programmation d'activités, le transport et l'accompagnement vers les lieux d'intérêt » (p. 9). Cette approche multisectorielle illustre l'importance d'une coordination entre différents acteurs pour créer un environnement favorable au bien-être global des personnes âgées, y compris leur cyberrésilience.

Rôle des municipalités et des institutions publiques

Les municipalités et autres institutions publiques ont un rôle important à jouer dans la création d'un environnement propice à la cyberrésilience des personnes âgées. L'Institut national de santé publique du Québec (2023) note que « les municipalités peuvent jouer un rôle clé pour accroître l'accessibilité et diminuer les inégalités dans l'utilisation des environnements bâtis » (p. 9). Il ajoute que « les établissements scolaires et d'enseignement peuvent aussi constituer des partenaires de choix pour établir des ententes de partage des installations sportives, et offrir des opportunités d'activités intergénérationnelles » (p. 9).

L'institut propose plusieurs mesures concrètes pour favoriser l'inclusion numérique des personnes âgées, notamment au palier national :

- « Impliquer des personnes âgées dans l'identification des besoins et le développement des ressources numériques qui leur sont dédiées.
- Sensibiliser les concepteurs des sites Internet et des outils technologiques à l'adoption de principes de conception inclusive centrés sur les utilisateurs.
- Prévoir des adaptations technologiques pour les personnes présentant des limitations physiques (p. ex. vision altérée ou difficultés de motricité fine) et des besoins linguistiques particuliers.
- Utiliser un langage simple pour rejoindre les personnes présentant un faible niveau de littératie ou d'alphabétisation.
- Lors de la transmission d'informations ou le déploiement d'interventions, proposer une gamme d'alternatives de qualité équivalente pour tenir compte des inégalités numériques et des préférences de communication (p. ex. en ligne, en présence, par téléphone, par la poste).
- Évaluer les programmes actuels du gouvernement visant à rendre accessible l'Internet haute vitesse afin d'en vérifier les retombées en matière d'accès chez les personnes âgées.
- Inciter les organisations aux paliers régionaux et locaux à investir dans la littératie numérique, notamment par l'intermédiaire d'une offre de services en ligne accessibles à tous, de la formation et de l'évaluation des résultats » (p. 18).

Aux paliers régionaux et locaux, l'institut recommande de :

- « Offrir des opportunités d'apprentissage et d'entraide permettant de développer la littératie numérique et les autres formes de littératie qui permettraient aux usagers de profiter pleinement des outils et des services gouvernementaux (p. ex. formation en milieu de travail et à travers des organismes communautaires, mise en place de réseaux d'apprentissage et d'entraide dans les bibliothèques).
- Développer la capacité des intervenants aux divers paliers de services à diriger les usagers vers des sources crédibles d'information » (p. 18).

Rôle des citoyens et campagnes de sensibilisation

La responsabilité face aux hypertrucages et à la désinformation ne repose pas uniquement sur les institutions, mais également sur les citoyens eux-mêmes. Le Service canadien du renseignement de sécurité (2023) souligne que « la population doit également renforcer sa connaissance des productions synthétiques et sa sensibilité à ces dernières, et il faut l'encourager à éviter de relayer des informations non fiables » (p. 43). Cette observation met en lumière l'importance de la responsabilité individuelle dans la lutte contre la propagation de la désinformation.

Les campagnes de sensibilisation constituent un moyen efficace de renforcer cette responsabilité citoyenne. Logie et Das (2024) notent que « les banques et les institutions financières ont pris l'initiative d'éduquer leurs clients et leurs consommateurs sur ces risques pour les consommateurs; cependant, il peut être nécessaire de mener des campagnes de sensibilisation communautaires sur le terrain pour souligner la nature sérieusement criminelle de ces catégories de fraude » (p. 26, traduction libre).

Cassar (2023) suggère, « conformément au plan d'action de l'UE, en particulier les Actions 7-9 qui impliquent le renforcement de la sensibilisation et de la résilience sociétales [que] le gouvernement est également encouragé à mettre en place une institution/entité dans le but de promouvoir la sensibilisation à la situation actuelle concernant la désinformation et de soutenir les médias indépendants et le journalisme de qualité » (p. 21, traduction libre).

Le Service canadien du renseignement de sécurité (2023) insiste sur le fait qu'« afin de lutter contre ce fléau, il est primordial de mieux sensibiliser la population à la fraude psychologique faisant appel aux hypertrucages, d'élaborer des protocoles efficaces de détection et d'intervention, et de favoriser la coopération entre corps policiers » (p. 60).

Potentiel de l'IA dans la protection des personnes âgées

Si l'intelligence artificielle est à l'origine de la création des hypertrucages, elle peut également contribuer à protéger les personnes âgées contre les fraudes qu'ils engendrent. Segal (2024) note qu'« une étude menée par Kumar et al. (2018) a cherché à étudier la faisabilité d'utiliser des techniques d'apprentissage et d'apprentissage automatique pour améliorer l'identification des activités frauduleuses ciblant les clients âgés au sein d'un établissement financier » (p. 529, traduction libre). L'auteur ajoute que « grâce à la personnalisation et à l'adaptation logique aux besoins spécifiques des adultes plus âgés, l'intelligence artificielle est prometteuse pour les protéger contre le fait de devenir victimes de fraude à la consommation » (p. 529, traduction libre).

Segal (2024) suggère également que « le site web ChatGPT peut s'avérer approprié pour ceux qui trouvent du réconfort à chercher des conseils et de l'aide auprès d'une source anonyme pour traiter de la fraude à la consommation » (p. 530, traduction libre). Cette observation souligne le potentiel des agents conversationnels comme ressource accessible pour les personnes âgées confrontées à des situations de fraude potentielle.

Cassar (2023) reconnaît que « malgré les preuves toujours plus nombreuses des préjudices causés par l'IA, il faut également la reconnaître pour les nombreuses fois où elle a aidé l'humanité à conquérir des tâches exigeantes et à repousser continuellement les frontières du possible, entre autres choses. La criminalistique d'image et la détection d'anomalies sont deux grands cas des capacités bénéfiques de l'IA, qui sont toutes deux des dérivés de la reconnaissance de motifs qui aident grandement à identifier les anomalies dans les textes, images et éventuellement vidéos fabriqués » (p. 19, traduction libre).

Adaptation des interfaces et développement de la pensée critique

L'adaptation des interfaces aux besoins spécifiques des personnes âgées constitue une approche complémentaire pour renforcer leur cyberrésilience. Lee et al. (2024) observent que « bien que la structure de navigation hiérarchique soit communément favorisée par les générations plus jeunes pour son efficacité, elle pourrait poser des défis pour les adultes plus âgés. L'adoption d'une structure de navigation linéaire peut améliorer l'utilité perçue et l'intention d'utiliser à long terme » (p. 10, traduction libre). Ils précisent que « notre étude démontre que même si la structure de navigation linéaire nécessite plus d'étapes pour naviguer dans les pages, elle peut simplifier le processus de navigation, permettant aux adultes plus âgés de suivre un chemin direct, réduisant ainsi le temps nécessaire pour naviguer et améliorant leur acceptation de la technologie » (p. 10, traduction libre).

Le développement de la pensée critique apparaît comme un élément essentiel de la lutte contre la désinformation. L'Académie de la transformation numérique (2024) rapporte que « 60 % des internautes estiment que le moyen le plus efficace de lutter contre les conséquences de la désinformation serait de modérer les fausses nouvelles, soit directement via les plateformes qui les diffusent (34 %), soit par l'instauration de lois (26 %) » (p. 17). Cependant, « seulement 20 % des internautes au Québec ont choisi comme moyen le plus efficace pour lutter contre les conséquences des fausses nouvelles le fait de développer la pensée critique du public, soit via de la sensibilisation dans les écoles (13 %), ou via des campagnes destinées au grand public (7 %) » (p. 17).

Ces résultats suggèrent un écart entre les approches privilégiées par les usagers (modération et régulation) et celles souvent recommandées par les experts (développement de la pensée critique). Cette observation souligne l'importance d'une approche équilibrée combinant différentes stratégies complémentaires.

Exemple d'approche gouvernementale intégrée

Cassar (2023) présente l'exemple du gouvernement maltais qui « avait déjà fondé la Malta Digital Innovation Authority (MDIA), qui encourage les développements technologiques dans plusieurs secteurs et surveille constamment ces arrangements » (p. 21, traduction libre). L'auteur suggère que cette autorité pourrait étendre son mandat pour fournir un soutien aux citoyens à travers plusieurs initiatives :

« (i) lancer une campagne anti-fake news visant à renforcer l'éducation aux médias du public à travers des formats audio et visuels sur plusieurs plateformes.

(ii) Publier une liste classée des médias en ligne maltais et étrangers selon le degré de légitimité et de véracité du contenu publié.

(iii) Formuler et rédiger un cadre, destiné aux éditeurs/entreprises de contenu en ligne, pour fournir des orientations sur la façon dont les informations devraient être présentées en ligne.

(iv) Développer une approche de modération basée sur l'IA avec la mise en œuvre de boucles de rétroaction provenant de la foule composée d'individus sélectionnés pour aider l'approche IA à établir une base de référence sur la véracité ou la fausseté du contenu en question » (p. 21, traduction libre).

Cette approche illustre une vision intégrée combinant sensibilisation, transparence, orientation et utilisation de l'IA comme outil de lutte contre la désinformation. Elle souligne l'importance d'une coordination entre différents leviers d'action pour créer un environnement médiatique plus fiable et transparent.

Synthèse des rôles des différentes parties prenantes

La cyberrésilience des personnes âgées face aux hypertrucages nécessite l'implication coordonnée de multiples parties prenantes, chacune apportant une contribution spécifique :

- **Créateurs d'outils et plateformes numériques** : Intégrer des garde-fous éthiques dès la conception, développer des mécanismes de détection des hypertrucages, signaler clairement les contenus générés par IA.
- **Famille et proches** : Offrir un soutien technique, encourager l'apprentissage numérique, établir des stratégies de vérification (mots de code, questions secrètes) pour prévenir les fraudes.
- **Organismes communautaires** : Proposer des ateliers de groupe, servir d'intermédiaires de confiance pour guider les victimes, créer des réseaux d'entraide entre pairs.
- **Municipalités et institutions publiques** : Adapter les services numériques aux besoins des personnes âgées, impliquer les personnes âgées dans la conception des services, offrir des alternatives non numériques équivalentes.
- **Citoyens** : Développer une conscience critique face aux médias, éviter de relayer des informations non vérifiées, participer aux réseaux d'entraide intergénérationnels.
- **Gouvernements** : Élaborer des cadres réglementaires, soutenir les campagnes de sensibilisation, coordonner les initiatives des différentes parties prenantes.

Cette approche écosystémique reconnaît que la cyberrésilience ne peut reposer uniquement sur la responsabilité individuelle des personnes âgées, mais nécessite un effort collectif impliquant l'ensemble de la société.

Cette recension des connaissances et des interventions terrain révèle un décalage préoccupant entre l'ampleur de la menace que représentent les hypertrucages pour les personnes âgées et les réponses actuellement déployées. Alors que la littérature scientifique documente abondamment la vulnérabilité spécifique de cette population face aux manipulations audiovisuelles sophistiquées, les interventions directement conçues pour les outiller contre ces technologies demeurent exceptionnellement rares.

Notre analyse révèle que seulement une poignée d'initiatives abordent directement la problématique des hypertrucages auprès des personnes âgées. La majorité des interventions recensées s'inscrivent dans des approches plus larges de littératie numérique, de prévention de la fraude ou de lutte contre la désinformation, sans nécessairement traiter des spécificités techniques et psychologiques des hypertrucages. Les données terrain confirment ce constat alarmant : au Québec, les organisations interrogées sensibilisent activement les personnes âgées aux fraudes traditionnelles - hameçonnage, rançongiciel, arnaque des grands-parents, fraude amoureuse - mais la notion d'hypertrucage généré par intelligence artificielle demeure largement absente de leurs interventions. Lorsque le sujet est effleuré, c'est généralement en réponse à une question spécifique d'un participant plutôt que dans le cadre d'une approche structurée.

Synthèse des stratégies pratiques par palier d'intervention

Au palier individuel et familial : L'objectif est de donner des outils simples et efficaces pour une vérification immédiate.

- Mettre en place des stratégies de vérification personnelle. Prendre du recul avant d'agir, tenter de joindre le proche concerné par un autre moyen de communication connu, ou contacter un autre membre de la famille pour valider l'information.
- Signaler systématiquement les tentatives de fraude. Informer les institutions financières et les autorités compétentes aide à la prise de conscience collective et au traitement des menaces.
- Adopter un « mot de code » familial. Cette stratégie intergénérationnelle, simple et efficace, consiste à établir un mot ou une phrase secrète qu'une IA ne peut connaître, permettant de vérifier l'identité d'un proche lors d'un appel suspect.

Au palier communautaire (organismes, associations) : Le but est de s'appuyer sur les réseaux de confiance existants.

- Offrir des ateliers de groupe interactifs dans des espaces communautaires connus et sécurisants.
- Positionner les intervenants communautaires comme des « tiers de confiance » neutres pouvant guider et soutenir les victimes dans leurs démarches de signalement.
- Miser sur l'expertise des pairs, car les personnes âgées ont tendance à faire confiance aux personnes de leur communauté ayant une expérience similaire.

Au palier institutionnel (municipalités et gouvernements) : Il s'agit de créer un environnement inclusif et de structurer l'offre de services.

- Impliquer les personnes âgées dans l'identification des besoins et le développement des ressources numériques qui leur sont destinées.
- Utiliser un langage simple et proposer des alternatives de qualité non numériques (téléphone, en personne, poste) pour tenir compte des inégalités.
- Offrir des opportunités d'apprentissage concrètes et mettre en place des réseaux d'entraide, par exemple dans les bibliothèques.
- Soutenir et financer les campagnes de sensibilisation nationales et les initiatives communautaires.

Au palier technologique (créateurs d'outils et plateformes) : La responsabilité est de concevoir des outils qui protègent en amont.

- Intégrer la « protection de la vie privée dès la conception » (privacy by design) comme un principe fondamental.
- Mettre en place des « garde-fous » techniques, comme le signalement automatique des contenus générés par IA ou la limitation des abus potentiels.



La tension fondamentale entre protection et autonomisation

au-delà de ces limites opérationnelles, notre analyse révèle une tension profonde entre deux visions de l'intervention. D'un côté, une approche protectrice cherche à mettre les personnes âgées à l'abri des dangers numériques, souvent au prix d'un certain paternalisme qui risque de renforcer les stéréotypes âgistes. De l'autre, une approche capacitante vise à développer leur autonomie, mais peut sous-estimer les défis réels auxquels ils font face et les laisser vulnérables.

Les initiatives les plus prometteuses sont celles qui parviennent à naviguer dans cette tension avec nuance. L'exemple de l'agent conversationnel développé par un participant de CyberCap, et qui est actuellement en phase exploratoire, illustre cette voie médiane : en offrant un soutien technologique accessible tout en préservant l'autonomie et la confidentialité, cet outil permet aux personnes âgées d'obtenir des réponses sans stigmatisation. De même, les projets intergénérationnels comme Générations@branchées démontrent comment les échanges entre jeunes, sensibilisés aux hypertrucages, et personnes âgées riches d'expérience créent des dynamiques d'apprentissage mutuellement enrichissantes. Le programme de jumelage intergénérationnel en informatique Générations@branchées est proposé par les bibliothèques publiques du Québec. Ce programme permet aux adultes désirant s'initier à l'informatique ou obtenir de l'aide de se tourner vers leur bibliothèque publique. Celle-ci organise ainsi un jumelage avec un adolescent bénévole possédant des compétences en informatique et favorisant ainsi l'entraide et le partage de connaissances entre générations.

L'émergence de pratiques porteuses d'espoir

malgré ce tableau préoccupant, notre recension identifie des pratiques prometteuses qui méritent d'être amplifiées. Les approches d'inoculation psychologique, particulièrement lorsqu'elles sont gamifiées, montrent un potentiel remarquable pour développer une résilience cognitive. En exposant progressivement les participants à des versions affaiblies de techniques de manipulation, ces méthodes permettent de développer des « anticorps » cognitifs contre les hypertrucages.

Les stratégies pragmatiques développées sur le terrain révèlent également une créativité encourageante. Certaines résidences pour personnes âgées ont mis en place des systèmes de mémos et d'infolettres pour maintenir leurs résidents informés des nouvelles formes de fraude. Les bibliothèques publiques, la FADOQ et les tables de concertation exploitent leur ancrage local pour diffuser l'information dans des environnements familiers et rassurants, comme le propose le programme Aîné-Avisé qui vise à sensibiliser les personnes âgées et le grand public à la maltraitance et à la fraude envers les personnes âgées. L'initiative Espace Aînés d'Insertech, financée par le Programme Québec ami des aînés (QADA), démontre également comment les programmes gouvernementaux peuvent catalyser des réponses communautaires adaptées.

Les enjeux éthiques et sociétaux sous-jacents

notre analyse soulève des questions éthiques fondamentales qui dépassent les considérations pratiques. La responsabilité de protéger les personnes âgées contre les hypertrucages malveillants ne peut reposer sur un seul acteur. Notre recension révèle une multiplicité d'intervenants – gouvernements à tous les niveaux, services de police, institutions financières, organismes communautaires, bibliothèques – agissant de manière fragmentée. Cette diversité témoigne d'une certaine mobilisation, mais souligne cruellement l'absence d'une coordination efficace et d'une vision partagée.

Les inégalités dans l'accès aux ressources de protection soulèvent des questions d'équité troublantes. Les initiatives se concentrent dans les centres urbains et dépendent souvent de financements ponctuels, laissant les personnes âgées en région éloignée ou à faible revenu dans une vulnérabilité accrue. Cette situation crée un cercle vicieux où les plus vulnérables ont le moins accès aux moyens de protection.

Le dilemme de la complexité technologique cristallise ces enjeux : comment transmettre des concepts sophistiqués à travers des intervenants qui se forment de manière autonome et à des personnes âgées aux compétences numériques variables ? La réponse ne peut être uniquement technique. Elle doit s'ancrer dans une approche écosystémique qui reconnaît la cyberrésilience non comme une compétence individuelle, mais comme le produit d'un environnement favorable combinant technologies adaptées, réseaux de soutien actifs et politiques publiques appropriées.



Conclusion

Conclusion

Ce livre blanc a entrepris d'examiner un défi émergent et complexe : comment renforcer la cyberrésilience des personnes âgées face à la menace croissante des hypertrucages. À travers une revue systématique de la littérature scientifique et une recension des interventions terrain, nous avons mis en lumière un paradoxe troublant : alors que les personnes âgées constituent une population particulièrement vulnérable aux manipulations par hypertrucages, les interventions spécifiquement conçues pour les protéger demeurent dramatiquement insuffisantes.



Principaux constats

Notre analyse a permis de dégager trois constats principaux :



Un décalage critique existe entre la menace et la réponse.

Alors que les personnes âgées sont une cible documentée et particulièrement vulnérable aux hypertrucages, les interventions spécifiquement conçues pour les outiller contre cette menace



La vulnérabilité des personnes âgées est multidimensionnelle.

Elle ne se limite pas à la fracture numérique, mais résulte d'une convergence de facteurs cognitifs (baisse des fonctions exécutives), sociaux (isolement, confiance envers l'autorité) et émotionnels que les fraudeurs exploitent activement.



Les efforts actuels sont freinés par des limites structurelles.

La lutte contre les hypertrucages est handicapée par la fragmentation des initiatives entre les différents acteurs, l'absence d'une terminologie francophone commune, des approches souvent trop génériques et des barrières d'accessibilité importantes.



Recommandations

Les résultats de cette étude appellent à une mobilisation urgente et coordonnée de l'ensemble des acteurs sociaux. Fondées sur les implications pratiques de notre analyse, les recommandations qui suivent visent à orienter cette mobilisation pour chaque grand groupe d'acteurs.

✓ Pour les décideurs politiques

Il est essentiel de mettre en place un cadre d'action clair pour encadrer la création et la diffusion des hypertrucages. Une approche qui combine prévention, détection et réponse, offre un modèle intéressant à adapter et à renforcer. Pour ce faire, il est recommandé de :

- Développer un cadre réglementaire spécifique aux hypertrucages qui protège les populations vulnérables sans entraver l'innovation légitime.
- Investir dans des programmes nationaux d'éducation aux médias synthétiques adaptés aux personnes âgées.
- Soutenir la recherche sur des outils de détection d'hypertrucages qui soient accessibles, fiables et conviviaux pour le grand public.
- Intégrer rapidement la notion d'hypertrucage et les risques liés à l'utilisation non éthique de l'IA dans tous les documents officiels et campagnes de sensibilisation à la fraude et à la cybersécurité.

✓ Pour les organismes communautaires

Les interventions communautaires, par leur proximité et leur lien de confiance, jouent un rôle crucial. Il est essentiel que ces acteurs valorisent la participation active des personnes âgées comme agents de changement pour éviter les approches paternalistes. Il est recommandé de :

- Intégrer la sensibilisation aux hypertrucages dans les programmes existants de littératie numérique et de prévention.
- Développer des approches d'apprentissage par les pairs qui valorisent l'expérience des personnes âgées et des initiatives intergénérationnelles, qui sont des vecteurs de résilience collective particulièrement efficaces.
- Créer des espaces sécuritaires pour l'expérimentation et l'apprentissage, où les personnes âgées peuvent poser des questions et manipuler les technologies sans jugement.
- Exploiter les événements récurrents comme le Mois de la prévention de la fraude pour introduire et normaliser la discussion sur ces nouvelles menaces.

✓ Pour les institutions financières et technologiques

La conception technologique doit passer d'une logique de protection paternaliste à une logique d'autonomisation. Il est impératif d'impliquer les personnes âgées dans le processus de développement pour créer des outils qui respectent leur autonomie et répondent à leurs besoins. Il est recommandé de :

- Adopter des principes de conception inclusive et de protection de la vie privée dès le départ (*privacy by design*).
- Concevoir des systèmes de vérification d'identité et des interfaces qui soient simples, clairs et adaptés aux capacités et préférences des personnes âgées.
- Investir dans le développement d'outils de détection automatique intégrés aux plateformes pour alerter les personnes utilisatrices face à un contenu potentiellement manipulé.
- Collaborer pour développer une terminologie francophone claire et accessible pour communiquer efficacement sur ces enjeux

✓ Pour les chercheurs et éducateurs

La recherche doit continuer à éclairer les interventions pour garantir leur pertinence et leur efficacité face à des menaces en constante évolution. Il est recommandé de :

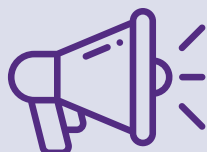
- Développer et évaluer rigoureusement des interventions éducatives basées sur des données probantes, en explorant notamment l'efficacité des approches innovantes comme l'inoculation psychologique et la ludification.
- Documenter et diffuser les meilleures pratiques émergentes
- Créer des ponts entre la recherche académique et les besoins terrain des intervenants



Vision pour l'avenir

L'objectif ultime transcende la simple protection contre une technologie malveillante. Il s'agit de construire une société numérique véritablement inclusive où les personnes âgées peuvent naviguer avec confiance et autonomie. Cette vision exige un changement de paradigme : abandonner les approches paternalistes pour embrasser une philosophie capacitante qui reconnaît les personnes âgées comme des actrices à part entière de leur sécurité numérique.

La cyberrésilience ne peut être le fruit d'interventions isolées ou de solutions purement technologiques. Elle nécessite une transformation sociétale profonde qui valorise l'expérience des personnes âgées, combat l'âgisme et garantit l'équité d'accès aux ressources de protection. Les solutions doivent s'ancrer dans les réalités locales, mobiliser les structures communautaires existantes et respecter la diversité des parcours de vie.



Appel à l'action

Le temps de l'action est venu. Chaque jour d'inaction expose davantage des personnes âgées aux manipulations sophistiquées, aux pertes financières dévastatrices et à la détresse psychologique profonde. Les coûts humains et sociaux de notre retard collectif dépassent largement les investissements nécessaires pour développer des stratégies de prévention efficaces.

Ce livre blanc lance un appel pressant à tous les acteurs de la société. Les pistes d'action sont identifiées, les acteurs sont mobilisables, les structures existent. Il ne manque qu'une volonté collective et une coordination efficace pour transformer cette vision en réalité. La protection de nos personnes âgées face aux hypertrucages n'est pas qu'un défi technique : c'est un test de notre humanité collective, de notre capacité à construire une société qui n'abandonne personne face aux bouleversements technologiques. En protégeant nos personnes âgées contre les hypertrucages, nous défendons bien plus que leur sécurité financière. Nous préservons la confiance sociale, les liens intergénérationnels et la dignité humaine qui constituent le socle de notre vivre-ensemble.

Bibliographie

Académie de la transformation numérique. (2024a). Portrait des générations. *NETendances*. <https://transformation-numerique.ulaval.ca/enquetes-et-mesures/netendances/portrait-numerique-des-generations-2023/>

Académie de la transformation numérique. (2024b). Portrait des personnes âgées connectées au Québec (2023). *NETendances* 14(8). <https://transformation-numerique.ulaval.ca/enquetes-et-mesures/netendances/portrait-des-personnes-aines-connectees-au-quebec-2023/>

Académie de la transformation numérique. (2025). Intelligence artificielle générative et données personnelles. *NETendances* 8(5). <https://transformation-numerique.ulaval.ca/enquetes-et-mesures/netendances/intelligence-artificielle-generative-et-donnees-personnelles-2024/>

Alphanumérique. (s. d.). *Développez vos compétences pour mieux naviguer dans la société numérique d'aujourd'hui!* <https://alphanumerique.ca/espace-public/>

Association des banquiers canadiens. (2025). *Trousse de prévention de la fraude pour aînés*. <https://cba.ca/article/trousse-pour-adultes-plus-ages>

Association des banquiers canadiens. (s. d.). *Trousse de cybersécurité*. <https://cba.ca/article/trousse-pour-particuliers>

Anthropic. (2025). *Claude Opus 4* [Grand modèle de langage]. <https://www.anthropic.com>

Augenbaum, S. E. (2024). Keeping Seniors Safe from Cyber Scams. *Geriatric Nursing*, 60, 711–712. <https://doi-org.acces.bibl.ulaval.ca/10.1016/j.gerinurse.2024.10.081>

Aung, K. W., Soubutts, E. et Singh, A. (2024). « What a stupid way to do business » : Towards an Understanding of Older Adults' Perceptions of Deceptive Patterns and Ways to Develop Resistance. *Proceedings of the ACM on Human-Computer Interaction*, 8(CHI PLAY), 1–31. <https://doi.org/10.1145/3677113>

Autorité des marchés financiers. (s. d.). *L'hypertrucage (deepfake)*. https://lautorite.qc.ca/grandpublic/types-de-fraude/lhypertrucage-deepfake?oft_d=638576754009600000&oft_id=1048051&oft_k=FVNhjt0&oft_lk=FtjQE7&cHash=3528194c78939cfeb0427082f6fbb2c4

Azam, N. A., Buja, A. G., Ahmad, R., Abdul Latip, S. F. et Sahri, N. M. (2024). An Analysis of the Deployment of Synergistic Cyber Security Awareness Model for the Elderly (SCSAM-Elderly) in Malaysia. *Akademika*, 94(3), 90–107. <https://ejournal.ukm.my/akademika/article/view/71148/16325>

Banque du Canada et Sûreté du Québec. (2024, mars). *La fraude en 3D*. <https://www.banqueducanada.ca/wp-content/uploads/2020/02/fraude-3d.pdf>

Banque Nationale. (s. d.). *Protéger nos clients de 60 ans et plus*. <https://www.bnc.ca/a-propos-de-nous/esg/protection-aines.html#fraude>

BMO. (s. d.). *Centre d'information*. <https://www.bmo.com/fr-ca/principal/particuliers/centre-de-securite/centre-de-formation/>

Bureau de la concurrence Canada. (2024, 4 mars). *La montée de l'IA : la fraude à l'ère numérique*. <https://www.canada.ca/fr/bureau-concurrence/nouvelles/2024/03/la-montee-de-lia-la-fraude-a-lere-numerique.html>

Élections Canada. (2024). *Protéger le processus électoral contre les menaces : principales recommandations*. <https://www.elections.ca/content.aspx?section=res&dir=rep/oth/prthr&document=index&lang=f>

Canadian Bankers Association. (s. d.). *Votre-Argent-Aînés*. <https://cba.ca/?tag=Votre-Argent-Aines>

Canadian Investment Regulatory Organization. (s. d.). *Artificial intelligence (AI) and investment fraud*. <https://www.ciro.ca/office-investor/avoiding-fraud-and-protecting-your-investments/artificial-intelligence-ai-and-investment-fraud>

- Cassar, D. (2023). The Misinformation Threat: A Techno-Governance Approach for Curbing the Fake News of Tomorrow. *Digital Government: Research and Practice*, 4(4), 1-28. <https://doi.org/10.1145/3631615>
- Centre canadien pour la cybersécurité. (2023, 14 juillet). *L'intelligence artificielle générative* (publication no ITSAP.00.041). <https://www.cyber.gc.ca/fr/orientation/lintelligence-artificielle-generative-itsap00041>
- Centre canadien pour la cybersécurité. (2023, 15 septembre). *Intelligence artificielle*. (publication no ITSAP.00.040.) <https://www.cyber.gc.ca/fr/orientation/intelligence-artificielle-itsap00040>
- Centre canadien pour la cybersécurité. (2024, mai). *Repérer les cas de désinformation*, *désinformation et malinformation* (publication no ITSAP.00.300). <https://www.cyber.gc.ca/fr/orientation/reperer-les-cas-de-mesinformation-desinformation-et-malinformation-itsap00300>
- Centre canadien pour la cybersécurité. (2024, 25 juin). *Conseils sur la cybersécurité pour les institutions démocratiques : intelligence artificielle* (publication no ITSAP.00.135). <https://www.cyber.gc.ca/fr/orientation/conseils-cybersecurite-institutions-democratiques-intelligence-artificielle-itsap00135>
- Charron, F. (s. d.). *Fraude web : à un clic de la catastrophe!* <https://www.fraudeweb.com/conference-fraude-web>
- Chen, Z., Wen, J., Gou, C., Wang, S. et Shao, J. (2024). Death anxiety and older adults' vulnerability to fraud: The mediating role of materialism. *Journal of Elder Abuse & Neglect*, 36(3), 291-309. <https://doi.org/10.1080/08946566.2024.2350995>
- Chen, Z., Wen, J., Li, Y., Zhang, X., Lv, C. et Shao, J. (2025). The Inevitability of Death : Mental Simulation Moderates the Effect of Death Anxiety on Older Adults' Vulnerability to Fraud. *Journal of Applied Gerontology*, 44(3), 463-472. <https://doi-org.acces.bibl.ulaval.ca/10.1177/07334648241273441>
- Chin, J., Desai, S., Lin, S. et Mejia, S. (2024). Like My Aunt Dorothy: Effects of Conversational Styles on Perceptions, Acceptance and Metaphorical Descriptions of Voice Assistants during Later Adulthood. *Proceedings of the ACM on Human-Computer Interaction*, 8(CSCW1), 1-21. <https://doi.org/10.1145/3637365>
- Chun, R. W. Y., Huang, S., Goh, D. H. L., Lee, C. S. et Theng, Y. (2024). Can Seniors Spot Deepfakes? A Diary Study of Deepfake Identification Strategies. *Proceedings of the Association for Information Science & Technology*, 61(1), 877-879. <https://doi-org.acces.bibl.ulaval.ca/10.1002/pra2.1126>
- CIBC. (s. d.). *Centre de soutien des aînés*. <https://www.cibc.com/fr/journeys/senior-support-centre.html#scams>
- Clinique de cyber-criminologie. (s. d.). *Fraude Alerte*. <https://www.fraude-alerte.ca/>
- Cyber-Seniors. (s. d.). *How Hackers and Scammers Use AI (Artificial Intelligence)*. <https://cyberseniors.org/uncategorized/how-hackers-and-scammers-use-ai-artificial-intelligence/>
- Décodeurs. (s. d.). Comment combattre la désinformation. *Radio-Canada*. <https://ici.radio-canada.ca/info/decodeurs/robot-conversationnel-combattre-desinformation/#top>
- DeLiema, M. (2024). Safeguarding Retirement in the Age of Scams. *TIAA Institute Research Paper Series Forthcoming*. <https://www.tiaa.org/public/institute/publication/2025/safeguarding-retirement-in-the-age-of-scams>
- Deng, Y., He, C., Zou, Y. et Li, B. (2025). « Auntie, Please Don't Fall for Those Smooth Talkers » : How Chinese Younger Family Members Safeguard Seniors from Online Fraud. *Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems*, 1-17. <https://doi.org/10.48550/arXiv.2501.10803>
- Desjardins. (s. d.). *Reconnaître et prévenir l'exploitation financière*. <https://www.desjardins.com/particuliers/projets-evenements/retraite/je-profite/exploitation-financiere/index.jsp>
- Diel, A., Lalg, T., Schröter, I. C., MacDorman, K. F., Teufel, M. et Bäuerle, A. (2024). Human performance in detecting deepfakes: A systematic review and meta-analysis of 56 papers. *Computers in Human Behavior Reports*, 16, article 100538. <https://doi.org/10.1016/j.chbr.2024.100538>

- Ebner, N. C., Pehlivanoglu, D. et Shoenfelt, A. (2023). Financial Fraud and Deception in Aging. *Advances in geriatric medicine and research*, 5(3), article e230007. <https://doi.org/10.20900/agmr20230007>
- Éducaloi. (s. d.). *Personnes âgées : petit guide pour vous y retrouver*. <https://educaloi.qc.ca/dossier/aines/#sujet-8>
- Elder Abuse Prevention Ontario. (2023, 21 novembre). *AI Fraud and Scams: Protecting Cyber Safety* [vidéo]. YouTube. [AI Fraud and Scams: Protecting Cyber Safety](https://www.youtube.com/watch?v=AI_Fraud_and_Scams_Protecting_Cyber_Safety)
- Espinoza, M. (2024). *The Grandparent Scam : A Systems Perspective Case Study On Elder Fraud And The Concept Of Human Layering*. <https://doi.org/10.48550/arXiv.2405.11789>
- European Union Agency for Cybersecurity. (s. d.). *European Cybersecurity Month*. <https://www.enisa.europa.eu/topics/awareness-and-cyber-hygiene/european-cybersecurity-month?tab=publications#contentList>
- FADOQ. (s. d.). *Ateliers Fadoq.ca*. https://www.fadoq.ca/laurentides/activites/activites-socio-educatives/ateliersfadoq_gl=1%2A2jwwtc%2A_up%2AMQ..%2A_ga%2AMTc5MTUzNDY1NS4xNzIxOTQxODE0%2A_ga_0FBTHRXRSE%2AMTcyMTk0MTgxMy4xLjAuMTcyMTk0MTgxMy4wLjAuMA..%2A_ga_2CXJQ0L9N6%2AMTcyMTk0MTgxMy4xLjAuMTcyMTk0MTgxMy4wLjAuMA_
- Fatima, M., Noah, N. et Das, S. (2024). Exploring Older Adults' Perceptions and Experiences with Online Dating. *IEEE BuildSEC'24 Building a Secure & Empowered Cyberspace*. <https://doi.org/10.48550/arXiv.2410.19783>
- Ferguson, L., Kürüm, E., Rodriguez, T. M., Nguyen, A., Lopes de Queiroz, I. F., Lee, J. et Wu, R. (2024). Impact of community-based technology training with low-income older adults. *Aging & Mental Health*, 28(4), 638-645. <https://doi.org/10.1080/13607863.2023.2256271>
- Frau-Meigs, D. (2024). *L'autonomisation des utilisateurs grâce aux réponses apportées par l'éducation aux médias et à l'information à l'évolution de l'intelligence artificielle générative (IAG)*. UNESCO. https://unesdoc.unesco.org/ark:/48223/pf0000388547_fre
- Gendarmerie royale du Canada. (2022, 20 octobre). *Nouveau système de signalement des incidents de cybercriminalité et de fraude*. <https://www.rcmp-grc.gc.ca/fr/nouveau-systeme-signalement-des-incidents-cybercriminalite-et-fraude>
- Gouvernement du Canada. (2024, 1 novembre). *Pensez Cybersécurité*. <https://www.pensezcybersecurite.gc.ca/fr>
- Gouvernement du Québec. (2024, 12 juin). *Programme Québec ami des aînés*. <https://www.quebec.ca/famille-et-soutien-aux-personnes/personnes-agees/aide-financiere-organismes/quebec-ami-des-aines/programme-quebec-ami-des-aines>
- Gouvernement du Québec. (2024, 22 août). *Détecter l'hypertrucage*. <https://www.quebec.ca/securite-situations-urgence/cybersecurite/conseils-cybersecurite/hypertrucage>
- Gouvernement du Québec. (2024, 30 mai). *Programmes et services pour les aînés*. <https://www.quebec.ca/famille-et-soutien-aux-personnes/personnes-agees/services-programmes-pour-les-aines>
- GPTzero. (s. d.). *How to Protect Seniors from AI Scams and Fraud*. <https://gptzero.me/guides/protecting-seniors-ai-guide>
- Hameleers, M. (2024). Cheap Versus Deep Manipulation: The Effects of Cheapfakes Versus Deepfakes in a Political Setting. *International Journal of Public Opinion Research*, 36 (1), 1-9. <https://doi.org/10.1093/ijpor/edae004>
- Hameleers, M., Van der Meer, T. et Dobber, T. (2025). How Far Can Political Deepfakes Credibly Deviate From Reality? Responses to Political Deepfakes With Varying Degrees of Deception. *International Journal Of Communication*, 19, 180-198. <https://ijoc.org/index.php/ijoc/article/view/22704>
- Havers, B., Tripathi, K., Burton, A., Martin, W., Cooper, C. et Collins, T. (2024). Exploring the Factors Preventing Older Adults From Reporting Cybercrime and Seeking Help : A Qualitative, Semistructured Interview Study. *Health & Social Care in the Community*, 2024, 1-10. <https://doi-org.acces.bibl.ulaval.ca/10.1155/2024/1314265>

- Havers, B., Tripathi, K., Burton, A., McManus, S. et Cooper, C. (2024). Cybercrime victimisation among older adults : A probability sample survey in England and Wales. *PLOS ONE*, 19(12), 1-10. <https://doi-org.acces.bibl.ulaval.ca/10.1371/journal.pone.0314380>
- Heemskerk, A., Lin, T., Pehlivanoglu, D., Hakim, Z., Valdes-Hernandez, P. A., Brinke, L. ten, Grilli, M. D., Wilson, R. C., Turner, G. R., Spreng, R. N. et Ebner, N. C. (2024). Interoceptive Accuracy Enhances Deception Detection in Older Adults. *Journals of Gerontology Series B: Psychological Sciences & Social Sciences*, 79(11), 1-8. <https://doi-org.acces.bibl.ulaval.ca/10.1093/geronb/gbae151>
- Herrera, L., Van Sickle, L. et Podhradsky, A. (2024) Bridging the Protection Gap: Innovative Approaches to Shield Older Adults from AI-Enhanced Scams. *Awareness and Research Symposium (CARS)*, 1-9. https://www.researchgate.net/publication/387047237_Bridging_the_Protection_Gap_Innovative_Approaches_to_Shield_Older_Adults_from_AI-Enhanced_Scams
- Horstmann, A. C., Schubert, T., Lambrich, L. et Strathmann, C. (2023). Alexa, I Do Not Want to Be Patronized. *Proceedings of the 23rd ACM International Conference on Intelligent Virtual Agents*, 1-10. <https://doi.org/10.1145/3570945.3607342>
- Ifop.(2024). *Les Français et les jeunes face aux deepfake*. <https://www.ifop.com/wp-content/uploads/2024/03/120667-presentation.pdf>
- Insertech. (s. d.). *Formations*. <https://insertech.ca/formations/>
- Insertech. (s. d.). *Espace Aînés*. <https://aines.insertech.ca/>
- Institut national de santé publique du Québec. (2023). *Doter le Québec d'une stratégie nationale pour améliorer la qualité de vie des personnes âgées : vers des milieux de vie inclusifs, sains et sécuritaires*. <https://www.inspq.qc.ca/publications/3322>
- Juridique. (s. d.). *Aînés en perte d'autonomie : Prévenir et reconnaître la maltraitance et la fraude*. <https://juridique.gouv.qc.ca/aines-en-perte-dautonomie/maltraitance-et-fraude/prevenir-et-reconnaitre-la-maltraitance-et-la-fraude>
- Kopecký, K., Szołkowski, R. et Kubala, L. (2024). *Rizika spojená s umělou inteligencí pro seniory*. <https://asociace.ai/wp-content/uploads/2024/07/rizika-umele-intelligence-pro-seniory.pdf>
- La puce. (s. d.). *AlphabéTICaction*. <https://lapuce.org/alphabeticaction/>
- L'autorité des marchés financiers. (s. d.). *Prévenir la fraude financière envers les aînés*. <https://lautorite.qc.ca/grand-public/prevention-de-la-fraude/prevenir-la-fraude-financiere-envers-les-aines>
- Lawson, A. (2023, 24 avril). A Look at Global Deepfake Regulation Approaches. *Responsible Artificial Intelligence Institute*. <https://www.responsible.ai/a-look-at-global-deepfake-regulation-approaches/>
- Lee, C. H., Lee, J., Kim, D., Kim, I. et Song, H. (2024). Designing self-ordering kiosk for older adults : Familiarity design focusing on representation, manipulation, and organization. *Computers in Human Behavior*, 156. <https://doi.org/10.1016/j.chb.2024.108236>
- Leeds Older People's Forum. (s. d.). *BOSS (Be online and Stay Safe)*. <https://www.opforum.org.uk/projects-and-campaigns/boss-be-online-and-stay-safe/>
- Liao, S., Wang, X. et Zhang, X. (2024). Loneliness could lead to risk of fraud victimization for middle-aged and older adults. *Journal of Elder Abuse & Neglect*, 36(5), 508-527. <https://doi.org/10.1080/08946566.2024.2404040>
- Logie, K. et Das, S. (2024). Lessons learned from Dread darknet communities : How and why are fraudsters targeting the elderly to be victims or accomplices? *Criminology & Public Policy*, 24(2), 237-271. <https://doi-org.acces.bibl.ulaval.ca/10.1111/1745-9133.12684>
- Makhortykh, M. (2024). *AI and the Holocaust: rewriting history? The impact of artificial intelligence on understanding the Holocaust*. UNESCO. <https://doi.org/10.54675/ZHJC6844>

- Marchand, I. et Laau-Laurin, O. (2025). La participation sociale des personnes âgées : un pilier au développement des communautés locales. *Revue Interventions économiques*. <https://doi.org/10.4000/11qwf>
- McDonald, N. et Mentis, H. M. (2023). 'Don't Fall for This' : Communications about Cybersafety from the AARP. *Proceedings of the ACM on Human-Computer Interaction*, 7(CSCW2), 1-21. <https://doi.org/10.1145/3610039>
- MediaJungle. (s. d.). *Super Fake Safari*. <https://mediajungle.eu/products/super-fake-safari>
- Microsoft. (2025). *Copilot* [Assistant d'intelligence artificielle]. <https://copilot.microsoft.com>
- Ministère de la Santé et des Services sociaux. (2023, 15 septembre). *Journées des partenaires pour contrer la maltraitance envers les personnes âgées*. <https://www.msss.gouv.qc.ca/professionnels/aines/journees-partenaires-pour-contrer-maltraitance-envers-personnes-aines/a-propos/>
- Missouri Department of Health and Senior Services Cible. (s. d.). *Artificial Intelligence Scams*. <https://health.mo.gov/seniors/scams.php>
- Napal, D. (2024). Imitation is the Sincerest Form of Fraudulent Activity : Artificial Intelligence in Financial Scams Against Older Adults. *Bifocal*, 45(6), 1-4. https://www.americanbar.org/content/dam/aba/administrative/law_aging/vol45issue6.pdf
- National council on aging. (2024, 30 octobre). *Understanding Deepfakes: What Older Adults Need to Know*. <https://www.ncoa.org/article/understanding-deepfakes-what-older-adults-need-to-know/>
- Nations Unies. (s. d.-a). *Journée internationale des personnes âgées 1er octobre*. <https://www.un.org/fr/observances/older-persons-day>
- Nations Unies. (s. d.-b). *Journée mondiale de sensibilisation à la maltraitance des personnes âgées 15 juin*. <https://www.un.org/fr/observances/elder-abuse-awareness-day>
- Obvia. (2024, septembre). *Abécédaire de l'IA*. https://www.obvia.ca/sites/obvia.ca/files/resources/202409-OBV-Pub-Abecedaire_IA_1.pdf
- Odil. (s. d.). *La plateforme francophone des initiatives de lutte contre la désinformation*. <https://odil.org/>
- Office québécois de la langue française. (2002). table de concertation. Dans *Grand dictionnaire terminologique*. <https://vitrinelinguistique.oqlf.gouv.qc.ca/fiche-gdt/fiche/8364034/table-de-concertation>
- Office québécois de la langue française. (2005). organisation. Dans *Grand dictionnaire terminologique*. <https://vitrine-linguistique.oqlf.gouv.qc.ca/fiche-gdt/fiche/8357343/organisation>
- Office québécois de la langue française. (2006). maltraitance. Dans *Grand dictionnaire terminologique*. <https://vitrine-linguistique.oqlf.gouv.qc.ca/fiche-gdt/fiche/8352166/maltraitance>
- Office québécois de la langue française. (2008a). organisme. Dans *Grand dictionnaire terminologique*. <https://vitrine-linguistique.oqlf.gouv.qc.ca/fiche-gdt/fiche/8401970/organisme>
- Office québécois de la langue française. (2008b). retraite. Dans *Grand dictionnaire terminologique*. <https://vitrinelinguistique.oqlf.gouv.qc.ca/fiche-gdt/fiche/8352214/retraite>
- Office québécois de la langue française. (2016a). baby-boomer. Dans *Grand dictionnaire terminologique*. <https://vitrinelinguistique.oqlf.gouv.qc.ca/fiche-gdt/fiche/26501953/baby-boomer>
- Office québécois de la langue française. (2016b). génération silencieuse. Dans *Grand dictionnaire terminologique*. <https://vitrinelinguistique.oqlf.gouv.qc.ca/fiche-gdt/fiche/26532902/generation-silencieuse>
- Office québécois de la langue française. (2017). cyberrésilience. Dans *Grand dictionnaire terminologique*. <https://vitrinelinguistique.oqlf.gouv.qc.ca/fiche-gdt/fiche/26544572/cyberresilience>

- Office québécois de la langue française. (2018a). cybercriminalité. Dans *Grand dictionnaire terminologique*. <https://vitrinelinguistique.oqlf.gouv.qc.ca/fiche-gdt/fiche/8350175/cybercriminalite>
- Office québécois de la langue française. (2018b). escroquerie en ligne. Dans *Grand dictionnaire terminologique*. <https://vitrinelinguistique.oqlf.gouv.qc.ca/fiche-gdt/fiche/26552144/escroquerie-en-ligne>
- Office québécois de la langue française. (2018c). fraude. Dans *Grand dictionnaire terminologique*. <https://vitrinelinguistique.oqlf.gouv.qc.ca/fiche-gdt/fiche/26548585/fraude#:~:text=D%C3%A9finition,ou%20%C3%A0%20violer%20le%20droit>
- Office québécois de la langue française. (2019). désinformation. Dans *Grand dictionnaire terminologique*. <https://vitrinelinguistique.oqlf.gouv.qc.ca/fiche-gdt/fiche/17017257/desinformation>
- Office québécois de la langue française. (2023a). organisme communautaire. Dans *Grand dictionnaire terminologique*. <https://vitrinelinguistique.oqlf.gouv.qc.ca/fiche-gdt/fiche/17033125/organisme-communautaire>
- Office québécois de la langue française. (2023b). personne âgée. Dans *Grand dictionnaire terminologique*. <https://vitrinelinguistique.oqlf.gouv.qc.ca/fiche-gdt/fiche/17049404/personne-agee#:~:text=orthographe%20de%201990.-,L'Office%20qu%C3%A9bécois%20de%20la%20langue%20fran%C3%A7aise%20consid%C3%A8re%20comme%20correctes,l'ensemble%20des%20personnes%20%C3%A2g%C3%A9es>
- OpenAI. (2025). *ChatGPT-4o* [Grand modèle de langage]. <https://openai.com/chatgpt>
- Option consommateurs. (s. d.). *Option aînés*. <https://option-consommateurs.org/pour-les-aînés/>
- Ping. (s. d.). *En savoir plus*. <https://pingcommunautaire.quebec/en-savoir-plus/>
- Puig, A. (2023, 20 mars). *Scammers use AI to enhance their family emergency schemes*. Federal Trade Commission : Consumer advice. <https://consumer.ftc.gov/consumer-alerts/2023/03/scammers-use-ai-enhance-their-family-emergency-schemes>
- Réseau Poivre et Sel. (s. d.). *Accueil* [page Facebook]. Facebook. Repéré le 20 novembre 2024 à <https://www.facebook.com/RPS.par.pour.avec.vous/>
- Robinson, J. et Edwards, M. (2024). Fraudsters target the elderly: Behavioural evidence from randomised controlled scam-baiting experiments. *Secur J* 37, 1173–1196. <https://doi.org/10.1057/s41284-023-00410-4>
- Rodríguez-Miranda, F. de P., Illanes-Segura, R., Ceada-Garrido, Y. et Infante-Moro, J. C. (2025). Validation of a scale based on the DigComp framework on internet navigation and cybersecurity in older adults. *Frontiers in Education* 10, 1–10. <https://doi.org/10.3389/feduc.2025.1520929>
- Royal Bank of Canada. (s. d.). *AI-Powered Scams: How AI is Enhancing Existing Scams*. <https://www.rbcroyalbank.com/en-ca/my-money-matters/money-academy/cyber-security/understanding-cyber-security/ai-powered-scams-how-ai-is-enhancing-existing-scams/>
- Sádaba, C., Salaverría, R. et Bringué, X. (2023). Overcoming the Age Barrier: Improving Older Adults' Detection of Political Disinformation With Media Literacy. *Media and Communication*, 11(4), 113–123. <https://doi.org/10.17645/mac.v11i4.7090>
- Schmitt, M. et Flechais, I. (2024) Digital deception: generative artificial intelligence in social engineering and phishing. *Artif Intell Rev* 57, article 324. <https://doi.org/10.1007/s10462-024-10973-2>
- Segal, M. (2024). Protecting older consumers in the digital age : A commentary on ChatGPT, helplines and the way to prevent accessible fraud. *Journal of Elder Abuse & Neglect*, 36(5), 528–533. <https://doi-org.acces.bibl.ulaval.ca/10.1080/08946566.2024.2364208>

Senior Planet. (2024). *AI for Older Adult*. https://seniorplanet.org/wp-content/uploads/2024/11/AI-Guide-for-Older-Adults_Dig.pdf

Senior Service of America. (s. d.). *Don't Fall Prey to Artificial Intelligence Scams: Tips for Recognizing and Guarding Against AI Scammers*. <https://seniorservicesofamerica.com/blog/artificial-intelligence-scams/>

Service canadien du renseignement de sécurité. (2023, octobre). Évolution de la désinformation : Un avenir « hypertruqué » (publication no 2023-10-01). <https://www.canada.ca/fr/service-enseignement-securite/organisation/publications/evolution-de-la-desinformation-un-avenir-hypertruque.html>

Service canadien du renseignement. (2024). *Rapport public de SCRS 2023*. <https://www.canada.ca/fr/service-enseignement-securite/organisation/publications/rapport-public-du-scrs-2023.html>

Sheil, A., Camilleri, J., Cronin, M., Gruben, M., O'Keeffe, M., Murray, H. et Das, S. (2024). Enhancing Personalised Cybersecurity Guidance for Older Adults in Ireland. *Companion Publication of the 2024 Conference on Computer-Supported Cooperative Work and Social Computing*, 478-484. <https://doi.org/10.1145/3678884.3681894>

SKPPSC. (s. d.). *N'hésitez pas, raccrochez !* <https://www.skppsc.ch/fr/sujets/escroquerie/nhesitez-pas-raccrochez/>

South Carolina Department of Consumer Affairs. (2024, 13 juin). *Protecting Older Adults from Scams* [video]. Youtube. https://www.youtube.com/watch?v=YHQ_xfWIADI

Sullivan, J., et Kosuth, E. (2024). Technology Use, Barriers, and Future Needs Among Community-Dwelling Older Adults. *Journal of Gerontological Nursing*, 50(2), 26-31. <https://doi.org/10.3928/00989134-20240110-04>

Sûreté du Québec. (2024, 28 mars). *5 conseils pour prévenir la fraude téléphonique | SQtv Prévention* [vidéo]. Youtube. <https://www.youtube.com/watch?v=fPOvMBKZvWc>

Sûreté du Québec. (s. d.). *Prévention de la fraude*. <https://www.sq.gouv.qc.ca/services/campagnes/mpf/>

Sûreté du Québec. (s. d.). *Prévention*. <https://www.sq.gouv.qc.ca/services/prevention/>

Statistique Canada. (2023, 20 décembre). Préoccupations concernant la désinformation en ligne, 2023. *Le Quotidien*. <https://www150.statcan.gc.ca/n1/daily-quotidien/231220/dq231220b-info-fra.htm>

Tang, Z., Goh, D. H.-L., Lee, C. S. et Yang, Y. (2024). Understanding strategies employed by seniors in identifying deep-fakes. *Aslib Journal of Information Management*. <https://doi.org/10.1108/AJIM-03-2024-0255>

The Bank of Nova Scotia. (2024, 18 septembre). *How to spot and avoid AI scams*. <https://gracevidalribas.ca/how-to-spot-and-avoid-ai-scams/>

The Poynter Institute. (2024, septembre). *MediaWise for Seniors: Self-Directed Fact-Checking Course*. <https://www.educations.com/institutions/the-poynter-institute/mediawise-for-seniors-self-directed-fact-checking-course>

Théâtre Déchaînés. (2024). *Parlez-moi d'amour*. <https://www.theatredechaines.com/projets/pda>

Thomas, D., Chowdhury, G. et Ruthven, I. (2023). Exploring older people's challenges on online banking/finance systems : Early findings. *Proceedings of the 2023 Conference on Human Information Interaction and Retrieval*, 333-337. <https://doi.org/10.1145/3576840.3578324>

Toronto public library. (s. d.). *What is Misinformation and Disinformation? What is Misinformation and Disinformation? : Toronto Public Library*

True Link. (2024, 9 septembre). *AI-Powered Scams: What You Need to Know to Help Safeguard Your Aging Loved Ones*. <https://www.truelinkfinancial.com/blog/ai-powered-scams-what-you-need-to-know-to-help-safeguard-your-aging-loved-ones>

Van Amstel, E. (2023, 7 septembre). *Deepfakes : de fausses vidéos d'une qualité inquiétante*. Seniorweb. <https://www.seniorweb.nl/artikel/deepfakes-nepvideo-s-van-verontrustend-hoge-kwaliteit>

Wang, D., Duan, Y. et Jin, Y. (2025). Navigating online perils : Socioeconomic status, online activity lifestyles, and online fraud targeting and victimization of old adults in China. *Computers in Human Behavior*, 162, article 108458. <https://doi.org/10.1016/j.chb.2024.108458>

Xin, Y., Xia, Y. et Chai, Y. (2024). Routine activities and fraud re-victimization among older adults : Do types of routine activities matter? *Criminology & Criminal Justice: An International Journal*. <https://acces.bibl.ulaval.ca/login?url=https://search.ebscohost.com/login.aspx?direct=true&db=aph&AN=177589597&login.asp&lang=fr&site=ehost-live&scope=site>

Xu, L., Lam, Y. Y., Ng, D. T. K., Peng, P., Suen, W. L., Lee, C. S. Y. et Chu, S. K. W. (2024). Digital Literacy Education for Older Adults : A Scoping Review. *Proceedings of the Association for Information Science & Technology*, 61(1), 691-696. <https://doi-org.accres.bibl.ulaval.ca/10.1002/pra2.1081>

Yan, Z., Yao, T., Chen, S., Zhao, Y., Fu, X., Zhu, J., Luo, D., Yuan, L., Wang, C., Ding, S. et Wu, Y. (2024). DF40 : Toward Next-Generation Deepfake Detection. *Arxiv*. <https://doi.org/10.48550/arXiv.2406.13495>

Yao, Y. et Yang, F. (2024). Perceptions of Consumer Fraud and Aging Among Older People and the Judiciary in China. *Journal of Aging & Social Policy*, 1-19. <https://doi-org.accres.bibl.ulaval.ca/10.1080/08959420.2024.2349496>

Zone AVA. (s. d.). À propos. <https://zoneava.ca/zoneava-accompagner-dans-un-veillissement-actif/>

The Obvia logo features the word "obvia" in a white, lowercase, sans-serif font. The letter "o" is stylized with a small white dot above it. The logo is positioned in the bottom left corner of the page, which has a solid purple background. A large, light purple circular shape is partially visible on the left side of the page, overlapping the logo.

obvia

obvia.ca