CRÉDOC
CENTRE DE RECHERCHE POUR L'ÉTUDE ET L'OBSERVATION DES CONDITIONS DE VIE

Cahier de recherche

C360

@ Mike Hindel - Unsplash

Malgré leurs précautions, quatre Français sur dix ont été victimes de cyber malveillance au cours de l'année écoulée

Auteurs :

Morgane BRENON

Lucie BRICE MANSENCAL

Patricia CROUTTE

Sandra HOIBIAN

Décembre 2025

CENTRE DE RECHERCHE POUR L'ETUDE ET L'OBSERVATION DES CONDITIONS DE VIE
142 rue du Chevaleret -75013 PARIS – Tél : +33 (0)1 40 77 85 00 www.credoc.fr

Principaux résultats

- Une exposition massive et en progression aux arnaques numériques.

73 % des internautes ont été exposés à des arnaques et fraudes en ligne au cours de l'année écoulée. (Réception d'e-mails ou d'appels frauduleux pour récupérer des informations personnelles, logiciel malveillant ou d'un virus sur un de vos appareils, piratage d'un compte de réseau social ou d'une boîte mail, escroquerie en ligne concernant l'achat d'un produit (non livré, contrefait ou non conforme), escroquerie en ligne concernant l'achat d'un service ou d'une prestation (location, voyage, etc.), escroquerie bancaire sur internet, demande de paiement ou demande de rançon en échange de la récupération de données, de photos ou de contrôle de votre appareil, usurpation d'identité). Parmi lesquels 34 % en ont été la cible mais les ont repérés à temps et ont réussi à y échapper, tandis que 4 internautes sur 10 (39 %) déclarent en avoir été victimes. Seuls 26 % des internautes dit ne pas avoir été victimes ni avoir repéré des tentatives de cyberattaques sur la période.

La plupart des faits frauduleux étudiés semblent concerner une part de la population en hausse par rapport à 2019.

- Les e-mails et appels frauduleux, de loin les pratiques les plus répandues.

La situation de loin la plus fréquente est la réception d'e-mails ou appels frauduleux, avec 63 % d'internautes exposés à ces pratiques, et 21 % qui en ont été victimes. Suivi par les escroqueries en ligne concernant l'achat de produits (non livré, contrefait ou non conforme) avec 32 % d'internautes exposés et 15 % de victimes.

- Les jeunes adultes sont les plus exposés.

Les moins de 40 ans sont plus fréquemment victimes de cyberattaques, et plus encore les moins de 25 ans. Il s'agit des publics qui sont les plus présents sur la toile et y multiplient les usages. Ils sont ainsi 59 % des 15 à 24 ans à déclarer avoir déjà été victimes de cyberattaques contre 35 % de leurs congénères de 40 à 59 ans. Et cette spécificité des jeunes de moins de 25 ans perdure quand on réalise une analyse toutes choses égales par ailleurs.

- Des pratiques de précaution largement adoptées qui n'empêchent pas la diffusion des arnaques

La fréquence de ces actes malveillants est d'autant plus notable que, pourtant, 88 % des internautes ont adopté des pratiques de précaution en ligne. Le recours aux outils destinés à se protéger sur internet se diffuse et se diversifie dans la population. La part de la population qui ne se protège pas du tout en ligne diminue (-5 points en 5 ans).

La cybercriminalité se développe et se perfectionne, nécessitant une formation continue de la population pour la déjouer.

- Moins d'une personne sur deux engage des démarches après avoir été la cible d'une arnaque en ligne.

Parmi les personnes ciblées ou victimes d'une arnaque numérique, 48 % des internautes entament une démarche de recouvrement ou de plainte.

Le niveau des réactions est plus élevé (66 % des cas) dès lors que l'internaute est tombé dans le piège et en a été victime. Alors que ceux qui n'ont subi que des tentatives (et qui ont pu intervenir avant qu'il y ait préjudice) ne réagissent « que » dans 27 % des cas.

- Des répercussions psychologiques fréquentes et socialement marquées

41 % des victimes et des cibles d'arnaques ou fraudes en ligne déclarent avoir été affectées psychologiquement à la suite de ces événements. Les personnes effectivement victimes sont davantage impactées (56 %) que celles qui ont réussi à parer l'attaque (22 %). Mais, même chez celles-ci, une sur cinq témoigne d'un contrecoup psychologique.

Parmi les victimes d'arnaques et fraudes en ligne, on observe que ceux ayant des séquelles psychologiques sont aussi plus fréquemment ceux qui se sentent exclus et ceux qui présentent des souffrances quotidiennes, du type : maux de tête et migraines, mal de dos, nervosité, état dépressif, insomnie.

SOMMAIRE

1. Introduction

Dans son rapport sur la cybercriminalité, le Centre d'analyse et de regroupement des Cybermenaces (CECyber) du Commandement du ministère de l'Intérieur dans le cyberespace (COMCYBER-MI)[1] constate une montée en puissance des réseaux de cybercriminalité. Ce « secteur » **s'industrialise** avec le recours aux forums cybercriminels et canaux de discussion ouverts (qu'ils mobilisent pour échanger au quotidien, acheter, louer et vendre des services comme des logiciels malveillants, accès initiaux, bases de données, recrutements de cybercriminels, partage de connaissance, etc.), aux messageries chiffrées (pour évoquer des sujets plus sensibles tels que les montants des transactions, recrutement des cybercriminels, etc.), aux réseaux sociaux (qui permettent de cibler un grand nombre de victimes) et à la téléphonie (pour échanger via des solutions chiffrées ou démarcher des victimes).

Les attaques se perfectionnent, notamment grâce à **l'intelligence artificielle** (IA) : elles se font à la fois **plus nombreuses, plus ciblées et moins discernables.** *« L'utilisation de l'intelligence artificielle permet aux acteurs malveillants de mettre en place des campagnes d'hameçonnage de plus en plus crédibles et difficiles à déceler par les victimes ».*

En 2024, 348 000 atteintes numériques auraient ainsi été commises, **en augmentation de 74 %** par rapport à 2019. 65 % des atteintes numériques enregistrées concernaient des **biens**, 30 % des **personnes** et 5 % des **institutions et de l'ordre public**[2].

Au fil de la diffusion et de la diversification des usages du numérique, les risques allant de pair concernent de plus en plus d'individus et sont devenus de nature plus variée, susceptibles d'affecter de nombreux pans de la vie des individus : depuis les achats en ligne, à la vie affective et sociale, en passant par les démarches administratives ou les réseaux sociaux. Ces usages malveillants du numérique évoluent de concert avec les avancées technologiques.

Au-delà des inquiétudes, quels sont les publics les plus concernés par ces actes de malveillance qui se propagent sur internet ? Quels sont les méfaits les plus répandus ? Comment les internautes français s'en protègent-ils, réussissent-ils à déjouer certaines pratiques ? Lorsqu'ils sont victimes, quels recours empruntent-ils et y a-t-il, selon eux, des répercussions psychologiques notables ?

Pour répondre à ces interrogations, cinq questions ont été insérées dans la vague d'enquête de juin 2025 du dispositif longitudinal « Conditions de vie et Aspirations ».

[1] COMCYBER-MI. (2025). *Rapport annuel sur la cybercriminalité.*

[2] COMCYBER-MI, *op. cit.*

Méthodologie

Les données utilisées proviennent de questions insérées dans le dispositif d'enquête du CRÉDOC sur les Conditions de vie et les aspirations de juin 2025. L'enquête a été réalisée du 5 au 21 juin 2025, auprès d'un échantillon représentatif de la population de 15 ans et plus.

L'échantillon a été interrogé par questionnaire auto-administré **en ligne** sur système CAWI (Computer-Assisted Web Interview) auprès des membres d'un panel en ligne. 3 473 personnes âgées de 15 ans et plus, résidant en France ont été sélectionnées selon la méthode des quotas. Ces quotas (région, taille d'agglomération, âge, sexe, habitat individuel ou collectif et PCS) ont été calculés d'après le dernier recensement général de la population disponible.

Afin d'assurer la représentativité par rapport à la population nationale, un redressement final a été effectué en fonction des critères suivants : variable croisée sexe x âge, région, taille d'agglomération, PCS de la personne interrogée, logement individuel ou collectif ainsi qu'une variable croisée âge x niveau de diplôme qui permet de limiter le biais de sélection lié au mode de recueil.

L'étude ayant été menée en ligne, elle exclut de fait les « non-internautes », c'est pourquoi, dans tout le rapport nous parlons systématiquement de cette cible des internautes et non pas des « Français » dans leur ensemble.

En effet selon l'Insee[3], en 2024, 11 % des individus de 15 ans et plus n'ont pas utilisé Internet dans les trois derniers mois. Le baromètre du numérique 2025[4] dénombre 6 % des 12 ans et plus.

[3]Insee. (2024). *Enquête sur les technologies de l'information et de la communication par les ménages entre 2009 et 2024.* Récupéré sur https://www.insee.fr/fr/statistiques/8278698?sommaire=8278710

[4]Arcep, Arcom, CGE, ANCT. (2025). *Baromètre du numérique, édition 2025.* Récupéré sur https://www.credoc.fr/publications/barometre-du-numerique-edition-2025

2. 73 % des internautes ont été confrontés à de la criminalité en ligne, 39 % en ont été victimes au cours des 12 derniers mois

2.1. La réception d'e-mails ou d'appels frauduleux est la cyberattaque la plus courante et la mieux repérée

Nous avons interrogé la population sur sept types de cyberattaques[5], en leur demandant, pour chacune d'entre elles, s'ils en avaient été victimes personnellement au cours des douze derniers mois, s'ils y avaient été confrontés mais avaient pu s'en rendre compte à temps, ou s'ils n'avaient pas été concernés.

- Les cyberattaques ou tentatives de cyberattaques sont de loin les plus repérées par la population concernent la **réception d'e-mails ou appels frauduleux.**

63 % d'internautes déclarent avoir été exposés à des tentatives d'hameçonnage par ce biais (Graphique 1). Parmi ces personnes visées, un tiers se dit victime (21 %) tandis que les deux tiers (42 %) disent y avoir été confrontés mais s'en être rendu compte à temps. Le phénomène semble en **nette augmentation**. Six ans plus tôt, une enquête de la Commission européenne (l'Eurobaromètre spécial 499 en 2019) dénombrait 47 % des internautes Français concernés par des courriels ou appels frauduleux (en tant que victimes et non-victimes) au cours des trois précédentes années[6]. Concernant plus spécifiquement les courriels frauduleux, la plateforme Signal Spam a recensé 1 175 209 signalements en France entre juillet et septembre 2025 (contre 922 740 au deuxième trimestre 2022), dont 60 % provenaient d'un plug-in installé par la plateforme et qui minore donc probablement l'ampleur du phénomène[7].

Le ministère de l'Intérieur évoque ainsi parmi les tendances en hausse : **le vishing** (*voice phishing*), en fort essor. *« Les appels téléphoniques sont devenus quotidiens et ciblent l'ensemble de la population. Les auteurs innovent dans les discours employés et l'identité des organismes utilisés, par exemple lors des campagnes au faux conseiller bancaire. Ces campagnes s'accompagnent le plus souvent de l'usurpation d'une ligne téléphonique légitime (spoofing) ».* Il signale également que le télétravail représente une source de compromission pouvant être exploitée par les cybercriminels, par exemple

[5] La question posée était la suivante Au cours des douze derniers-mois, avez-vous été confronté aux situations suivantes sur internet ? Pour chacune des 7 situations étudiées, le répondant pouvait répondre Oui, j'en ai personnellement été victime /Oui, j'y ai été confronté mais j'ai pu m'en rendre compte à temps /Non/ Ne sait pas.
Réception d'e-mails ou d'appels frauduleux pour récupérer des informations personnelles, logiciel malveillant ou d'un virus sur un de vos appareils, piratage d'un compte de réseau social ou d'une boîte mail, escroquerie en ligne concernant l'achat d'un produit (non livré, contrefait ou non conforme), escroquerie en ligne concernant l'achat d'un service ou d'une prestation (location, voyage, etc.), escroquerie bancaire sur internet, demande de paiement ou demande de rançon en échange de la récupération de données, de photos ou de contrôle de votre appareil, usurpation d'identité.

[6] La différence de formulation entre la question posée par le Crédoc et celle posée par l'Eurobaromètre laisse supposer que les taux mesurés par l'Eurobaromètre en 2019 captent une version élargie du phénomène. La question posée par l'Eurobaromètre se fonde sur les événements au *cours des 3 dernières années* (vs 12 derniers mois dans le cadre du Crédoc) : mécaniquement, l'horizon de temps plus long de l'Eurobaromètre élargit la base des personnes concernées, et de plus, il est vraisemblable que les répondants intègrent des évènements leur étant arrivé au-delà des 3 dernières années, la mémoire précise des dates pouvant être floue.

[7] Voir Signal Spam, Baromètre du spam, URL : https://www.signal-spam.fr/barometre-du-spam/ Consulté le 16/12/2025

via l'arnaque au PDG « *whale phishing* » ou le malfrat se fait passer pour le PDG de la structure et demande à son interlocuteur (comme le directeur financier) d'exécuter ses demandes.

- **La découverte de virus et logiciels malveillants** est la seconde cyberattaque la plus citée, par 32 % d'internautes. 12 % de la population déclare en avoir été victime**.**

En 2019, selon l'enquête *Eurobarometer special* 499[8], 37 % des internautes Français disaient avoir repéré ou avoir été affectés par un virus ou logiciel malveillant au cours des trois dernières années. Cette situation pourrait donc avoir un peu **reculé ou être moins détectée** par la population.

- Les escroqueries en ligne, **concernant l'achat de produits (non livré, contrefait ou non conforme)** sont en deuxième position ex-aequo : 32 % d'internautes y ont été exposés, et 15 % victimes.

Faux sites d'achat en ligne, produit qui n'est jamais reçu ou qui est très différent de celui commandé, contrefaçon, produit dangereux ou non conforme, les arnaques peuvent être nombreuses. L'Eurobaromètre de 2019 mesurait 14 % d'internautes *exposés* au cours des 3 dernières années, ce qui laisse supposer **une augmentation** du phénomène, probablement en liaison avec la diffusion des achats en ligne auprès de publics moins expérimentés, et avec la hausse des volumes de transactions. La **part des acheteurs** en ligne est en effet passée de 53 % de la population en 2019 à 63 % en 2024 selon l'Insee[9]. Le baromètre du numérique[10] constate ainsi un mouvement de hausse quasi continue depuis le début des années 2000 où seuls 7 % de la population effectuait alors des achats en ligne. Au-delà de la progression du nombre d'acheteurs, **les volumes d'achats de biens et de services** ont beaucoup progressé dans l'intervalle. Selon la FEVAD, le e-commerce représentait 175,3 milliards d'euros en 2024[11], contre 103,4 milliards d'euros en 2019[12], soit +70 % de croissance en cinq ans.

Dans notre enquête, l'**escroquerie en ligne concernant l'achat d'un service** est moins courante que concernant les produits : elle est mentionnée par 26 % des répondants (10 % de victimes)

Les données d'Eurostat[13] en 2023 avec des situations étudiées un peu différentes, décomposaient certaines des problématiques liées à l'achat en ligne de *produits ou services* auprès des personnes ayant utilisé internet au cours des 3 derniers mois : 14,13 % d'entre elles indiquaient une livraison plus lente qu'indiquée, 6,07 % des produits ou services différents de ceux souhaités ou endommagés, 3,09 % des cas de fraude, et 3,08 % un coût plus élevé qu'annoncé.

---

[8]Commission Européenne. (2019). *Special Eurobarometer 499.*
C'est de cette étude qu'ont été repris les items soumis aux enquêtés cette année.

[9]Insee. (2025). *Achats de produits et de services en ligne.* Récupéré sur https://www.insee.fr/fr/statistiques/8616823?sommaire=8616883

[10] Arcep, Arcom, CGE, ANCT, *op. cit.*

[11] Fevad. (2025). *Bilan du e-commerce en France en 2024 : les ventes sur internet franchissent le cap des 175 milliards d'euros, en hausse de 9,6 % sur un an.* Récupéré sur https://www.fevad.com/bilan-du-e-commerce-en-france-en-2024-les-ventes-sur-internet-franchissent-le-cap-des-175-milliards-deuros-en-hausse-de-96-sur-un-an/

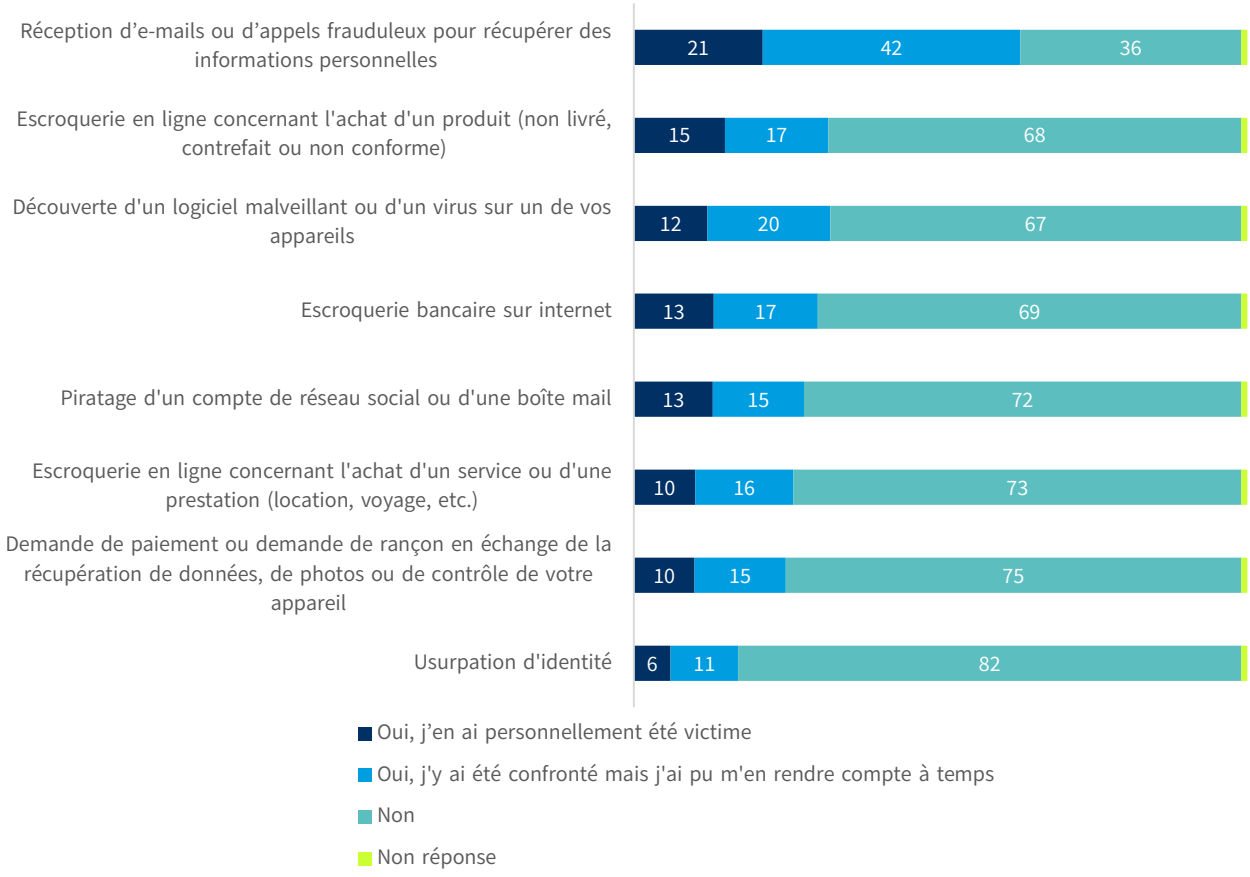
NB : les chiffres de 2025 ne sont pas encore disponibles.

[12] *Ibid.*

[13]Eurostat. (2025). *Problems experienced when buying online (isoc_ec_iprb21).* Récupéré sur https://ec.europa.eu/eurostat/databrowser/view/isoc_ec_iprb21/default/table?lang=en&category=isoc.isoc_i.isoc_iec

Graphique 1 – « Au cours des douze derniers mois, avez-vous été confronté aux situations suivantes sur internet ? »

- Champ : ensemble de la population internaute de 15 ans et plus, en % - effectif total pondéré n : 3 473 -



Source : CREDOC, enquête Conditions de vie et aspirations juin 2025

Lecture : sur 100 internautes de 15 ans et plus, 21 ont été victimes au cours des douze derniers mois de réception d'e-mails ou d'appels frauduleux, 42 ont repéré des tentatives sans en devenir victimes et 36 ne sont pas concernées.

- Les **escroqueries bancaires sur internet** constituent la **4e cyberattaque la plus fréquente**.

Carte contrefaite, numéro de carte usurpé, fraude au prélèvement, fraude par manipulation (c'est-à-dire quand le client est amené à valider lui-même l'opération après une manipulation, souvent faux conseiller / faux service anti-fraude), les cas d'escroqueries liées aux opérations bancaires sont nombreux. Le service statistique ministériel de la sécurité intérieure[14] met ainsi en évidence une **augmentation rapide des escroqueries et fraudes aux moyens de paiement** (qu'ils passent par les modes de contacts numériques ou pas). En France entre 2016 et 2023, on a dénombré 411 700 victimes en 2023 contre 250 900 victimes en 2016, soit une progression moyenne de +7,3 % par an (+64 % sur l'ensemble de la période).

[14] Interstat, Service statistique ministériel de la sécurité intérieure. (2024). *Les escroqueries enregistrées par les services de sécurité entre 2016 et 2023.* Récupéré sur https://www.bnsp.insee.fr/ark:/12148/bc6p0934n7g.pdf

Dans l'enquête du Crédoc, l'escroquerie bancaire sur internet est citée par 30 % de la population internaute, dont 13 % de victimes. Soit un taux de personnes exposées supérieur à celui observé en 2019 par l'Eurobaromètre (14 %), laissant supposer une **progression** de la diffusion de celles-ci.

Pourtant les données de la Banque de France et des plateformes de signalement mettent en avant plutôt des tendances au recul de la fraude :

- La Banque de France signale une baisse du **taux** de fraude à 0.053 % de la valeur totale des paiements avec carte bancaire (qui représente le gros des transactions avec 62 % des paiements). Elle y voit notamment les effets de **la mise en place de règles d'authentification forte** définies par la deuxième directive européenne sur les services de paiement.
- Les **signalements** sur la plateforme Perceval[15] du ministère de l'Intérieur, qui recense les signalements d'achats frauduleux en ligne avec une carte bancaire, enregistraient 230 537 usages frauduleux de cette nature en 2024, soit moins qu'en 2023 (259 094 signalements) et qu'en 2022 (304 923 en 2022).
- La plateforme Thésée, ouverte en mars 2022 et gérée par l'Office anti-cybercriminalité (OFAC) de la Police nationale, permet aux particuliers victimes d'escroqueries en ligne de déposer plainte à distance. En 2024, cette plateforme a recensé 53 300 dépôts de plainte relatifs à une escroquerie ou une fraude aux moyens de paiement. Cela représente 11 % du total des victimes d'escroquerie ou de fraude aux moyens de paiement recensées par le SSMSI, taux en baisse par rapport à 2023 (14 %).

Plusieurs phénomènes expliquent cette apparente dissonance :

- Tout d'abord, nous l'avons vu, les **achats en ligne**, notamment par carte, ont progressé, ainsi que le recours aux modes de paiement numériques[16], tels que le paiement **par mobile ou le virement instantané**, et donc même si le *taux* de fraude reste stable, les ***montants*** constatés de fraude ont progressé (Par exemple sur la carte bancaire les montants de fraude passent de 470 millions d'euros à 519 millions d'euros, soit +10 % entre 2019 et 2024)
- Lorsqu'il y a plainte pour escroquerie auprès de la banque, rappelons que 9 % du nombre d'opérations et **38 % des montants ne sont pas remboursés** : si la **victime a consenti à l'opération**, dans le cadre d'une manipulation, d'un chantage (par exemple, faux site usurpant l'identité d'un e-commerçant, faux investissements, chantage amoureux ou paiement de rançongiciel) ; lorsque la banque est en mesure de démontrer que le client a fait preuve de négligence grave dans la protection de ses identifiants personnels ou de ses moyens d'authentification, lorsque les opérations résultent d'un **litige commercial** (bien ou service non livré ou non conforme aux attentes du client, ou liquidation judiciaire du commerçant), lorsque la **contestation est jugée abusive** (cas d'un achat effectué par les enfants à l'insu du client par exemple). Les répondants à l'enquête Crédoc ont vraisemblablement intégré ces situations même s'ils n'ont pas obtenu remboursement.

[15] Par exemple 10 % des paiements de proximité par carte sont réalisés avec le téléphone mobile.

[16] Banque de France. (2024). *Rapport de l'Observatoire de la sécurité des moyens de paiment 2023.* Récupéré sur https://www.banque-france.fr/fr/publications-et-statistiques/publications/rapport-de-lobservatoire-de-la-securite-des-moyens-de-paiement-2023

Les internautes ont donc probablement **renoncé à signaler** ces escroqueries ne sachant pas comment procéder ou anticipant l'impossibilité à obtenir dédommagement dès lors que leur responsabilité était en jeu, par exemple dans le cadre des arnaques perpétrées par de faux conseillers bancaires.

- Ensuite les données de la Banque de France concernent aussi bien **les particuliers, que les entreprises et les institutions**. Or les particuliers sont moins armés face à ce type d'arnaques dont ils sont plus souvent victimes.
- Les données du Crédoc sont plus **récentes**, et intègrent probablement les nouvelles escroqueries liées à l'essor de la **plateforme Wero** (qui permet un paiement instantané vers un téléphone mobile sans indiquer son IBAN) comme les cas de demande de remboursement de « trop perçu » de faux acheteurs, ou d'envoi de liens de phishing.

- Les **piratages ou tentatives de piratage d'un compte de réseau social ou de courriel** sont repérés par 28 % de la population active sur la toile, 13 % s'en déclarant victimes.

En 2019, 20 % des internautes y avaient été confrontés selon la Commission européenne, soit là aussi une **hausse** des expositions à ce type de malveillance.

- Vient ensuite la **demande de paiement ou demande de rançon** citée par 25 % des répondants (10 % des internautes s'en disent victimes).

- C'est **l'usurpation d'identité** qui clôt le classement.

Cette infraction est, certes, **la moins répandue** (17 % des internautes Français disent y avoir été exposés), mais **il semble difficile de la déjouer** (puisque 6 % des internautes Français s'en disent victimes, soit 46 % de ceux qui ont été visés).

Selon le site internet du ministère de la Justice[17], l'usurpation d'identité est le fait d'utiliser, **sans son accord**, les informations d'identifications ou les données personnelles d'une autre personne. Ces éléments sont ensuite utilisés dans un **but malveillant** (délivrance d'une carte d'identité, souscription d'un crédit, d'un abonnement, nuire à la réputation, commettre des infractions pénales...). L'usurpation d'identité peut être commise à la suite des situations suivantes, par exemple :

- Piratage sur les réseaux sociaux avec récupération de données personnelles
- Vol ou perte d'une pièce d'identité
- Envoi de documents personnels à de fausses annonces de location ou d'emploi
- Envoi de renseignements personnels à un faux organisme ou une fausse administration
- Récupération de documents contenant des données personnelles de la victime (relevé bancaire, bulletin de salaire...).

Mais il est probable que les répondants dans notre enquête aient une acception assez large de l'usurpation d'identité, car nous ne leur avons pas proposé de définition de celle-ci, et la longueur du questionnaire ne permettait pas de vérifier qu'ils étaient réellement dans les cas de figure prévus et punis par le législateur.

[17] Ministère de la Justice. (2025). *"Usurpation d'identité".* Récupéré sur https://www.justice.fr/fiche/usurpation-identite

Concernant ce méfait, il est difficile de déterminer la tendance d'évolution : les **données existantes pour 2019-2020 ne semblent pas converger**, **variant entre 1 % et 18 % de personnes victimes, selon les questions posées**. Les travaux de l'Insee en collaboration avec le Service statistique ministériel de la sécurité intérieure (SSMSI) du ministère de l'Intérieur, en collaboration avec le Service statistique ministériel de la Justice (SDSE),[18] estimaient en effet à 1 % les individus concernés **par un vol d'identité** en 2019 (dans le cadre d'une question portant sur les problèmes de sécurité informatique). L'Eurobaromètre mesurait 7 % des internautes Français qui se disaient concernés en 2019 par la situation suivante « vol d'identité : quelqu'un vous a volé vos données personnelles et s'est fait passer pour vous ». Un sondage IPSOS effectué en octobre 2020 pour le programme France identité numérique, décomptait plus d'un internaute Français sur quatre (28 %) ayant fait l'objet d'une ou plusieurs tentatives de vol de son identité en ligne, au cours des deux dernières années, et un sur cinq (18 %) effectivement victime d'une usurpation d'identité[19].

2.2. Les trois-quarts des internautes ont conscience d'avoir été exposés à des menaces numériques au cours de l'année écoulée

En 2025, si l'on prend en compte les huit situations étudiées, **une très large majorité de la population (73 %)** a été confrontée de près ou de loin à des menaces en ligne.

- **39 % ont été victimes** d'au moins une de ces malveillances au cours des 12 derniers mois.
- 34 % ont **repéré et évité à temps** toutes les cyberattaques dont ils ont été la cible.
- 26 % déclarent n'avoir **jamais** été victimes ni repéré des tentatives de cyberattaques durant les douze mois qui précèdent l'enquête. Seul un internaute Français sur quatre échappe donc à toute tentative de cybercriminalité

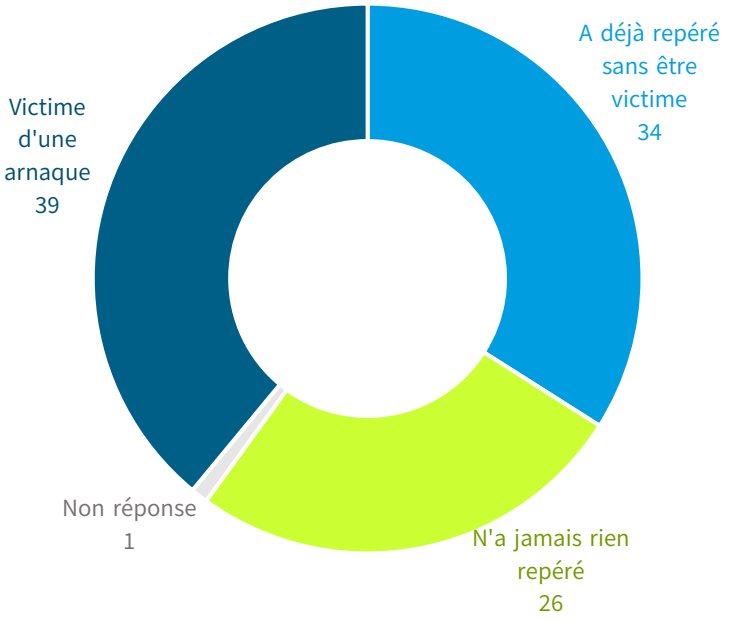
[18] Insee. (2021). *Sécurité et société, édition 2021.* Récupéré sur https://www.insee.fr/fr/statistiques/5763599?sommaire=5763633

[19] Le détail du rapport et de la question posée précisément n'est pas disponible sur la toile. Ces données proviennent du site de France identité, commanditaire de ce sondage auprès d'IPSOS : https://france-identite.gouv.fr/en-savoir-plus/de-quoi-s-agit-il/

Graphique 2 – « Au cours des douze derniers-mois, avez-vous été confronté aux situations suivantes sur internet ? »

Regroupement des internautes selon qu'ils ont été victimes d'au moins un méfait, qu'ils ont repéré et évité toutes les cyberattaques, ou qu'ils n'ont été concernés par aucune de ces attaques [20]

- Champ : ensemble de la population de 15 ans et plus, en % - effectif total pondéré n : 3 473 -



Source : CREDOC, enquête Conditions de vie et aspirations juin 2025

Les différentes arnaques évoquées intègrent les attaques à l'identité numérique, et le vol de données personnelles (identité sur les réseaux, vols de photos, contrôle d'appareil, virus ou logiciel malveillant, etc.), ainsi que les problèmes liés à l'achat en ligne de produits (produit contrefait ou non conforme). Notons que si l'on se concentre uniquement sur les victimes d'arnaques en ligne **ayant abouti à une perte d'argent** (3,2 %), ou à un débit frauduleux sur le compte bancaire (4,7 %), le taux de personnes concernées serait beaucoup plus faible, selon l'enquête de victimisation menée par le SSMSI (2023)[21], qui dénombre moins de 8 % de la population Française victime **au cours de sa vie**.

Le baromètre Cybermalveillance de l'Ipsos (2024) met en évidence des niveaux d'exposition aux cyberattaques plus élevés que ceux observés dans l'enquête du SSMSI. Au total, 61 % d'internautes

[20] Cet indicateur a été élaboré à partir des 7 situations étudiées dans l'enquête du Crédoc. Pour rappel, cette liste comprend : *la réception d'e-mails ou d'appels frauduleux pour récupérer des informations personnelles, la découverte d'un logiciel malveillant ou d'un virus sur un de ses appareils, le piratage d'un compte de réseau social ou d'une boîte mail, l'escroquerie en ligne concernant l'achat d'un produit (non livré, contrefait ou non conforme), l'escroquerie en ligne concernant l'achat d'un service ou d'une prestation (location, voyage, etc.), l'escroquerie bancaire sur internet, la demande de paiement ou demande de rançon en échange de la récupération de données, de photos ou de contrôle de son appareil, l'usurpation d'identité*.
À chacune de ces situations, les répondants indiquent s'ils en ont déjà été victime ou bien s'ils y ont été confrontés et s'en sont rendus compte à temps ou encore aucun des deux. L'indicateur a été construit à partir d'un compteur pour les victimes d'un côté et pour ceux qui ont repéré des arnaques d'un autre côté.

[21] SSMSI. (2023). *Vécu et ressenti en matière de sécurité: Victimation, délinquance et sentiment d'insécurité.*

déclarent avoir été touchés par des cyberattaques (virus informatique, fraude bancaire, ordinateur bloqué, piratage de comptes, menaces de diffusion de contenus intimes…) au cours des douze derniers mois. Parmi eux, ils dénombrent 73 % déclarent des e-mails, SMS ou appels frauduleux (-13 points en 2025). Par ailleurs, 20 % des internautes disent avoir été confrontés à des escroqueries bancaires et faux conseillers (-5 points en 2025) et 30 % ont été exposés à des logiciels malveillant ou des virus, 24 % au piratage d'un compte en ligne, 11 % à des demandes de paiement ou de rançon et enfin 11 % à du cyberharcèlement.

Au-delà du champ des malversations numériques plus large étudié par le Crédoc, l'écart avec les données du SSMSI peut être amplifié par des questions de méthode :

- Le recours, au CREDOC, à un panel en ligne peut contribuer à cette différence : les personnes de notre échantillon pourraient se trouver plus exposées aux cyberattaques que celles de l'enquête du SSMSI qui ont été enquêtées en mix-mode (internet, mais aussi papier et téléphone, intégrant donc davantage de personnes peu présentes sur Internet).
- La façon dont les questions ont été formulées et leur nombre peut avoir son importance : dans l'enquête du CREDOC, le sujet de la cybercriminalité était largement abordé, au travers des inquiétudes qu'il suscite, des précautions qu'il est possible de prendre pour se protéger et la liste des actes malveillants est, par ailleurs, relativement détaillée : toutes ces questions de contexte peuvent aider le répondant à mieux solliciter sa mémoire et à citer davantage de faits (voir le questionnaire en annexe, page 52). Dans l'enquête du SSMSI : il s'agit de deux questions simples, arrivant sans introduction ni contexte, (Avez-vous été victimes de débit frauduleux ? Avez-vous été victimes d'escroqueries ou arnaques ayant engendré une perte d'argent ?)
- Dans l'enquête du SSMSI, les deux questions de cyberattaque apparaissent dans un bloc qui comprend également :
    - Tentative de vol avec violence physique ou menace
    - Vol avec violence physique ou menace
    - Tentative de vol sans violence physique ou menaces
    - Vol sans violence physique ou menace

  La cyberattaque peut dès lors apparaître comme un acte bénin par rapport aux vols et tentatives de vol (surtout face à ceux incluant des violences et menaces) et/ou être largement mis en retrait dans la mémoire au profit d'événements plus traumatisants (notamment les violences physiques).

2.3. Un portrait des victimes

Les travaux de Cohen et Felson (1979) ont révélé l'importance des habitudes et des pratiques en lien avec l'environnement socioéconomique dans la probabilité d'être victime de criminalité. Des travaux de recherche ultérieurs ont démontré la pertinence de leur théorie de l'activité routinière (Routine Activity Theory ou RAT) dans le cas plus précis de la cybercriminalité : des usages numériques actifs et intenses ainsi que des pratiques numériques plus spécifiques (achats en ligne, réseaux sociaux…) vont de pair avec une surexposition à la cybercriminalité, de la même manière que certaines routines de la

vie quotidienne hors ligne peuvent également surexposer à certains types de crimes (Näsi et al., 2015 ; Oksanen & Keipi, 2013[22]).

Les usages numériques sont un construit social[23] modelé tant par le parcours de l'individu que par son environnement social. Le contexte de vie[24] de l'usager numérique détermine son parcours d'appropriation de certaines compétences, de certaines pratiques et donc son exposition ou sa protection à l'égard de certains risques. À titre d'exemple, les internautes avec une diversité d'usages d'internet sont confrontés à des situations qui imposent des routines de sécurité (achats en ligne, gestion de comptes bancaires, démarches sur les plateformes officielles), ce qui les conduit à adopter certaines pratiques de vérification (contrôle des URL, authentification renforcée). À l'inverse, les internautes n'ayant qu'un usage récréatif d'internet, les apprentissages se font davantage par imitation et habitudes que par règles explicites. Ces conditions favorisent des pratiques plus risquées (clics rapides, échanges d'informations), pouvant accroître la vulnérabilité aux risques de cybercriminalité.

Le lauréat du prix Nobel d'économie de 1998, Amartya Sen (1997)[25], a développé le concept d'environnement capacitant, applicable à de nombreux domaines. Dans le cadre de la sensibilisation à la cybercriminalité, ce concept permet d'expliquer en partie les inégalités sociodémographiques. En effet, un individu bénéficiant d'un environnement plus favorable, c'est-à-dire doté d'un capital social, culturel ou économique plus propice, sera mieux préparé, sensibilisé et performant. S. Esmer (2023)[26] reprend cette théorie en l'appliquant aux problématiques socioéconomiques du numérique. Selon lui, les inégalités ne résident plus uniquement dans l'accès aux technologies de l'information et de la communication (TIC), mais dans leurs usages. Les internautes issus de milieux favorisés disposent d'un capital numérique plus riche, leur offrant de meilleures conditions et opportunités d'usage, contrairement à ceux issus de milieux défavorisés : en effet, les personnes appartenant à des catégories socioprofessionnelles dites « supérieures » ont plus fréquemment recours à des outils numériques au quotidien, dans le cadre de leur travail, et sont donc à la fois familiarisés à des usages réguliers et renouvelés des outils numériques. Ils disposent également d'une plus grande culture de l'écrit, qui constitue toujours un point d'entrée important des usages numériques[27]. Les catégories sociales dont le profil se rapproche des concepteurs des espaces numériques[28] (sites, plateformes…) ont en outre une plus grande facilité à s'en emparer[29].

---

[22] M. Näsi, A. O. (2015, Avril 22). Cybercrime victimization among young people: a multi-nation study. *Journal of Scandinavian Studies in Criminology and Crime Prevention, 16*(2), pp. 203-210. doi:https://doi.org/10.1080/14043858.2015.1046640

[23] Plantard, P. (2021). *La fracture numérique : mythe ou réalité ?* Education Permanente.

[24] Smoreda, Z. B. (2007). *Saisir les pratiques numériques dans leur globalité.* doi:https://doi.org/10.3917/res.145.0019.

[25] Sen, A. (1997). Editorial: Human Capital and Human Capability. *World Development, 25*(12), pp. 1959-1961.

[26] Esmer, S. (2023). Evaluating the digital divide through Amartya Sen's capability approach. *STS Meets Ethics Conference Proceedings*, (pp. 165-175).

[27] Pasquier, D. (2022). Le numérique à l'épreuve des fractures sociales. *Informations sociales*, 205, 14-20.

[28] Akrich, M. (1998). Les utilisateurs, acteurs de l'innovation. *Éducation permanente*, 134, 79-90.

[29] Dares. (2019). *Data scientists, community managers... et informaticiens : quels sont les métiers du numérique?* Récupéré sur https://dares.travail-emploi.gouv.fr/publications/data-scientists-community-managers-et-informaticiens-quels-sont-les-metiers-du

En France, les data scientists sont plus souvent des moins de 38 ans (50 %), des hommes (77 %), diplômés (44 % de bac+5 ou plus), des cadres (61 %) vivant en Île de France (40 %). Ces données sont comparables à celles d'autres pays d'Europe : European Institute for Gender Equality. (2020). *Gender Equality Index 2020 : Digitalisation and the future of work.* Récupéré sur https://eige.europa.eu/publications-resources/toolkits-guides/gender-equality-index-2020-report/men-dominate-technology-development?language_content_entity=en

Ainsi, être une victime de cybercriminalité constitue un phénomène socialement situé, dont les déterminants peuvent **recouper des formes de victimation observables hors ligne** : l'âge, le genre, le niveau de revenus ou encore le contexte résidentiel ont une incidence sur les pratiques d'exposition et de protection. À ce titre, l'enquête du SSMSI sur le vécu et le ressenti en matière de sécurité[30], atteste d'une surexposition des **jeunes adultes**, de façon générale, aux atteintes personnelles qu'elles soient en ligne ou hors ligne : par exemple, les Français âgés de 18 à 24 ans auraient une probabilité 3 et 5 fois supérieure aux autres de déclarer avoir subi une violence sexuelle non physique ou une violence sexuelle physique.

Les résultats de l'enquête Conditions de Vie et Aspirations mettent aussi en évidence une surreprésentation des **adolescents et jeunes adultes et des personnes disposant de faibles revenus** parmi les victimes de cybercriminalité, dans la lignée de travaux antérieurs sur le sujet (notamment Näsi et al. (2015)[31]), de même que des **hommes**, et confortent **l'importance des usages** dans l'exposition aux risques.

2.3.A. Des pratiques numériques variées favorisent l'exposition à la cybermalveillance

L'enquête Conditions de Vie et Aspirations interroge l'échantillon sur son adoption de différents types d'usages numériques appelant chacun des expositions contrastées à différents risques :

- Les usages administratifs et organisationnels, comme les achats en ligne, l'accomplissement de démarches administratives, la recherche d'information et suivi de l'actualité sont monnaie courante chez 94 % des répondants.
- Les usages sociaux et de loisirs comme les jeux, la fréquentation des réseaux sociaux et l'abonnement à des services de VOD concernent 53 % des répondants
- Les usages économiques, principalement le travail au profit de son activité professionnelle ou de ses études sont réalisés par 35 % des répondants.

23 % des internautes sont concernés par **ces trois types d'usages** de manière simultanée. Les **15-24 ans** (46 %), les **diplômés du supérieur** (35 %) et les **hauts revenus** (31 %) et, dans une moindre mesure, les **hommes** (25 %) sont davantage concernés par ces usages diversifiés de numérique.

Cette **population aux pratiques numériques variées** est, toutes choses égales par ailleurs, **plus fréquemment victime de cyberattaques**, quel que soit le type et une fois contrôlées les variables mentionnées ci-dessus (âge, niveau de diplôme et de revenus, genre) ainsi que la taille d'agglomération de résidence.

La variété des usages accroît donc l'exposition aux risques, indépendamment des caractéristiques socioéconomiques. Ces caractéristiques ont cependant elles aussi un effet propre, mesuré dans le cadre des régressions réalisées, et notamment l'âge.

[31] Näsi et al. (2015), *op. cit.*
[31] Näsi et al. (2015), *op. cit.*

2.3.B. Les jeunes sont plus concernés

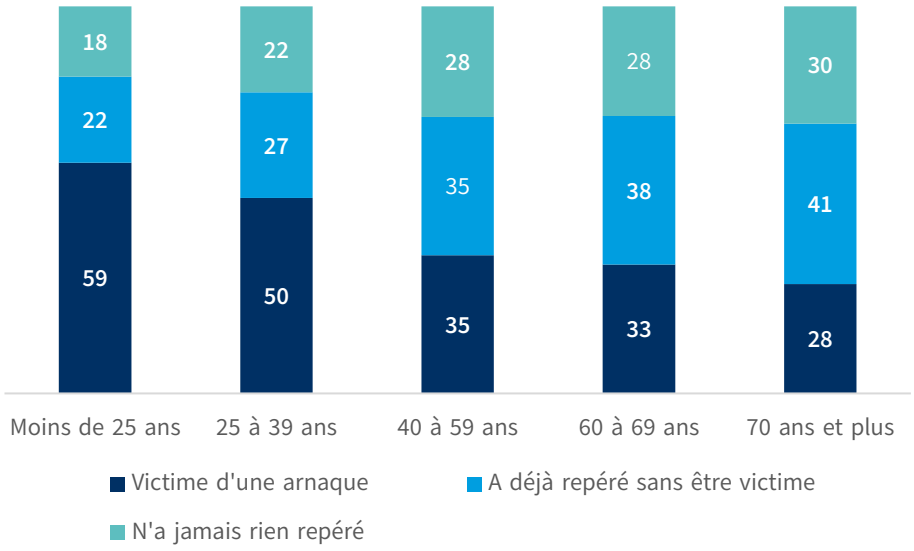
Les victimes de cyberattaques, tous types confondus, sont plus fréquemment les internautes âgés de **moins de 40 ans, et plus encore les moins de 25 ans**. Ils sont ainsi 59 % des 15 à 24 ans à déclarer avoir déjà été victimes de cyberattaques contre 35 % de leurs congénères de 40 à 59 ans.

Et cette spécificité **des jeunes de moins de 25 ans** perdure à la suite d'une analyse « toutes choses égales par ailleurs » (Figure A 2, page 42) que ce soit en considérant les actes de cybermalveillance dans leur ensemble ou isolément, un par un.

Graphique 3 – « Au cours des douze derniers mois, avez-vous été confronté aux situations suivantes sur internet ? »

Regroupement des cyberattaques par catégories d'âge

- Champ : ensemble de la population internaute de 15 ans et plus, en % - effectif total pondéré n : 3 473 -



Source : CREDOC, enquête Conditions de vie et aspirations juin 2025

Une enquête d'IPSOS (2024)[32] portant sur la sécurité numérique et réalisée pour la plateforme du gouvernement CyberMalveillance.gouv.fr brosse également le portrait de jeunes adultes, de 18-34 ans, comme victimes privilégiées de l'ensemble des cyberattaques listées[33].

Dans le détail, les jeunes adultes sont le plus souvent victimes d'escroqueries en ligne, 40 % d'entre eux ont déclaré en avoir été victimes durant les douze mois précédent l'enquête et 29 % pour les atteintes à l'identité.

Les jeunes adultes **manquent d'expérience en matière de cybersécurité**, celle-ci s'accroissant avec l'âge[34], et font souvent état d'un sentiment de manque de maîtrise technique ou de manque de

[32] IPSOS et cybermalveillance.gouv. (2024, Septembre). *Les Français et la sécurité numérique*.

[33] Virus informatique, comptes en ligne piraté, appel frauduleux d'un faux conseiller bancaire, utilisation frauduleuse de la carte bancaire, diffusion d'informations personnelles, menaces de publication de contenus intimes, appareil bloqué avec demande de rançon et virement pour une fausse facture

[34] M. Mahipal, N. S. (2025). Cybersecurity awarness among young adults: An analytical study. *International Symposium on Electronic Imaging*. doi:10.2352/EI.2025.37.3.MOBMU-312

compétences[35]. À partir de 18 ans, l'individu acquiert une pleine autonomie juridique et voit ses pratiques d'achat en ligne s'intensifier, ce qui accroît également son exposition aux risques de fraude. En 2024, selon l'Autorité des marchés financiers, 3.2 % de la population aurait spécifiquement été victimes d'une escroquerie sur un **placement financier,** en forte augmentation par rapport à 2021 (1.2 %)[36]. L'Autorité des marchés financiers (2024) constate que cette hausse des victimes potentielles est particulièrement marquée auprès des jeunes de 18-34 ans, dont **l'acceptation du risque plus élevée** (64 % contre 48 % de la population en moyenne) et une **confiance dans des sources d'informations moins officielles** comme provenant d'influenceurs (30 % contre 13 % de la population), d'avis ou discussions sur internet (39 % contre 20 % en moyenne) exposent à de forts risques.

Lorsqu'il s'agit d'usages exposant **leurs données personnelles**, les adolescents et jeunes adultes semblent en revanche disposer de **davantage d'expérience** pour développer une certaine sensibilisation et des méthodes de vigilance. Parmi la population de moins de 25 ans, 29 % ont été victimes d'une atteinte à leur identité, en ligne, mais 46 % ont réussi à s'en rendre compte à temps pour l'éviter.

2.3.C. Les personnes aux revenus modestes sont également plus souvent victimes

En parallèle de l'âge, le facteur du niveau de vie offre un autre déterminant de différenciation de victimisation (notamment par rapport aux personnes de la classe moyenne, voir Figure A 2). On trouve chez les personnes disposant de **faibles revenus**, un mécanisme similaire à celui des moins de 25 ans : le type de cyberattaque le plus fréquemment évité est l'atteinte à l'identité (16 % contre 8 % des classes moyennes supérieures).

Ce sont aussi la réception d'e-mails et appels frauduleux et les escroqueries en ligne à l'achat d'un produit dont ils déclarent le plus être victimes (respectivement 25 % et 19 %).

Enfin, ils sont les moins ciblés par les usurpations d'identités et les demandes de paiement ou rançon en échange de la récupération de données, photos ou contrôle de son appareil (respectivement 73 % et 71 % déclarent ne jamais avoir été confronté à de telles arnaques en ligne).

2.3.D. Les hommes davantage soumis à des risques

Le genre apparait comme un autre facteur discriminant. Des dynamiques de genre imprègnent bel et bien les usages du numérique. Ainsi, le baromètre du numérique montre de longue date l'appropriation prioritaire des nouvelles technologies par les hommes.[37] Ces derniers se distinguent par un profil plus

---

[35] ANCT, CREDOC, Université Rennes 2 CREAD-M@rsouin. (2023). *La société numérique française : définir et mesurer l'éloignement numérique.* https://www.credoc.fr/publications/la-societe-numerique-francaise-comprendre-les-freins-psychosociaux-a-lusage-du-numerique

[36] Autorité des Marchés Financiers. (2024). *Les arnaques à l'investissement.* Récupéré sur https://www.amf-france.org/sites/institutionnel/files/private/2024-12/amf-rapport-bva_arnaques-a-linvestissement_-version-publiable_19-dec.pdf

[37] Arcep, Arcom, CGE, ANCT, *op. cit.*.

technophile, vérifient moins les conditions générales d'utilisation des plateformes qu'ils utilisent et font état de moins de craintes à l'égard de l'usage des outils numériques[38].

Sur le plan des risques, les données de l'enquête Conditions de Vie et Aspirations révèlent une plus forte probabilité pour les **hommes d'être victimes de la découverte d'un logiciel malveillant ou d'un virus** sur l'un de leurs appareils (14 % des hommes vs. 11 % des femmes) et d'une demande de paiement ou demande de **rançon** en échange de la récupération de données, de photos ou de contrôle de leur appareil (11 % des hommes vs. 10 % des femmes). Ces écarts, bien que faibles, sont statistiquement significatifs et résistent à une analyse « toutes choses égales par ailleurs » : à âge, niveau de diplôme et de revenus, taille d'agglomération de résidence et variété des pratiques numériques identiques, les hommes sont plus susceptibles d'être victimes de ces actes cybermalveillants.

Les hommes indiquent également avoir pu réaliser à temps être en présence d'un acte de cybermalveillance sur l'ensemble des items proposés, davantage que les femmes.

L'enquête d'Ipsos[39] pointe également une surexposition des jeunes hommes à l'ensemble des cyberattaques, et particulièrement aux virus informatiques ou les utilisations frauduleuses de la carte bancaire par rapport aux femmes du même âge.

L'AMF identifie en outre une plus grande confiance dans leur expertise en matière de placement financier et une habitude à prendre les décisions seuls comme exposant davantage les hommes à des arnaques aux placements financiers sur Internet[40].

2.4. L'identification à temps des actes de cybermalveillance, des profils similaires aux victimes

Le repérage à temps des actes de cybermalveillance est lui aussi corrélé aux caractéristiques sociodémographiques des individus : l'âge, le niveau de diplôme et de revenus et le genre apparaissent particulièrement déterminants, tout comme la variété des usages numériques pratiqués. La réalisation d'une régression logistique, ou analyse « toutes choses égales par ailleurs », confirme l'effet propre de ces caractéristiques.

Ainsi, les **hommes repèrent mieux** la totalité des actes de cybermalveillance listés, à l'exception de e-mails ou appels frauduleux, avant d'en être victimes. De manière similaire, les **moins de 40 ans** décèlent davantage l'ensemble des actes de cybermalveillance, à l'exception des e-mails ou appels frauduleux que les 70 ans et plus identifient plus souvent à temps, toutes choses égales par ailleurs. Ces deux catégories de la population confirment ainsi leur exposition à ces risques : elles en sont davantage victimes et, pour celles ne l'étant pas, témoignent davantage d'une identification d'un risque potentiel qu'elles sont parvenues à écarter.

[38] ANCT, CREDOC, Université Rennes 2 CREAD-M@rsouin, *op. cit.*
[39] IPSOS (2024), *op cit*
[40] Autorité des Marchés Financiers. *op.cit.*

Les **diplômés du supérieur** évoquent plus souvent le repérage à temps d'e-mails ou appels frauduleux, de logiciels malveillants ou virus, d'escroquerie lors de l'achat d'un service, d'escroquerie bancaire ou de demande de paiement. Cette vigilance s'étend aux personnes de niveau bac pour les tentatives de piratage d'un compte de réseau social ou d'une boîte mail.

Le revenu a une incidence propre plus marginale au niveau de l'identification des risques. Les bas revenus déjouent plus facilement les tentatives d'usurpation d'identité, toutes choses égales par ailleurs.

Enfin, le repérage des e-mails et appels frauduleux et des logiciels malveillants ou virus sans en être victimes est davantage le fait de personnes ayant des **pratiques numériques diversifiées** (de loisirs mais aussi organisationnelles et professionnelles).

La probabilité d'être victime d'un acte de cybermalveillance est donc lié à des usages diversifiés, mais aussi à des représentations du risque pouvant varier selon les catégories de la population. Les plus jeunes et les hommes sont toutes choses égales par ailleurs plus victimes des arnaques et fraudes sur internet mais aussi plus nombreux à identifier les risques à temps pour les déjouer. Les personnes à faibles revenus sont en revanche plus nombreuses à être victimes, sans identifier massivement les risques en présence à temps.

3. 88% des internautes Français disent prendre des précautions face à la cybercriminalité

3.1. Une vigilance en hausse

La forte exposition à des risques numériques constatée dans l'étude est d'autant notable qu'en 2025, **88 % des internautes Français de 15 ans et plus déclarent prendre des précautions** quand ils utilisent internet, soit en renonçant à certains usages d'internet, soit en faisant preuve de vigilance.

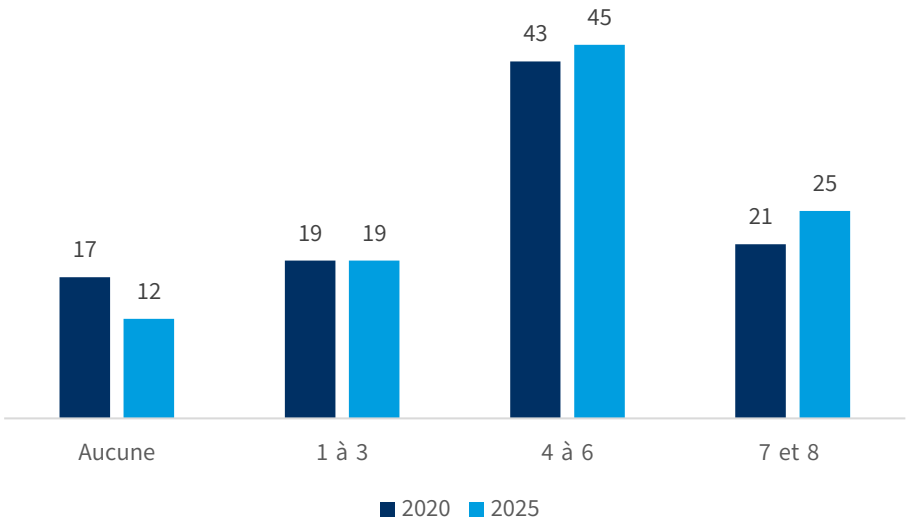
Alors qu'en 2020, 17 % des internautes déclaraient n'avoir adopté aucune mesure de précaution parmi la liste proposée, ils ne sont plus que 12 % en 2025. Cette hausse des comportements de prudence est surtout le fait des internautes **les plus experts**, utilisant sept ou huit types de précautions. Au total, on mesure en moyenne une hausse de +0,4 précautions prises par les internautes depuis 2020.

Cette hausse déclarée des précautions prises par nos concitoyens est à mettre en regard de **l'essor des cybermenaces documenté par la Cour des comptes**[41] dans leur rapport d'observation sur « La réponse de l'Etat aux cybermenaces sur les systèmes d'information civils ».

Graphique 4 – « Il est possible de prendre certaines précautions ou d'adopter certains comportements quand on utilise internet. Vous, personnellement, avez-vous déjà … »

Par nombre de précautions prises

- Champ : ensemble de la population internaute de 15 ans et plus, en % - effectif total pondéré n : 3 473 -



Source : CREDOC, enquête Conditions de vie et aspirations juin 2025

Les actions de renoncement et vigilance listées dans l'enquête Conditions de vie et Aspirations du Crédoc couvrent une large diversité d'actions plus ou moins contraignantes passant par le simple refus

[41] Cour des comptes. (2025). *La réponse de l'Etat aux cybermenaces sur les systèmes d'information civils.*

de partager sa localisation à la souscription à un service de sécurisation de paiement en ligne (Graphique 5).

Les types de précaution les plus fréquemment utilisés ont connu des variations plus ou moins importantes depuis 2017 avec en premières occurrences, **le renoncement à un achat pour manque de confiance au moment du paiement** (70 % des internautes Français en 2025 et 67 % en 2020 et 61 % en 2017) et **le refus de géolocalisation sur internet** (68 % des internautes Français en 2025, 70 % en 2020 et 67 % en 2017).

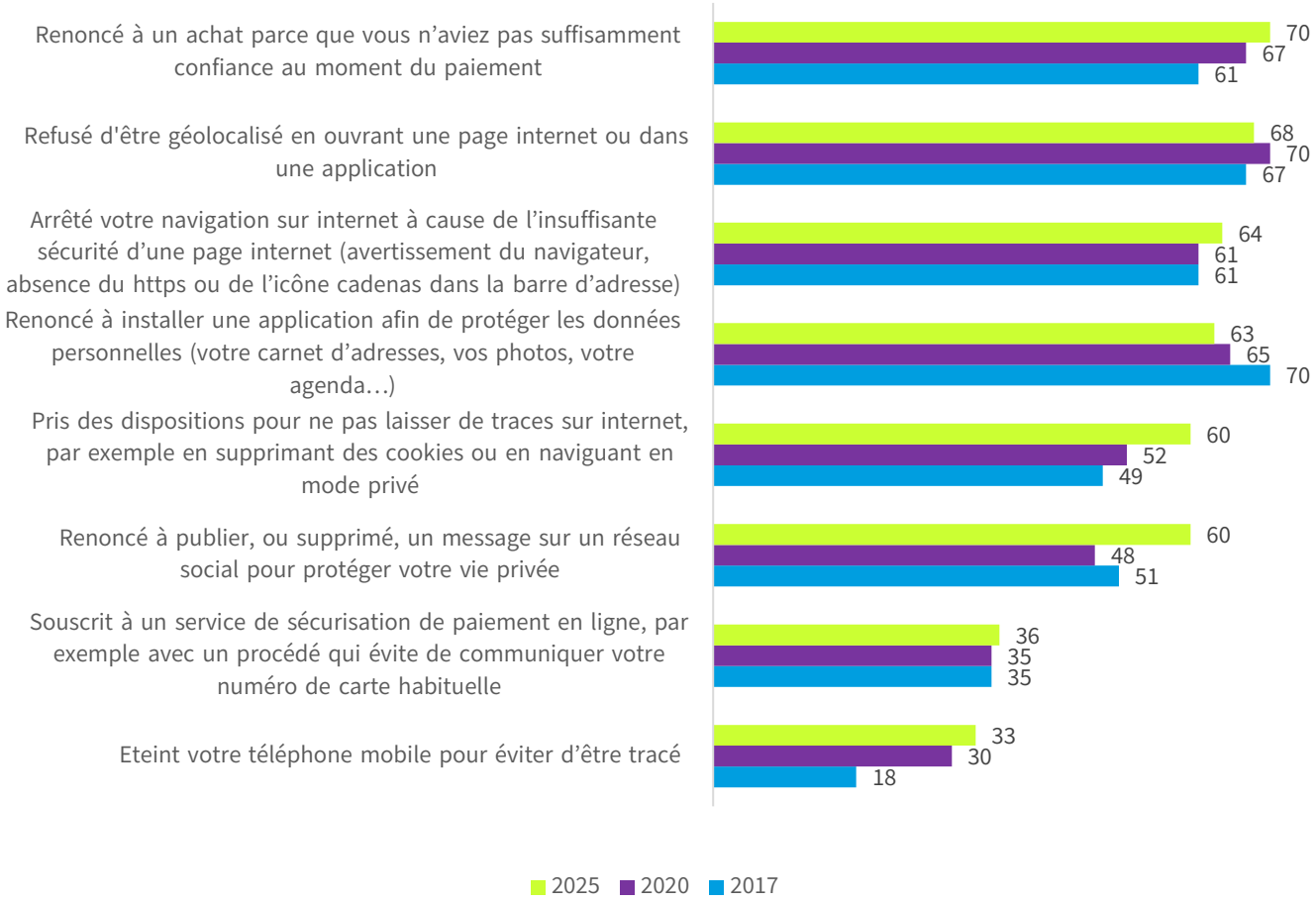
On observe, sur certains types de précaution, **des hausses significatives**, comme pour la prise de dispositions pour **ne pas laisser de traces sur internet** (+ 8 points entre 2020 et 2025), le **renoncement à publier ou la suppression de message sur les réseaux sociaux** pour protéger sa vie privée (+ 12 points sur la même période), ou le fait **d'éteindre son téléphone mobile** pour éviter d'être tracé (+ 15 points entre 2017 et 2025).

En particulier, en 2021, les internautes de **18 à 24 ans** étaient 57 % à déclarer renoncer à publier ou supprimer un message sur leur réseau social alors qu'ils sont 68 % en 2025. Le même mécanisme s'est opéré chez les internautes **diplômés du supérieur** qui étaient 51 % à déclarer renoncer à publier ou supprimer un message sur leur réseau social en 2021 et qui sont maintenant 64 % en 2025.

Le classement des types de précaution les plus utilisés a, également, connu quelques changements notables, notamment, le renoncement à installer une application afin de protéger ses données personnelles qui arborait la première place en 2017, la deuxième place en 2020 continue de perdre des places pour se retrouver en 2025, à la quatrième position. Le renoncement à l'achat d'un bien pour manque de confiance au moment du paiement de son côté, ne cesse de gagner en popularité depuis 2017 où il était placé à la troisième position ex-aequo avec l'arrêt de navigation sur internet à cause de l'insuffisante sécurité d'une page internet, puis s'est hissé en 2020 à la deuxième place pour finir à la première en 2025.

Graphique 5 – « Il est possible de prendre certaines précautions ou d'adopter certains comportements quand on utilise internet. Vous, personnellement, avez-vous déjà … »

- Champ : ensemble de la population internaute de 15 ans et plus, en % - effectif total pondéré n : 3 473 -



Source : CREDOC, enquête Conditions de vie et aspirations juin 2017, septembre 2020 et juin 2025

3.2. Avoir déjà été victime, avoir des usages numériques diversifiés, induit une vigilance accrue

L'Eurobaromètre spécial 499 (2019)[42] indique que les Français sont un peu plus inquiets qu'en moyenne face à l'utilisation de leurs données personnelles sur internet, puisque 49 % des Français sont inquiets que quelqu'un utilise leurs données personnelles de manière abusive (contre 46 % de l'ensemble des Européens en moyenne). Cette préoccupation se reflète dans le fait que les deux principales mesures de précaution adoptées par les Français visent en priorité la protection de leurs données. Cependant, la crainte de la cybercriminalité ne constitue pas un facteur déterminant, toutes choses égales par ailleurs, pour expliquer la prise de précautions en ligne (voir Figure A 3, page 51). Notre analyse permet de mettre en évidence en revanche, le **rôle central de la victimisation** dans l'explication des comportements.

[42] Commission Européenne. (2019). *op.cit.*

Nous avons analysé la probabilité de changer de comportement est analysée selon des variables similaires : l'expérience (avoir été victime d'arnaque en ligne ou non), l'inquiétude face à la cybercriminalité, les compétences numériques déclarées des internautes et d'autres variables sociodémographiques.

Les individus ayant déjà été **victimes de cyberattaques** au cours des douze derniers mois sont **92 % à déclarer mettre en place au moins un acte de vigilance** contre 73 % de ceux qui n'ont pas été victimes. De même, ils sont **95 % à déclarer renoncer** à au moins un usage d'internet contre 78 % des internautes qui n'ont jamais été victimes.

Encadré

Ces résultats pourraient sembler contradictoires avec l'étude de R. Böhme (2012)[1] sur la réaction des consommateurs face aux cyberattaques. Il montre en effet que l'inquiétude de la cybercriminalité entraine un changement de comportement chez les internautes pour s'en protéger. Alors que nos résultats révèlent pour leur part que, toutes choses égales par ailleurs, l'inquiétude de la cybercriminalité ne constitue pas un facteur de changement de comportement (caractérisé par des actes de vigilance et de renoncement).

R. Böhme analyse la probabilité de changer de comportement (à l'achat de produit et envers l'usage de banque en ligne) selon des variables d'expérience (avoir été victime ou non), d'inquiétude face à la cybercriminalité, d'exposition aux arnaques, de compétences du numérique et des variables constantes. Une piste possible pour expliquer la divergence réside donc plutôt dans la construction de nos variables respectives. R. Böhme a créé son indicateur de compétences numériques à partir d'éléments qui relèvent déjà de ce que nous considérons dans notre méthode, des *pratiques de précaution* (par exemple, la gestion des mots de passe ou l'utilisation d'un antivirus). Ainsi une partie de l'effet qu'il attribue à l'inquiétude pourrait être renforcée par une redondance entre les caractéristiques des compétences et du changement de comportement. Dans notre étude, les variables sont distinguées plus nettement : les compétences numériques sont auto-déclarées (ce qui n'en constitue pas moins une limite bien entendu), tandis que les actes de vigilance et de renoncement représentent le changement de comportement. Cette distinction nous permet de mettre en évidence le rôle central de la victimisation dans l'explication des comportements, contrairement à R. Böhme où l'inquiétude, ainsi renforcée par la variable des compétences numériques occupe une place plus importante.

Tout de même, on retrouve dans son étude, des mécanismes similaires à ce que l'on trouve dans l'analyse de notre enquête, selon lesquels la sensibilisation à la cybercriminalité et la victimisation sont des facteurs qui augmentent la probabilité de modifier le comportement des internautes sur internet.

La victimisation est aussi corrélée, toutes choses égales par ailleurs, avec une plus grande capacité de **repérage** des arnaques en ligne.

Autre facteur augmentant la vigilance : 53 % des internautes utilisant **tous les types d'usages** décrits dans la section précédente (loisirs et réseaux sociaux ; administratifs ou organisationnels ; économique) sont très précautionneux. De plus, ne jamais se connecter à internet ou d'en avoir un usage rare est

associé à un niveau de précaution (vigilance) plus faible, toutes choses égales par ailleurs. Les individus se déclarant **très compétents** avec l'usage des plateformes en ligne sont aussi plus fréquemment des utilisateurs très précautionneux (44 %), toutes choses égales par ailleurs.

3.3. La vigilance ne va pas de pair avec la protection

Contre toute attente, les internautes les **plus vigilants** ont, toutes choses égales par ailleurs, une **probabilité plus importante d'être victime de cyber arnaques**. Notre analyse se heurte ici à une limite, les propositions de précautions prises dans ce questionnaire ne permettent pas de contrer tous les types d'attaques proposés. Les précautions portent plus sur la protection des données privées que sur la riposte des arnaques de réception d'e-mails ou d'appels frauduleux, d'usurpation d'identité ou de demande de paiement ou rançon en échange de données ou du contrôle d'un appareil. On remarque par exemple que les individus les plus précautionneux dans leurs usages d'internet sont moins nombreux à déclarer renoncer à un achat parce qu'ils n'avaient pas suffisamment confiance au moment du paiement. Ils ne sont que 58 % à déclarer avoir recours à ce type de précaution alors qu'ils sont 74 % à éteindre leur téléphone mobile pour éviter d'être tracé. Et ce, alors que les escroqueries à l'achat d'un produit se positionnent à la deuxième place des arnaques les plus récurrentes.

En outre, nous ignorons le sens de la corrélation : les personnes vigilantes le sont-elles parce qu'elles ont déjà été victimes ou leur vigilance préexistante n'a-t-elle pas suffi à les protéger ?

3.4. Des précautions plus élevées chez les plus diplômés, les femmes

Nous avons distingué deux grandes catégories de précaution, en regroupant les différents types d'action étudiées dans notre enquête :

Des précautions que nous avons appelé **de vigilance** : *refus d'être géolocalisé en ouvrant une page internet ou dans une application, éteindre son téléphone mobile pour éviter d'être tracé, prendre des dispositions pour ne pas laisser de traces sur internet par exemple en supprimant des cookies ou en naviguant en mode privé, souscrire à un service de sécurisation de paiement en ligne, par exemple avec un procédé qui évite de communiquer le numéro de carte habituelle*.

Des précautions qui relèvent du **renoncement** : *renoncer d'installer une application afin de protéger ses données personnelles (carnet d'adresses, photos, agenda …), renoncer à un achat pour manque de confiance au moment du paiement, renoncer à publier ou supprimer un message sur un réseau social pour protéger la vie privée, arrêter la navigation sur internet à cause de l'insuffisante sécurité d'une page internet (avertissement du navigateur, absence du https ou de l'icône cadenas dans la barre d'adresse)*.

De manière générale, les internautes ont **un peu plus tendance à renoncer à certains usages d'internet** (84 %) tels que renoncer à un achat pour manque de confiance au moment du paiement (70 %), qu'à adopter des comportements de vigilance (81 %) comme éteindre son téléphone mobile pour éviter d'être tracé (33 %).

Ce phénomène s'explique par plusieurs facteurs : des ressources financières limitées, un niveau de compétences insuffisant, ou encore un manque de temps et de motivation pour investir l'énergie nécessaire à la sécurisation des pratiques numériques.

Il s'ancre aussi dans des pratiques dépassant le cadre de la vie en ligne. Ainsi, les **femmes** sont, toutes choses égales par ailleurs, plus enclines à déployer des actions de vigilance par rapport aux hommes, ce qui renvoie à des dynamiques de **prise de risques** genrées.

Les actes de renoncement sont plutôt répartis de manière équivalente le long de la distribution de l'âge. Lorsqu'on compare les catégories les plus touchées par les cyberattaques, les internautes de **moins de 25 ans** se distinguent plutôt par un fort taux de vigilance (87 %) plutôt que de renoncement à des pratiques.

3.5. Les plus diplômés sont plus vigilants, les bas revenus moins

Les **non diplômés sont les moins précautionneux** avec 73 % qui utilisent des méthodes de vigilance et 75 % qui renoncent à certains usages (vs 81 % et 84 % en moyenne).

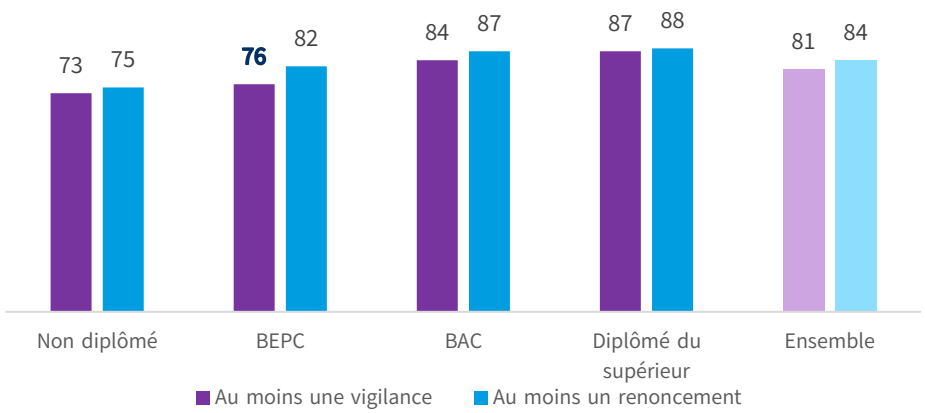
Les **moins diplômés** font aussi partie de ceux qui sont le moins fréquemment victimes, ils sont ainsi moins concernés par les attaques en ligne que les plus diplômés, justifiant en partie leurs plus faibles taux de vigilance et renoncement des usages. Mais ils se disent aussi, en moyenne, **moins compétents dans le numérique**, et ne peuvent donc se protéger de manière équivalente. En effet, les plus compétents dans le numérique ont plus de probabilité d'être vigilants sur internet, toutes choses égales par ailleurs.

D'un autre côté, les **plus diplômés** sont plus au courant des cyberattaques et des pratiques pour les éviter, les incitant à changer leur comportement.

Graphique 6 – « Il est possible de prendre certaines précautions ou d'adopter certains comportements quand on utilise internet. Vous, personnellement, avez-vous déjà … »

Regroupement en actes de vigilance ou renoncement (par type de diplôme)

- Champ : ensemble de la population internaute de 15 ans et plus, en % - effectif total pondéré n : 3 473 -



Source : CREDOC, enquête Conditions de vie et aspirations juin 2025

La population à **faibles revenus** apparait peu encline à renoncer à certains usages d'internet (81 % contre 84 % de l'ensemble de la population) ou adopter des comportements de vigilance sur internet (78 % contre 85 % des hauts revenus). L'enquête des TIC de l'Insee (2019)[43] confirme que les individus avec un revenu parmi les 20 % les plus faibles sont ceux qui ont moins tendance à limiter ou arrêter des activités en ligne à cause de leurs craintes sur la sécurité. Ils seraient 74,7 % contre 80,9 % des plus aisés.

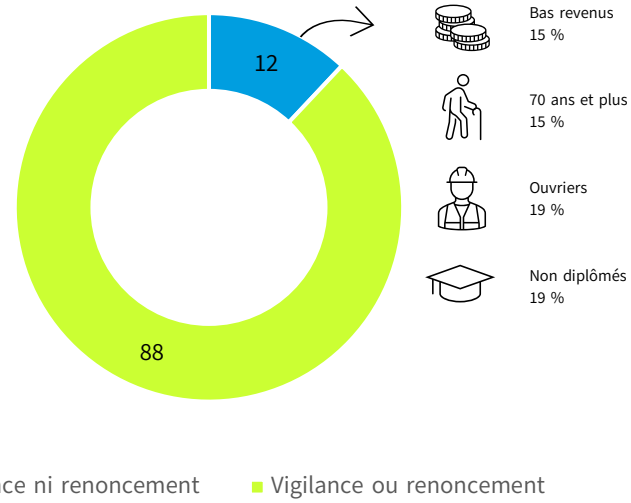
Les individus à **faibles revenus** montrent significativement le plus faible taux d'actes de vigilance alors qu'ils **font parmi des victimes les plus récurrentes** de cyberattaques. La théorie d'environnement capacitant de Amartya Sen (1997)[44] permet de formuler une hypothèse expliquant ce phénomène. En effet, bien que les individus à bas revenus possèdent un accès similaire à internet que les autres, cet environnement ne leur est pas capacitant. En clair, bien qu'ils se déclarent très compétents dans l'usage du numérique, la cybersécurité reste un enjeu primordial. Lorsqu'il leur est posé la question : « *On peut parfois se sentir dépassé par les évolutions rapides des technologies numériques, sur quels sujets liés au numérique et Internet souhaiteriez-vous avoir de l'aide pour améliorer votre vie quotidienne ?* » en excluant les personnes déclarant ne pas avoir besoin d'aide, la majorité des répondants citent « *La sécurité numérique (fraudes et arnaques sur internet*) » comme le domaine dans lequel ils souhaiteraient être accompagnés par rapport aux autres réponses (*l'intelligence artificielle, l'accompagnement à l'utilisation du numérique des enfants, l'usage des réseaux sociaux et des outils de communication numérique, la prise en main des équipement numériques*). Suivant la reprise de la théorie d'environnement capacitant de Sen adaptée au « digital divide » par S. Esmer (2023)[45], les internautes à bas revenus font partie de ces internautes pour qui l'accès aux compétences du numérique est moins évident.

Graphique 7 – « Il est possible de prendre certaines précautions ou d'adopter certains comportements quand on utilise internet. Vous, personnellement, avez-vous déjà … »

Regroupement en actes de vigilance et renoncement

- Champ : ensemble de la population internaute de 15 ans et plus, en % - effectif total pondéré n : 3 473 -

[43] Insee. (2025, Avril 14). *Enquête sur les technologies de l'information et de la communication*.
[44] Sen, A. (1997). *Op.cit.*
[45] Esmer, S. (2023). *Op. cit.*.



Source : CREDOC, enquête Conditions de vie et aspirations juin 2025

Concernant les connaissances en cybersécurité, on émet souvent en premier lieu l'hypothèse de transmission par les pairs. Les résultats de l'enquête nous permettent d'ajuster cette hypothèse puisque les internautes se sentant exclus ont une probabilité plus élevée d'être vigilants toutes choses égales par ailleurs. Cette vigilance a probablement été motivée par la **victimisation**, les internautes qui se sentent **exclus** ont une probabilité plus importante d'être **victimes** de cyberattaques. La vigilance n'est ainsi pas seulement diffusée par les pairs mais aussi par le fait d'avoir, soi-même, été victime d'une fraude ou arnaque en ligne.

Ces résultats s'inscrivent dans la lignée de notre précédent cahier de recherche sur « L'escroquerie en ligne et à la téléphonie en France » de 2021[46], où les catégories prenant le plus de précaution sur internet étaient déjà les jeunes adultes (**18-24 ans**), les **diplômés du supérieur** et ceux déclarant avoir **déjà été concernés** par les cyberattaques (victimes ou repérées). Notre apport à ces résultats antérieurs réside dans le fait que, toutes choses égales par ailleurs, les **femmes** sont plus vigilantes, et en ce que les **bas revenus** sont particulièrement moins vigilants.

[46] CREDOC. (2021). *L'escroquerie en ligne et à la téléphonie en France.* Cahier de recherche. URL : https://www.credoc.fr/publications/lescroquerie-en-ligne-et-a-la-telephonie-en-france-ampleur-du-phenomene-et-profils-des-victimes

4. Les conséquences de la cybercriminalité

Lorsqu'une personne est victime d'une arnaque ou d'un acte malveillant sur internet, quelles sont ses réactions et quelles répercussions ces actes ont-ils d'un point de vue psychologique ?

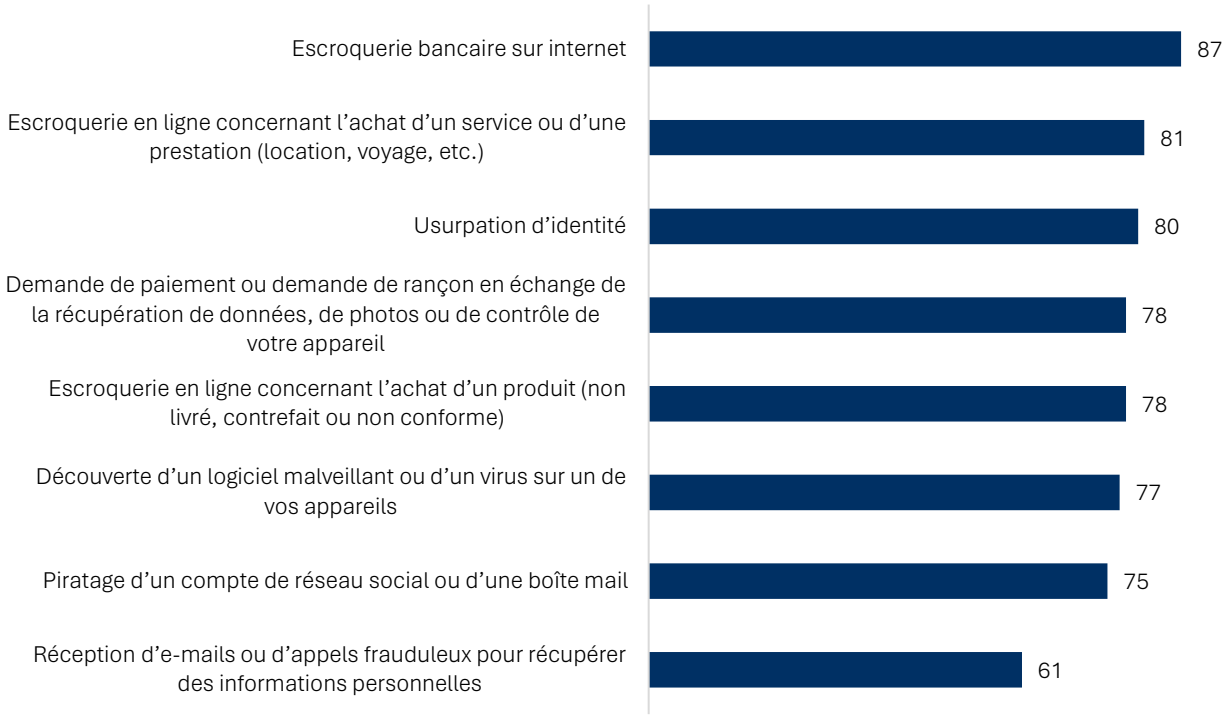
4.1. Les victimes d'escroqueries bancaires sur internet engagent davantage de démarches de recouvrement

Le niveau des réactions est plus élevé dès lors que la personne en a été victime : 66 %, alors que ceux qui n'ont subi que des tentatives (et qui ont pu intervenir avant qu'il y ait préjudice) ne réagissent « que » dans 27 % des cas.

En particulier, au sein des victimes, les internautes victimes d'escroqueries bancaires sur internet ont davantage tendance à déclarer engager des démarches de recouvrement (87 % des victimes) que les victimes de réception d'e-mails ou d'appels frauduleux ou le piratage d'un compte de réseau social ou d'une boîte e-mail (respectivement 61 % et 75 %). Cette tendance reste stable par rapport à 2021 comme nous avons pu le mettre en lumière avec le précédent cahier de recherche sur « L'escroquerie en ligne et à la téléphonie en France »[47].

Graphique 8 –Niveau de réaction des victimes selon les différents types d'arnaque

- Champ : population victime de cyberattaques âgés de 15 ans et plus (39% de la population internaute), en % -



Source : CREDOC, enquête Conditions de vie et aspirations juin 2025

[47] CREDOC. (2021). *Ibid.*

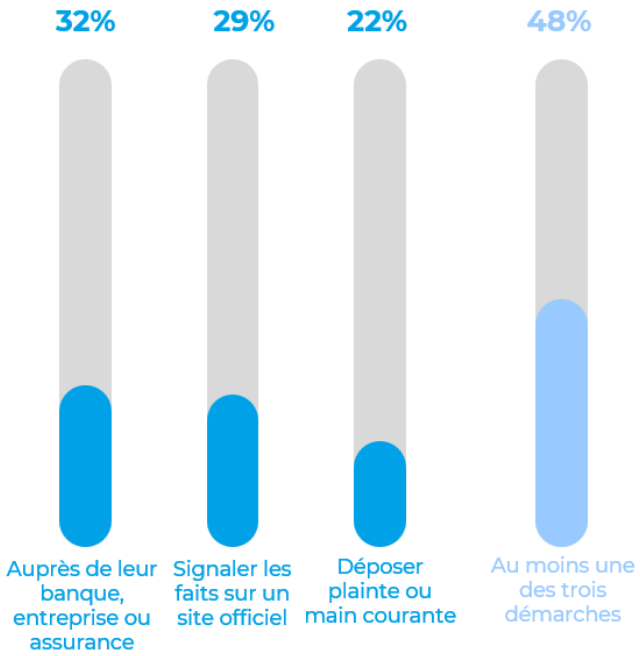
4.2. Moins d'une victime ou cible sur deux a entamé des démarches et recours, les jeunes, les femmes et bas revenus sont plus actifs

Au total, **48 % des victimes ou cibles**, soit moins d'une personne sur deux, déclarent avoir entamé des démarches et recours après avoir été victime de cyberattaque. Trois types de recours ont été mesurés.

Une minorité de victimes ou cibles a recours à des **démarches de recouvrement** afin d'obtenir gain de cause à la suite du préjudice subi. 32 % tentent ainsi d'obtenir réparation auprès des banques, des entreprises et assurances (Graphique 9), les victimes ont davantage tendance à utiliser ce recours (48 %) que les cibles n'ayant subi que des tentatives (14 %). Ce résultat est convergent avec d'autres travaux : selon Interstats, en 2019[48], seulement 27 % des victimes d'arnaques ont effectué une demande d'indemnisation auprès d'un tiers.

Graphique 9 – « À la suite de ces arnaques, avez-vous réalisé les démarches suivantes ? »

- Champ : population de 15 ans et plus victime ou cible d'au moins une arnaque ou tentative d'arnaque au cours des douze mois précédents l'enquête (74 % de l'ensemble des internautes), en % -



Source : CREDOC, enquête Conditions de vie et aspirations juin 2025

29 % des victimes et des personnes ciblées se sont donné la peine de signaler les faits **sur un site officiel** (39 % des victimes contre 18 % des internautes ciblés). Les **dépôts de plainte** ou de main courante en gendarmerie ou poste de police sont plus rares encore, elles concernent seulement 33 % des victimes et 8 % cibles.

On observe que les **femmes** qui ont été victimes d'arnaques ou fraudes en ligne vont significativement plus fréquemment effectuer des démarches de recouvrement auprès des banques, assurances ou

[48] Interstats. (2019). *Plus de la moitié des arnaques passent par internet - Analyse N°21.*

entreprises que les hommes (34 % contre 30 % des hommes). R. Dennehy (2020)[49] et l'Autorité des Marché Financiers (2024)[50] expliquent le faible taux de démarches à la suite de cyberattaques pourrait aussi venir de **la honte et le sentiment de vulnérabilité et faiblesse** qu'il provoque chez les victimes. Les **jeunes hommes**, particulièrement, voulant apparaître « capables et forts », ont moins tendance à aller demander de l'aide. Ces tendances sont entretenues par les réseaux sociaux et les idéaux masculins qui y circulent.

Le SSMSI (2023)[51] a mis en avant le **fatalisme de la population face aux arnaques frauduleuses en ligne** : la déclaration à la suite d'une arnaque est jugée « *inutile* » par 67 % des Français. Tandis que parmi les individus n'ayant pas signalé les faits dans le cas de vols et tentatives de vol avec effraction dans les logements, ils sont seulement 37 % à déclarer que cela n'aurait servi à rien. La population a probablement le sentiment que l'immatérialité de l'arnaque rend plus incertaine l'issue donnée à une plainte.

Les auteurs de cyberattaques étant souvent **anonymes**, il est difficile de les identifier. Les Français estiment ainsi plus souvent qu'il est vain de réaliser les démarches de recouvrement pour les cyberattaques contrairement aux délits physiques (vols, agressions…) où l'auteur des faits est identifiable plus facilement. Au sein de l'enquête du SSMSI (2023)[52] ce sont 52 % des victimes de vols ou tentatives de vol avec effraction qui ont déposé plainte ou fait une déclaration de type main courante contre 18% pour les victimes d'escroqueries bancaires et 16 % pour les victimes de débits frauduleux.

L'Eurobaromètre spécial 499 (2019)[53] met en lumière **la méconnaissance des sites officiels** pour rapporter des cyberattaques par le grand public, expliquant ainsi en partie la faible quantité de démarches réalisées. Il soulève aussi un mécanisme contre-intuitif, à la question suivante : « *Que vous ayez été victime ou non d'un cybercrime, que feriez-vous si vous vous retrouviez dans l'une des situations suivantes ou en deveniez victime ?* », pour chacune des cyberattaques listées entre 65 % et 92 % des individus répondent qu'ils entreprendraient au moins une des démarches. Avec en tête de liste, les fraudes bancaires (92 %) ainsi que l'usurpation d'identité (91 %) et en dernière position la réception d'e-mail ou appels frauduleux (66 %).

A. Almansoori (2023)[54] documente l'écart entre les intentions et les comportements adoptés par les internautes. Elle se base sur la théorie des comportements planifiés (« Theory of Planned Behavior ») qui met en avant l'effet des normes sociales, du contrôle perçu et de la perception des coûts et bénéfices. Concernant la cybersécurité, les intentions de comportements sont influencées par les normes sociales, les conseils de cybersécurité étant diffusés massivement. Seulement, les comportements réels ne **suivent pas toujours les intentions, à cause d'un manque de compétences**, à cause des **coûts en temps et en efforts perçus trop élevés**. L'écart entre les actions et les intentions

[49] R. Dennehy, S. M. (2020, Février 15). The psychosocial impacts of cybervictimisation and barriers to seeking social support: Young people's perspectives. *Children and Youth Services Review*. doi:10.1016/j.childyouth.2020.104872

[50] Autorité des Marchés financiers. (2024). *Op. cit.*.

[51] SSMSI. (2023). *Vécu et ressenti en matière de sécurité: Victimation, délinquance et sentiment d'insécurité.*

[52] SSMSI. (2023). *Ibid.*

[53] Commission Européenne. (2019). *Op.cit..*

[54] A. Almansoori, M. A.-E. (2023). Exploring the frontiers of cybersecurity behavior: A systematic review of studies and theories. *Applied Sciences, 13*. doi:10.3390/app13095700

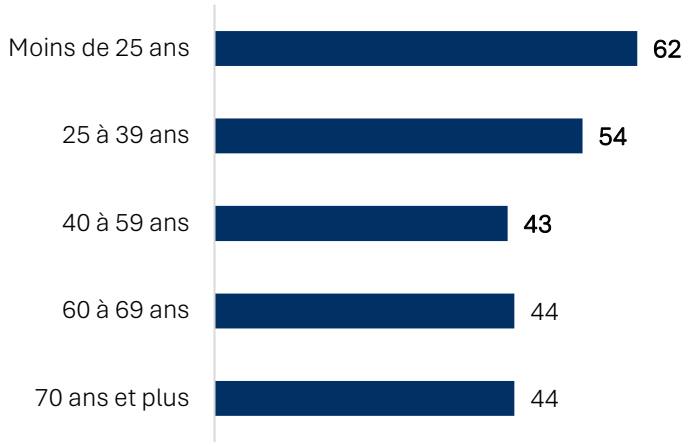
est également due à des biais comportementaux tels que **la procrastination, les excès de confiance, ou la normalisation des risques.**

Sauf chez les moins de 40 ans et les bas revenus, où les réactions sont majoritaires

On observe des différences significatives dans les recours et démarches selon les catégories d'âges (Graphique 10). Une majorité des **jeunes adultes** de moins de 40 ans (exactement 62 % des moins de 25 ans et 54 % des 25 à 39 ans) effectuent au moins une démarche ou un recours après avoir été victimes ou cibles d'arnaques ou fraudes en ligne, contre seulement 43 % des 40-59 ans. Les moins de 25 ans ont plutôt tendance à **signaler les faits sur internet** (42 %) alors que les 25-39 ans sont plus nombreux à demander **réparation auprès de leur banque, entreprise ou assurance** (37 %).

Graphique 10 – Les victimes les plus jeunes sont les plus réactives

- Champ : population de 15 ans et plus qui ont été victime ou cible d'au moins une arnaque au cours des douze mois précédents l'enquête (74 % de l'ensemble des internautes), en % ayant fait au moins une démarche à la suite de ces arnaques -



Source : CREDOC, enquête Conditions de vie et aspirations juin 2025

On remarque que les internautes de **moins de 40 ans** sont également ceux qui, toutes choses égales par ailleurs, accordent le plus de **confiance à la justice** (11 % des moins de 25 ans et 12 % des 25 à 39 ans contre 8 % de l'ensemble de la population. Et le recours aux démarches de recouvrement est plus fréquent chez les internautes qui ont confiance dans l'action de la justice, cette confiance les confortant dans l'idée qu'ils ont de réelles chances d'obtenir réparation. Toutes choses égales par ailleurs, avoir **confiance dans la justice** est lié à une probabilité plus élevée d'avoir recours à des démarches de recouvrement.

Concernant les internautes à **bas revenus**, ils peuvent se trouver plus motivés à effectuer des démarches de recouvrement à cause du **poids significativement plus important dans leurs ressources pour un même montant extorqué** que les catégories avec de plus hauts revenus. En effet, les internautes à qui il arrive de devoir s'imposer régulièrement des restrictions sur le budget ont une probabilité supérieure aux autres de faire des demandes de recouvrement à la suite d'arnaques et fraudes en ligne. Bien qu'ils ne fassent pas partie des catégories qui font le plus confiance à la justice cependant, les restrictions de budget sont un élément suffisant pour les motiver à demander réclamation.

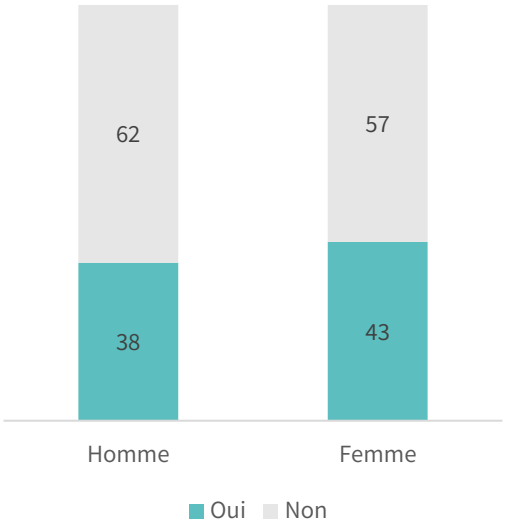
4.3. Des répercussions psychologiques fréquentes

Parmi les victimes d'arnaques ou fraudes en ligne et ceux qui ont réussi à y échapper, **41 % déclarent avoir été affectés psychologiquement** à la suite de ces événements. L**es personnes effectivement victimes sont davantage touchées (56 %) que celles qui ont réussi à parer l'attaque (22 %)**. Mais, même chez celles-ci, une sur cinq témoigne d'un contrecoup psychologique.

L'enquête du SSMSI (2023)[55] mesure un taux similaire : en moyenne 53 % des personnes victimes d'une atteinte non physique à la personne perpétrée par téléphone/ sms, courriel, réseaux sociaux ou autre site web ou moyen numérique, déclarent avoir eu des dommages psychologiques plutôt et très importants.

Graphique 11 – « À la suite de ces arnaques, avez-vous été affecté.e psychologiquement ? »

- Champ : population de 15 ans et plus victime ou cible de cyberattaques (74 % de l'ensemble des internautes), en % -



Source : CREDOC, enquête Conditions de vie et aspirations juin 2025

Toutes les victimes d'arnaques ou fraudes en ligne ne sont pas égales face aux répercussions psychologiques post-cybermalveillance. Certains sous-groupes sont plus fréquemment impactés que d'autres. Parmi ces groupes les plus touchés, on retrouve les **femmes**, qui sont 43 % à affirmer avoir été affectées psychologiquement contre 38 % des hommes (Graphique 11). Les **jeunes adultes** sont aussi plus nombreux à déclarer avoir été affectés à la suite de cyberattaques (52 % des moins de 25 ans et 49 % des 25 à 39 ans contre 35 % des 40 à 59 ans) de même que les internautes à **bas revenus** (50 % contre 38 % des classes moyennes supérieures).

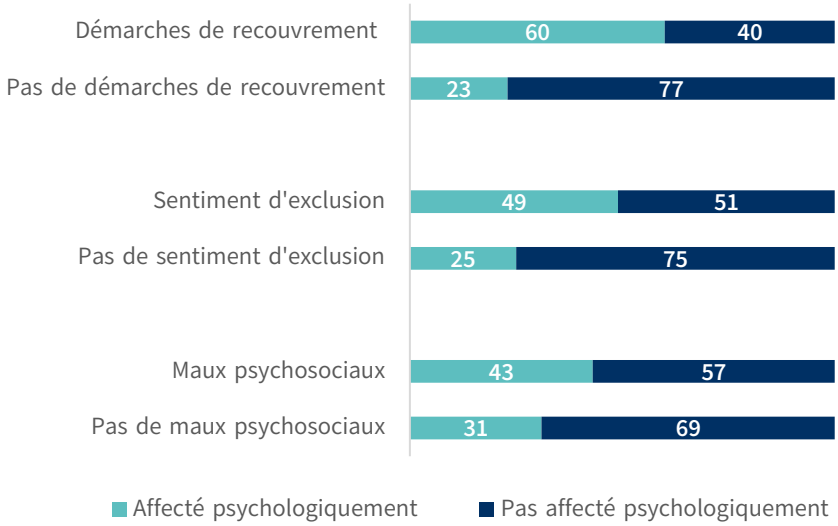
Les victimes de cyberattaques qui engagent des démarches de recouvrement semblent aussi le faire en raison du choc psychologique subi. En effet, 60 % de celles et ceux qui ont entrepris de telles démarches ont aussi déclaré avoir été affectés sur le plan psychologique après l'attaque (Graphique 12).

[55] SSMSI. (2023). *Op.cit.*

Parmi les victimes d'arnaques et fraudes en ligne, on observe que ceux ayant des séquelles psychologiques sont aussi plus fréquemment ceux qui se **sentent exclus** et ceux qui présentent des **souffrances psychosociales quotidiennes** du type mal de tête et migraine, mal de dos, nervosité, état dépressif, insomnie. Les deux phénomènes étant souvent liés[56].

Graphique 12 – « A la suite de ces arnaques, avez-vous été affecté.e psychologiquement ? »

- Champ : population de 15 ans et plus victime ou cible de cyberattaques (74 % de l'ensemble des internautes), en % -



Source : CREDOC, enquête Conditions de vie et aspirations juin 2025

R. Dennehy (2020)[57], dans son étude qualitative sur le cyberharcèlement des jeunes, relie les ressentis des victimes de cyberattaques au fait de **ne pas connaitre l'identité de l'agresseur**. Il résulte de ses entretiens que le cyberharcèlement (en opposition au harcèlement physique traditionnel) ne permet **pas d'échappatoire** chez les jeunes. Les technologiques numériques désormais omniprésentes dans la vie quotidienne, entretiennent un rappel constant de la cyberattaque pour les victimes. Contrairement au harcèlement dans un lieu physique (à l'école par exemple), dont la victime peut temporairement s'éloigner en changeant de lieu. Ainsi, l'environnement numérique rend l'évasion beaucoup plus difficile.

[56] La psychologue M. Allé met en évidence le lien entre l'exclusion sociale et l'apparition de troubles tels que la dépression, l'anxiété ou le stress.
A. Mengin, M. A. (2020, Juin 30). Conséquences psychopathologiques du confinement. *L'Encéphale, 46*(3), pp. S43-S52. doi:10.1016/j.encep.2020.04.007

[57] R. Dennehy, S. M. *Op. cit.*

5. Une inquiétude globalement stable qui tend à se polariser dans certains groupes en 2025

5.1. Une stabilité des inquiétudes face à l'insécurité numérique, à un niveau assez bas

Malgré la montée en puissance observée de la criminalité en ligne (+ 74 % en cinq ans[58]) et le fort niveau d'exposition de la population, celle-ci ne génère qu'une inquiétude **limitée** dans la population. Seuls 10 % des répondants la citent en effet comme la plus inquiétante dans une liste de neuf faits relatifs à la violence et l'insécurité. Le taux était identique en 2021, et à peine moins élevé (4 %) au début des années 2000.

Les préoccupations pour les violences dans la rue ou les lieux publics (20 %), les violences urbaines (16 %), les violences à l'école ou aux abords des établissements scolaires (15 %) et les atteintes aux biens (13 %) sont perçues comme bien plus inquiétantes.

De plus, la **hiérarchie** des craintes reste **inchangée** malgré l'augmentation des atteintes numériques commises : la cybercriminalité occupe en effet une place constante (la cinquième place) au sein des inquiétudes de la vie quotidienne en 2025 comme en 2021. Tout juste remonte-t-elle d'une place si l'on compare les résultats obtenus en 2005.

Tableau 1 – « Dans votre vie quotidienne, quels sont, parmi les faits suivants, les trois qui provoquent en vous la plus forte inquiétude ? »

- Champ : ensemble de la population de 15 ans et plus, en % de première réponse
effectif total pondéré en 2025 n : 3 473 -

	2005	2021	2025
Les violences contre les personnes dans la rue ou les lieux publics	32	19	20
La violence urbaine	7	15	16
La violence à l'école et aux abords des établissements scolaires	17	12	15
Les atteintes aux biens	24	16	13
La criminalité sur internet	4	10	10
Les violences sexuelles	10	9	9
Les troubles de la vie quotidienne	4	10	8
Les violences entre proches	2	5	6
Non réponse	1	6	5

Source : CREDOC, enquête Conditions de vie et aspirations juin 2005, 2021 et 2025

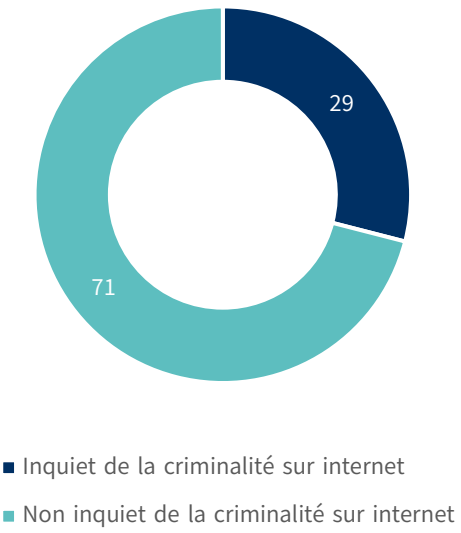
Au total (quand on cumule les trois réponses possibles), les inquiétudes des internautes Français concernant les risques de cybercriminalité sur internet restent également stables par rapport à 2021. En effet, **29 % des répondants se déclarent inquiets** face à la criminalité sur internet en 2025 (que ce

[58] Crédoc (2021), *Op.cit.*

soit en première, seconde ou troisième réponse, Graphique 10**Erreur ! Source du renvoi introuvable.**), soit la même proportion en 2021.

Graphique 13 – « Dans votre vie quotidienne, quels sont, parmi les faits suivants, les trois qui provoquent en vous la plus forte inquiétude ? »
Total de citations « La criminalité sur internet » en 1er ; 2ème ou 3ème réponse

- Champ : ensemble de la population de 15 ans et plus, en % - effectif total pondéré : 3 473 -



Source : CREDOC, enquête Conditions de vie et aspirations juin 2025

5.2. Une cybercriminalité qui inquiète davantage les femmes et les plus diplômés

Cette stabilité de surface ne rend pas compte des différences intra-groupes. Là où, en 2021 les inquiétudes liées à la criminalité sur internet étaient **uniformément distribuées** selon les caractéristiques sociodémographiques de la population, on **observe en 2025 quelques divergences**.

Ainsi, en 2025, les **femmes** sont un peu plus soucieuses de la criminalité sur internet (31 % contre 28 % pour les hommes). L'inquiétude est particulièrement vive chez les **25-39 ans** (35 % contre 16 % des 70 ans et plus), de même que chez les **cadres et professions intellectuelles supérieures** (35 % contre, par exemple, 26 % des retraités). Autrement dit chez les internautes les plus actifs sur la toile.

L'inquiétude face à la criminalité sur internet croît significativement avec le niveau d'étude des internautes. On constate ainsi que 33 % des **diplômés du supérieur** déclarent être inquiets de la criminalité en ligne contre 25 % seulement des non diplômés. Alors même que l'hypothèse inverse aurait pu être émise, puisque les plus diplômés disposent en théorie d'un capital socioculturel

numérique plus élevé[59] et donc potentiellement d'une meilleure capacité à se prémunir des risques. Etant mieux informés des risques d'internet, et en ayant un usage plus assidu, les diplômés du supérieur en sont plus inquiets.

Les profils des groupes les plus inquiets de la criminalité en ligne sont cohérents avec les données publiées en 2023 par le SSMSI[60] qui font état d'une corrélation avec le genre et le diplôme. En effet, c'est 35 % des femmes qui craignent être victime d'arnaques, fraudes, menaces, et exposition à des contenus illégaux en ligne contre 32 % des hommes ; et 36 % des diplômés de niveau Bac +3 ou supérieur contre 23 % des non-diplômés.

Par ailleurs, l'enquête du SSMSI (2023)[61] permet, dans un second temps, de pointer des craintes spécifiques selon les niveaux des revenus des internautes : les 20 % les **plus aisés** seraient plus inquiets du piratage et vol de données personnelles, tandis que la **classe moyenne** serait plus craintive de l'exposition aux contenus illégaux.

L'inquiétude de la criminalité sur internet n'est, en outre, qu'une facette d'une tendance plus générale à l'inquiétude développée par certains (craintes des maladies graves, des agressions dans la rue, des accidents de la route, du chômage …). L'inquiétude quant à la cybercriminalité est, en effet, corrélée à un **indicateur synthétique d'inquiétude** dans la vie quotidienne* (**Erreur ! Source du renvoi introuvable.**). Les plus inquiets dans la vie de tous les jours sont aussi les plus inquiets face à la criminalité sur internet (34 %), contre 24 % de ceux ne déclarant aucune inquiétude particulière dans la vie de tous les jours.

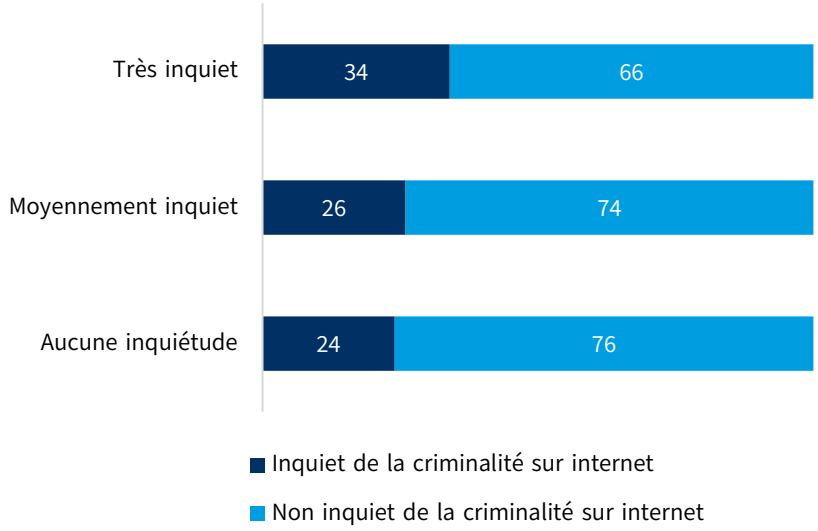
[59] ANCT, CREDOC, Université Rennes 2 CREAD-M@rsouin. (2023). *La société numérique française : définir et mesurer l'éloignement numérique*. https://www.credoc.fr/publications/la-societe-numerique-francaise-definir-et-mesurer-leloignement-numerique

[60] SSMSI. (2023). *Op.cit.*.

[61] SSMSI. (2023). *Ibid.*

Graphique 14 – « Dans votre vie quotidienne, quels sont, parmi les faits suivants, les trois qui provoquent en vous la plus forte inquiétude ? » - « La criminalité sur internet » selon le degré d'inquiétude dans la vie quotidienne

- Champ : ensemble de la population internaute de 15 ans et plus, en % - effectif total pondéré n : 3 473 -



Source : CREDOC, enquête Conditions de vie et aspirations juin 2025

* Construction de l'indicateur synthétique d'inquiétude :

L'indicateur d'inquiétude dans la vie quotidienne a été créé grâce à un compteur d'inquiétudes. Une liste de neuf risques (*maladie grave, agression dans la rue, accident de la route, chômage, guerre, accident de centrale nucléaire, risques liés à la consommation de produits alimentaires, terrorisme, changement climatique*) pouvant inquiéter la population a été donné aux répondants, ils devaient estimer si cela les inquiétait « Beaucoup », « Assez », « Un peu » ou « Pas du tout ». Sont comptabilisés comme inquiets de l'item en question, les individus ayant répondu « Beaucoup » ou « Assez ».

Un compteur des inquiétudes a été créé : ne sont pas considérés comme inquiets les individus ayant un score de zéro. Ceux comptabilisant entre 1 et 6 inquiétudes sont considérés « Moyennement inquiets » et ceux comptabilisant entre 7 et 9 inquiétudes comme « Très inquiets ».

Toutes choses égales par ailleurs (Figure A 1, page 41), les diplômés du supérieur et les femmes sont significativement plus inquiets.

On observe donc, en 2025, à taux d'inquiétude similaire à celui de 2021, **une certaine polarisation** de ces inquiétudes vis-à-vis de la criminalité sur internet : les plus diplômés, les femmes, les 25 à 39 ans et les cadres se montrent davantage préoccupés par la criminalité en ligne.

6. Annexe 1 : résultats des régressions logistiques

Figure A 1 - Résultats de la régression logistique « Cite la criminalité sur internet »
comme l'un des trois principaux faits provoquant la plus grande inquiétude »

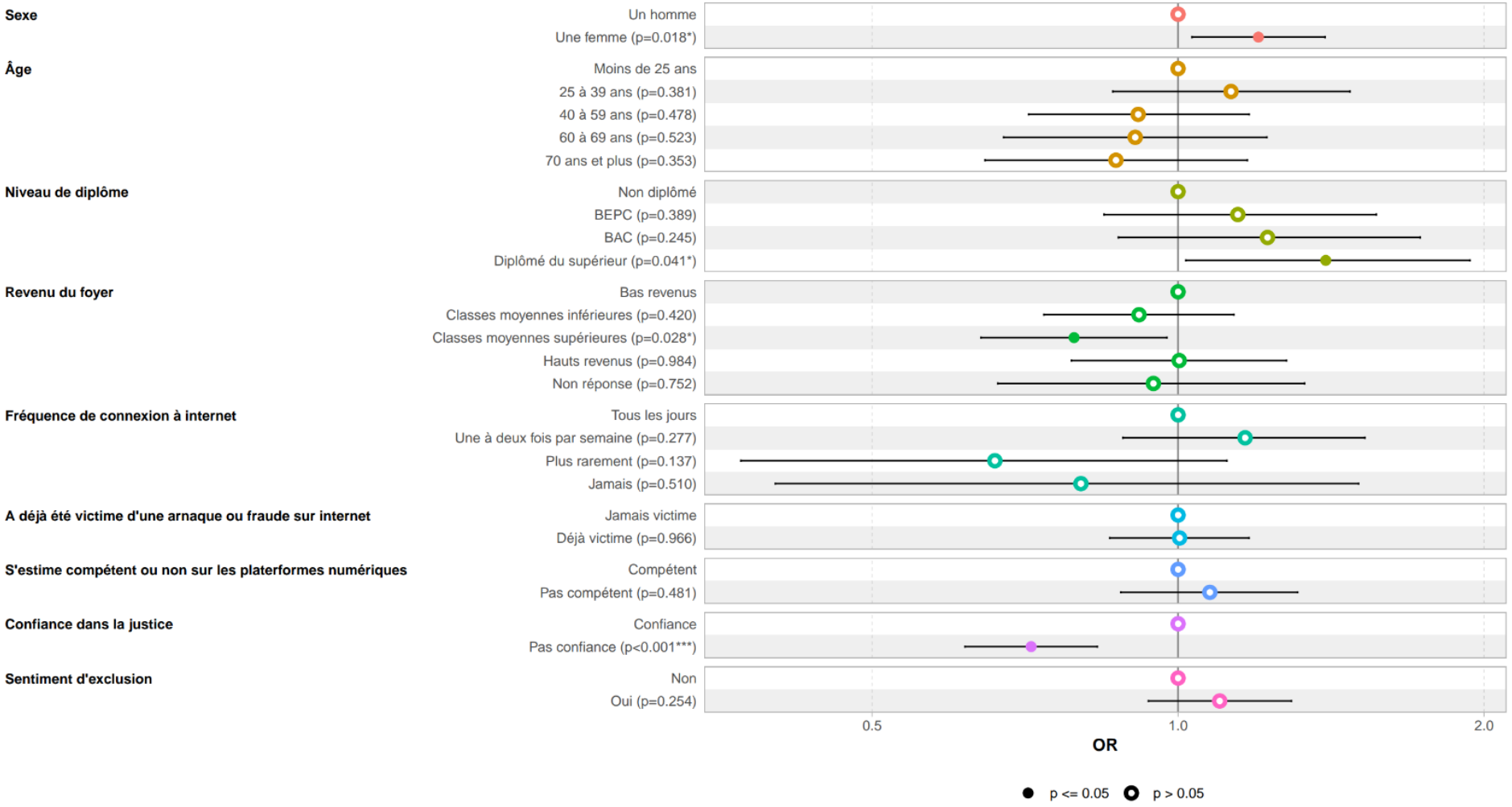
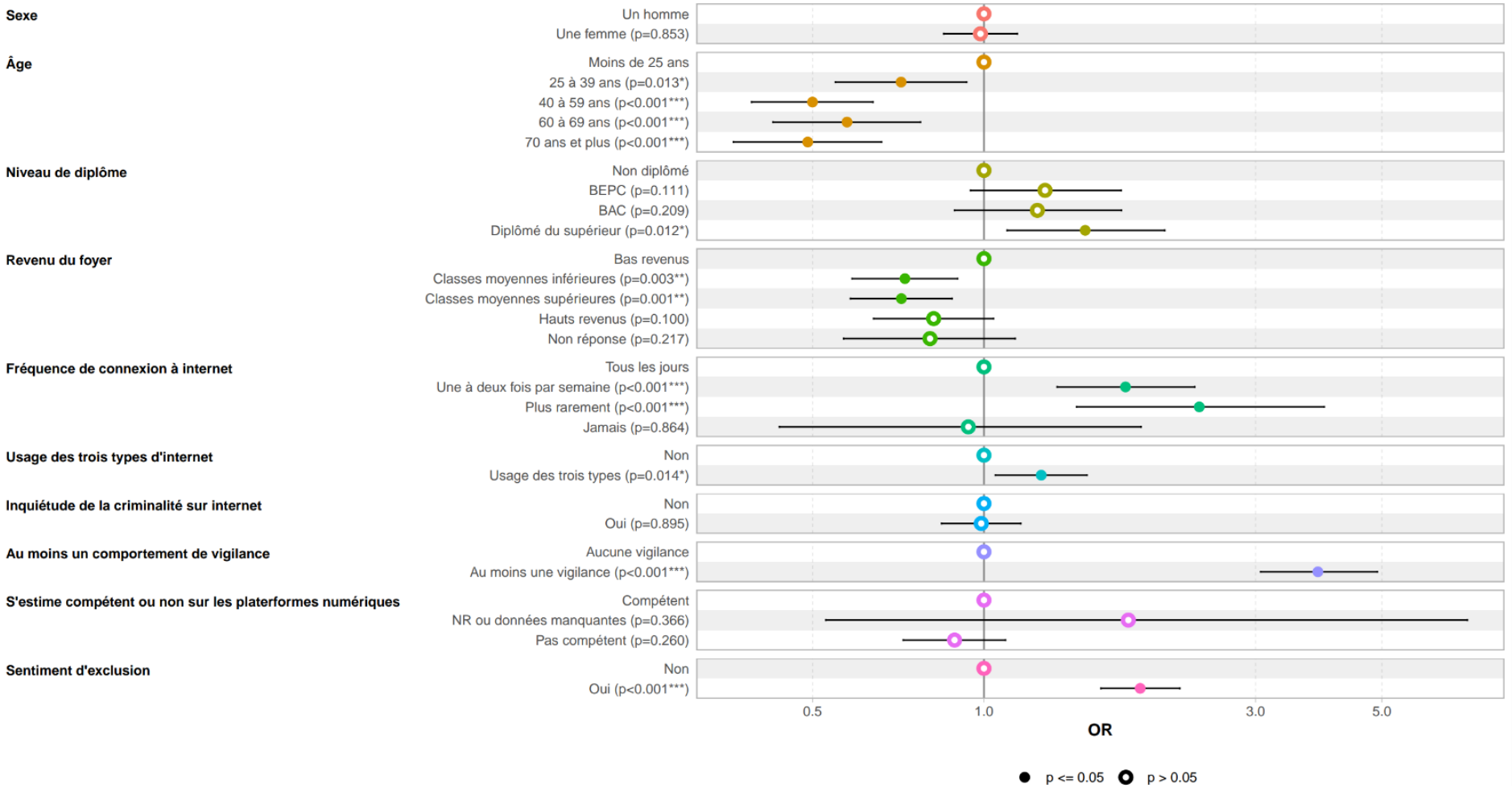
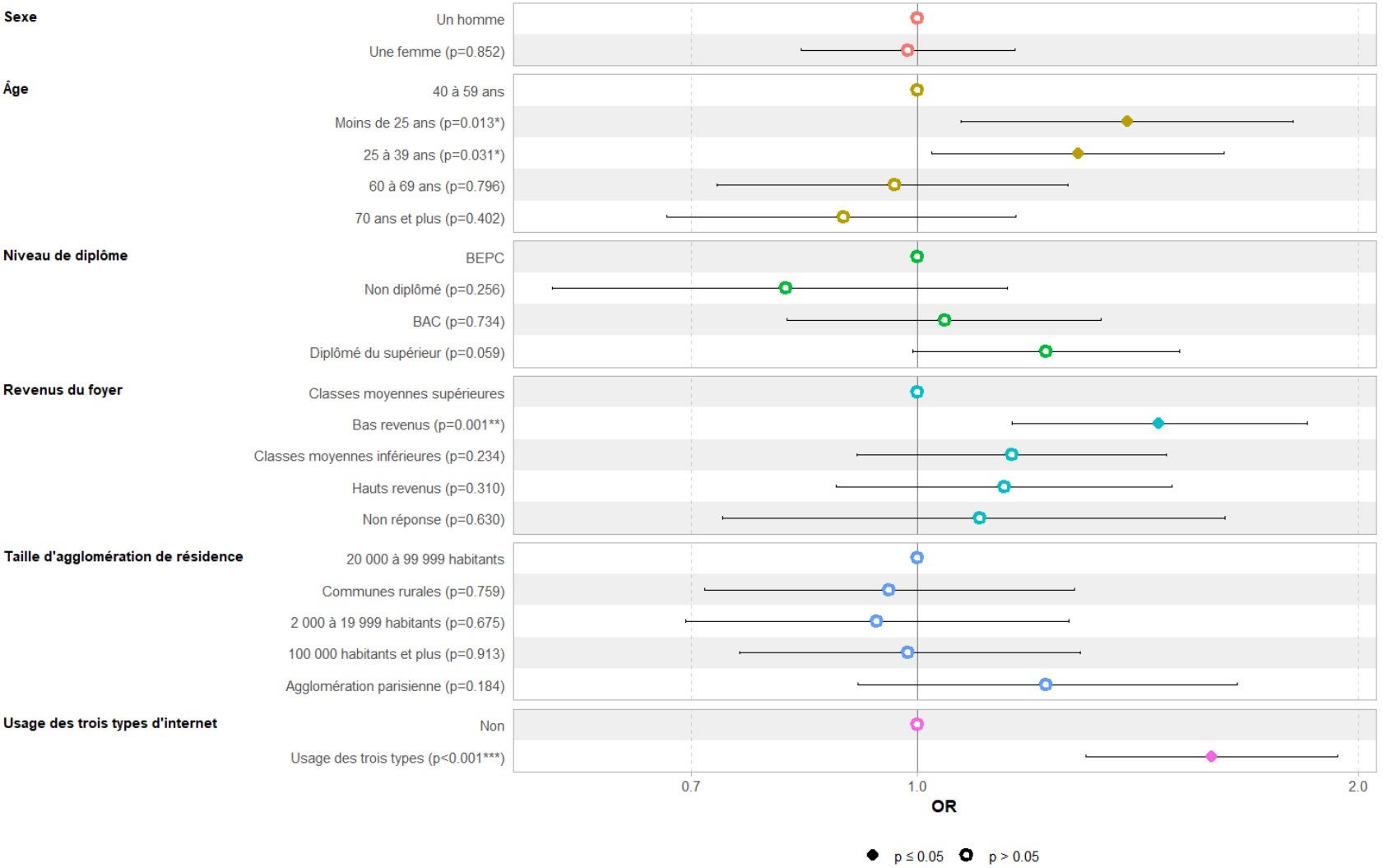


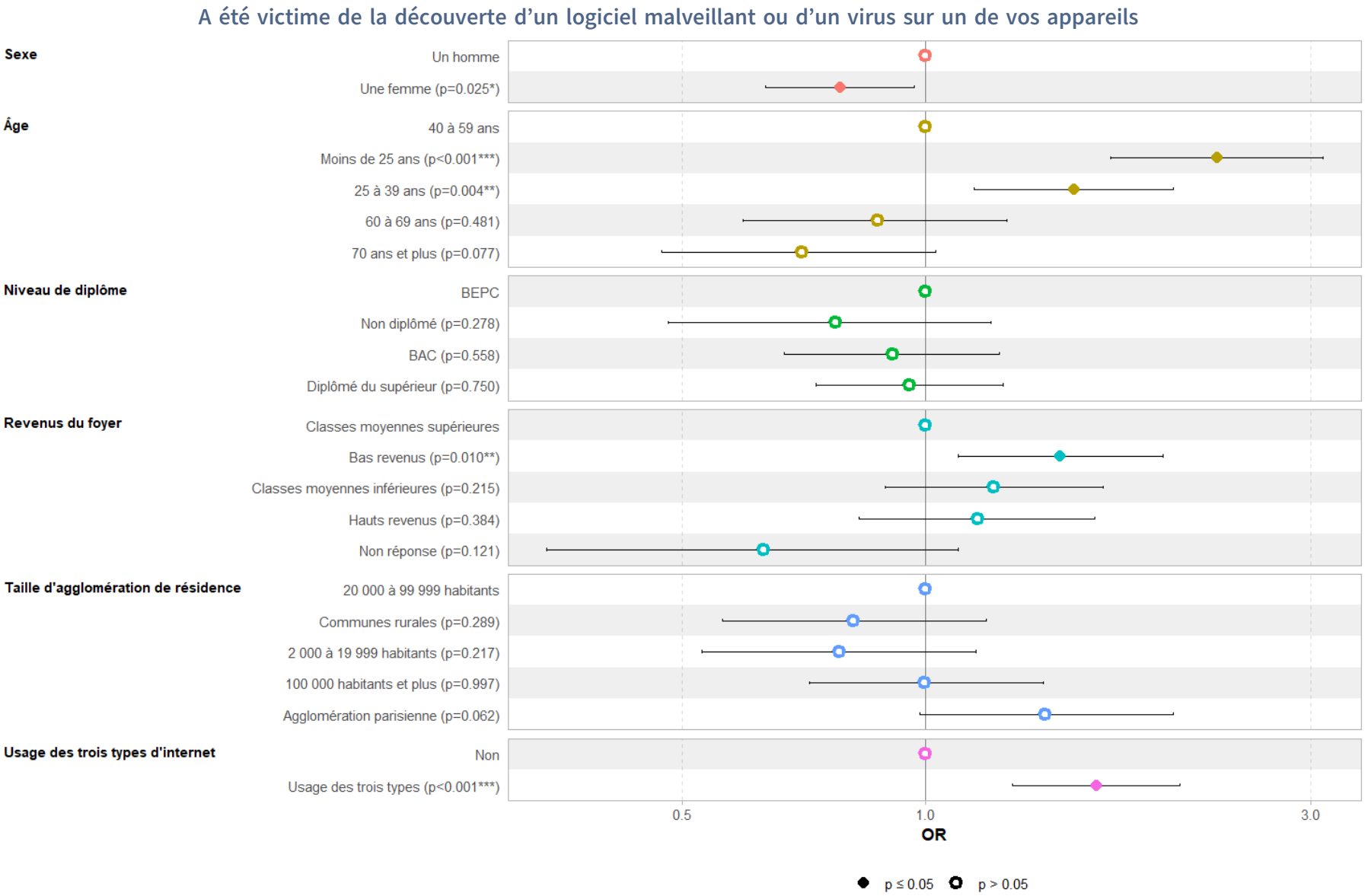
Figure A 2 - Résultats des régressions logistiques sur la victimation

« A été victime d'au moins une arnaque sur internet » oui / non

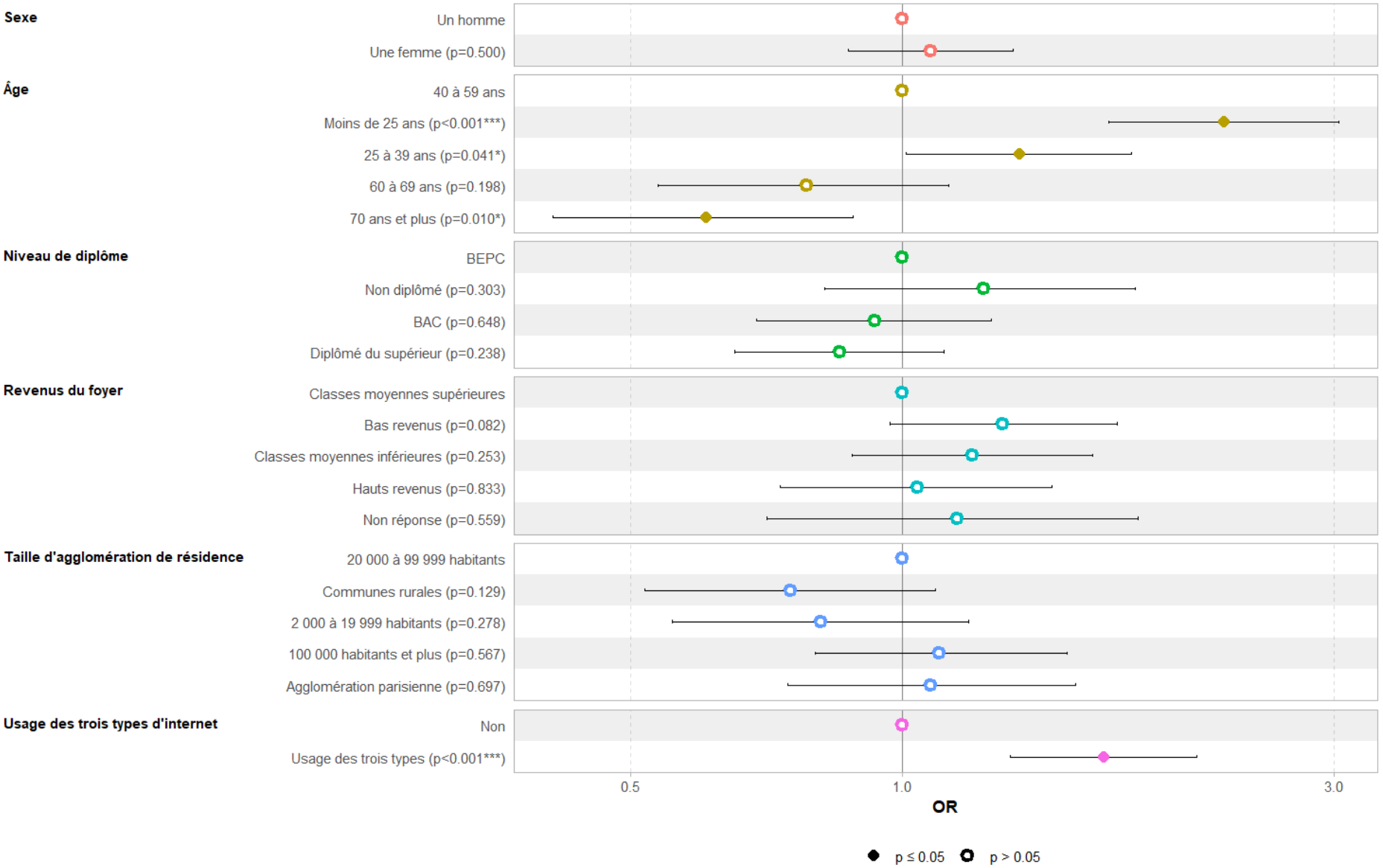


A été victime de la réception des e-mails ou appels frauduleux pour récupérer des informations personnelles

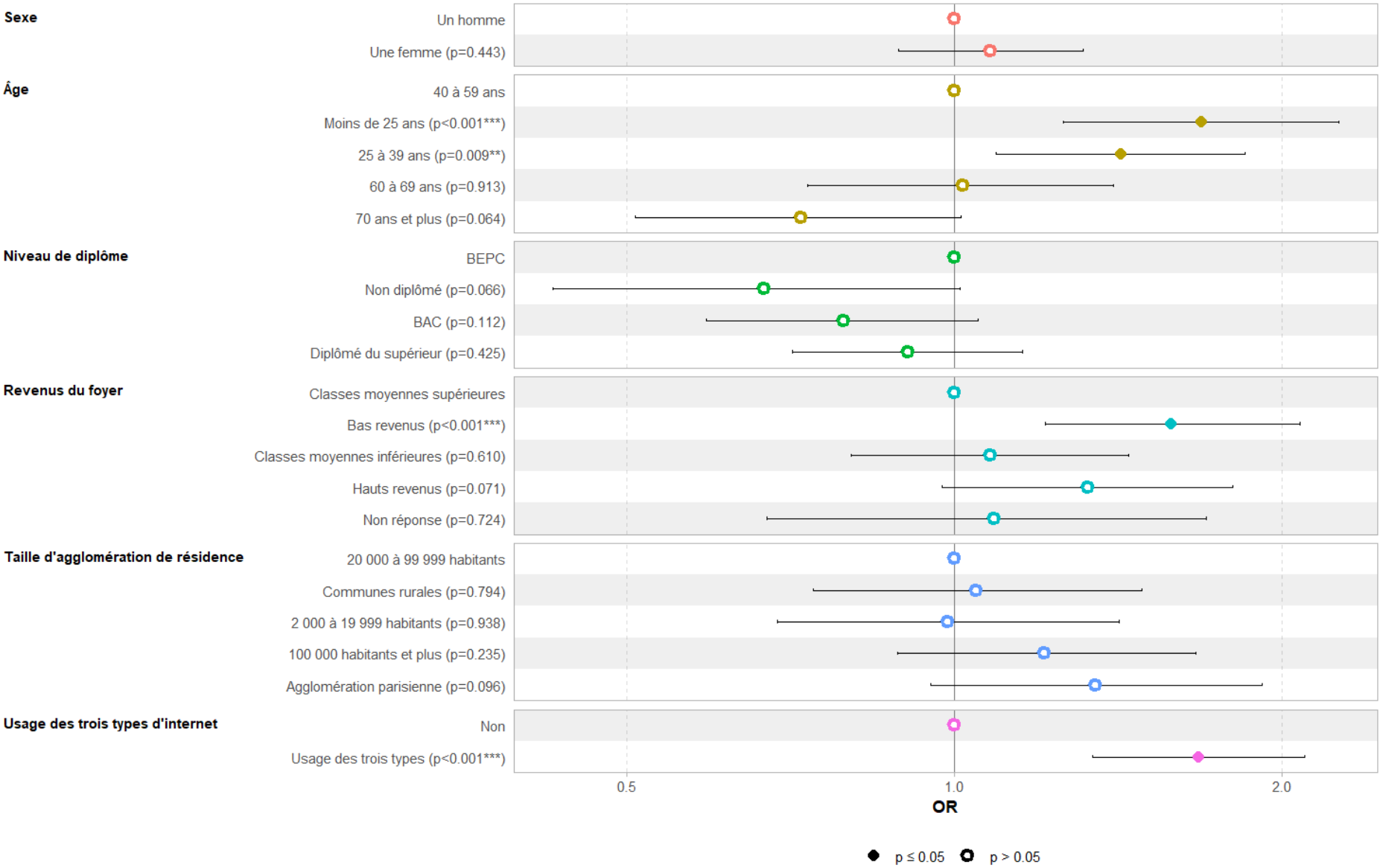



A été victime de la découverte d'un logiciel malveillant ou d'un virus sur un de vos appareils
Sexe
Un homme
Une femme (p=0.025*)
Âge
40 à 59 ans
Moins de 25 ans (p<0.001***)
25 à 39 ans (p=0.004**)
60 à 69 ans (p=0.481)
70 ans et plus (p=0.077)
Niveau de diplôme
BEPC
Non diplômé (p=0.278)
BAC (p=0.558)
Diplômé du supérieur (p=0.750)
Revenus du foyer
Classes moyennes supérieures
Bas revenus (p=0.010**)
Classes moyennes inférieures (p=0.215)
Hauts revenus (p=0.384)
Non réponse (p=0.121)
Taille d'agglomération de résidence
20 000 à 99 999 habitants
Communes rurales (p=0.289)
2 000 à 19 999 habitants (p=0.217)
100 000 habitants et plus (p=0.997)
Agglomération parisienne (p=0.062)
Usage des trois types d'internet
Non
Usage des trois types (p<0.001***)
0.5
1.0
3.0
OR
p ≤ 0.05
p > 0.05

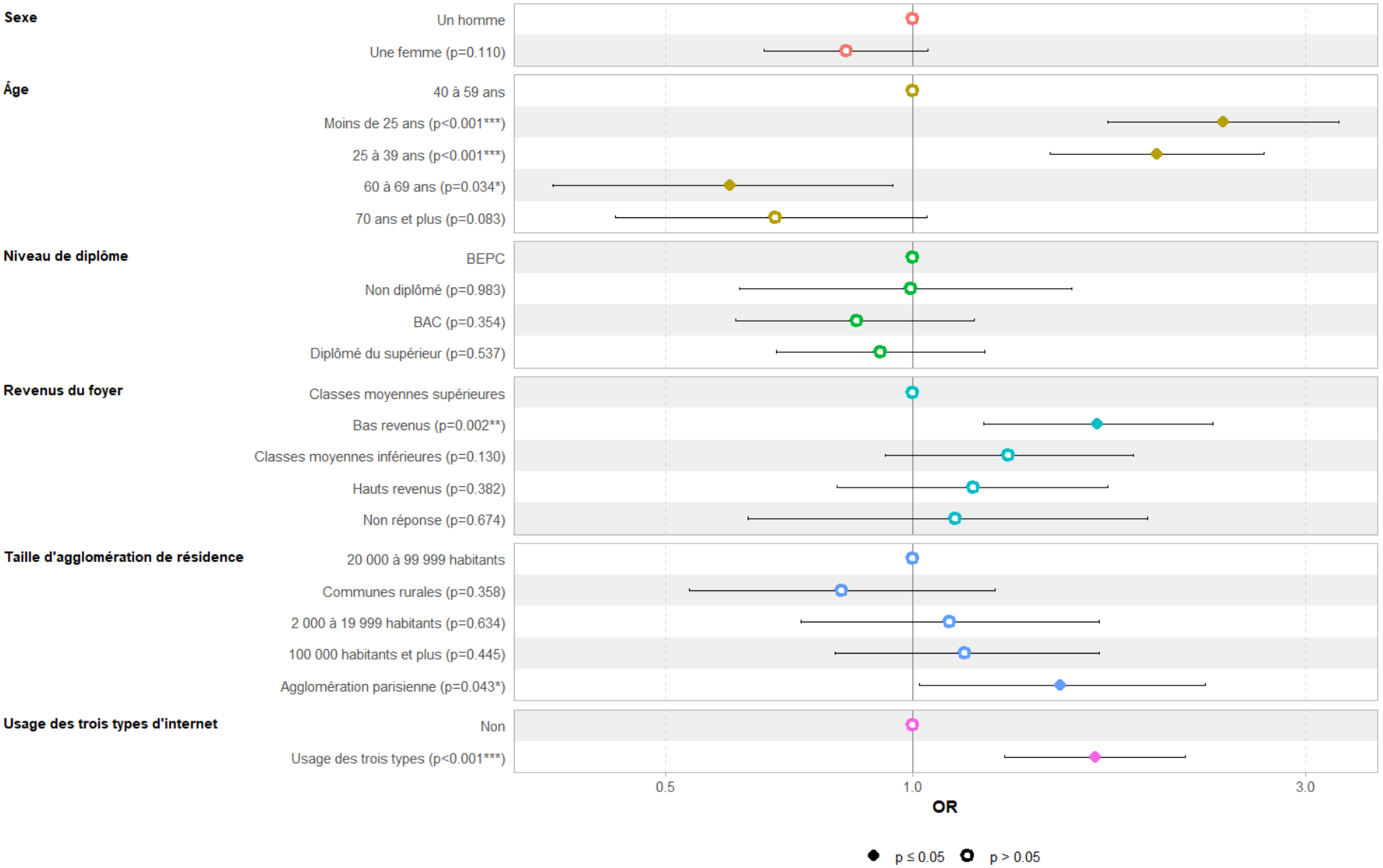
A été victime du piratage d'un compte de réseau social ou d'une boîte mail



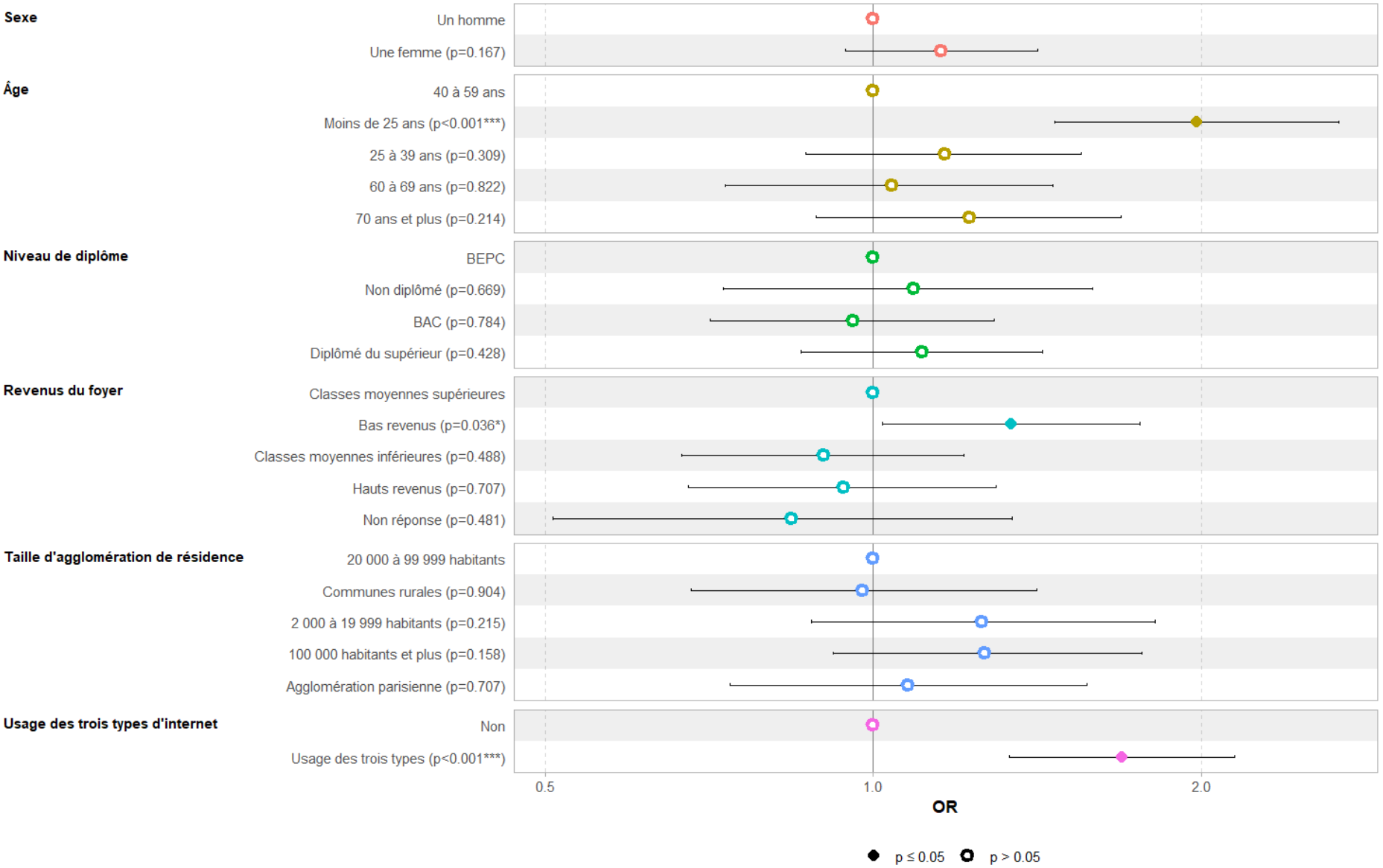
A été victime d'une escroquerie en ligne concernant l'achat d'un produit (non livré, contrefait ou non conforme)



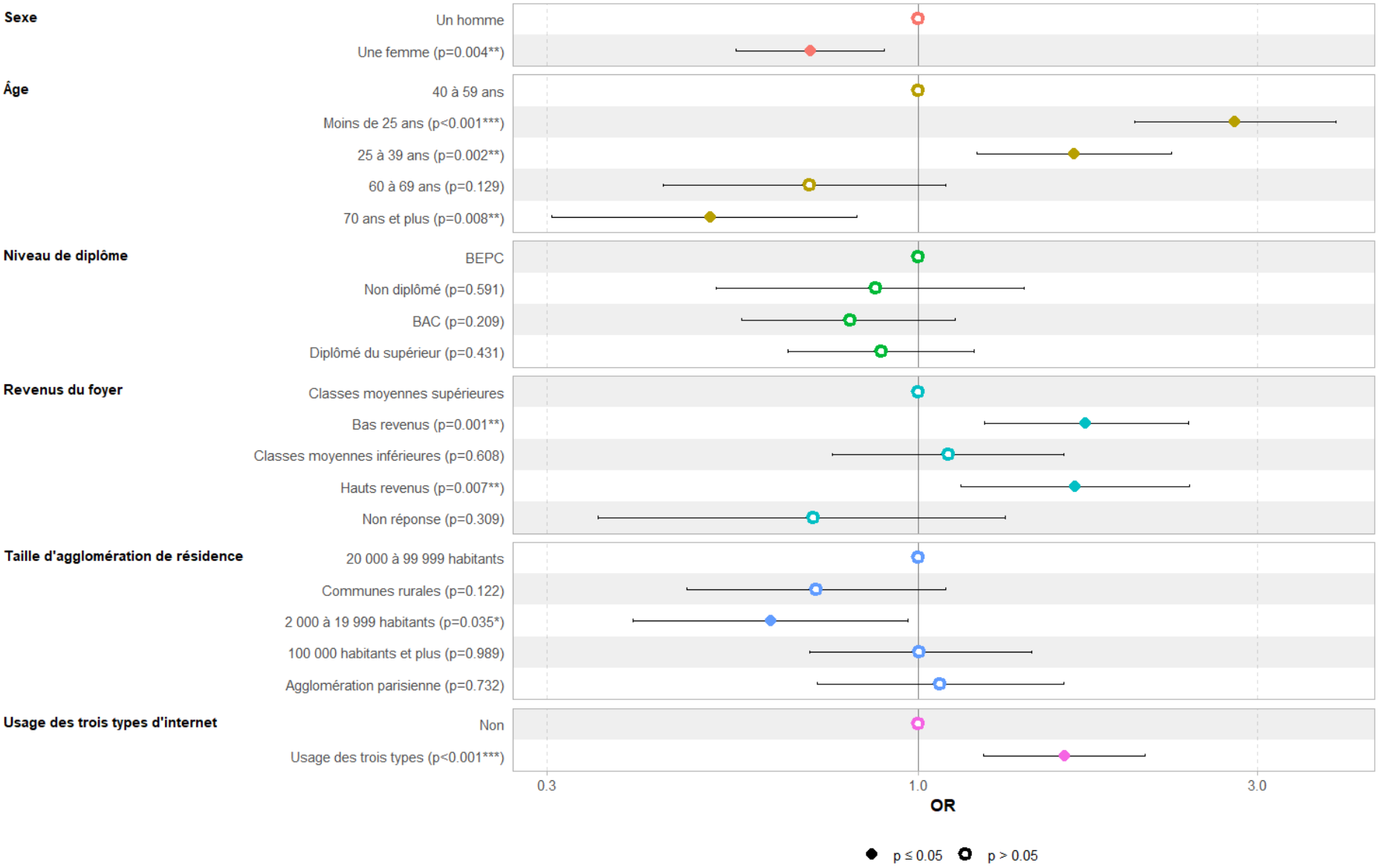
A été victime d'une escroquerie en ligne concernant l'achat d'un service ou d'une prestation (location, voyage, etc.)



A été victime d'une escroquerie bancaire sur internet



A été victime d'une demande de paiement ou demande de rançon en échange de la récupération de données, de photos ou de contrôle de votre appareil



A été victime d'une usurpation d'identité

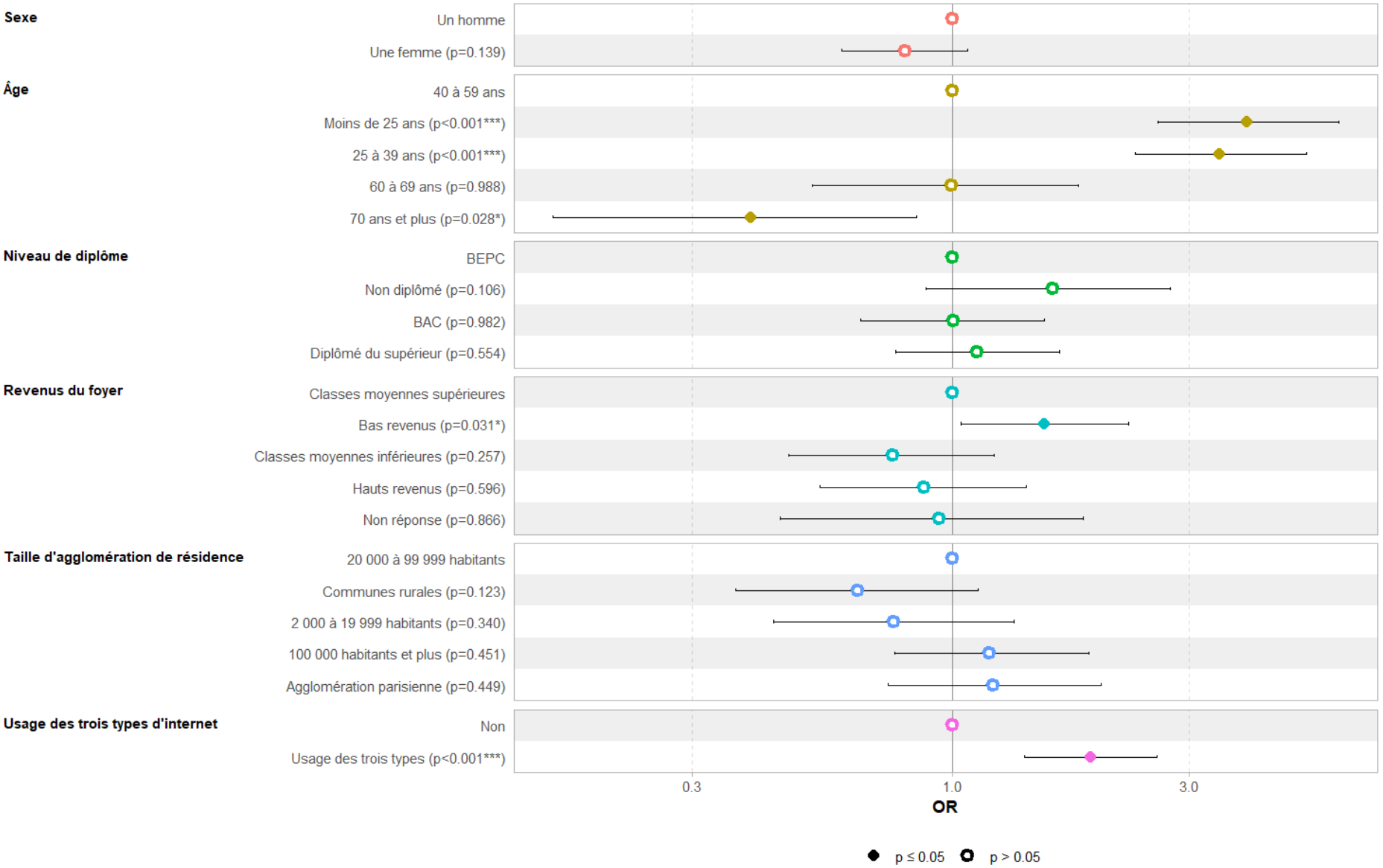
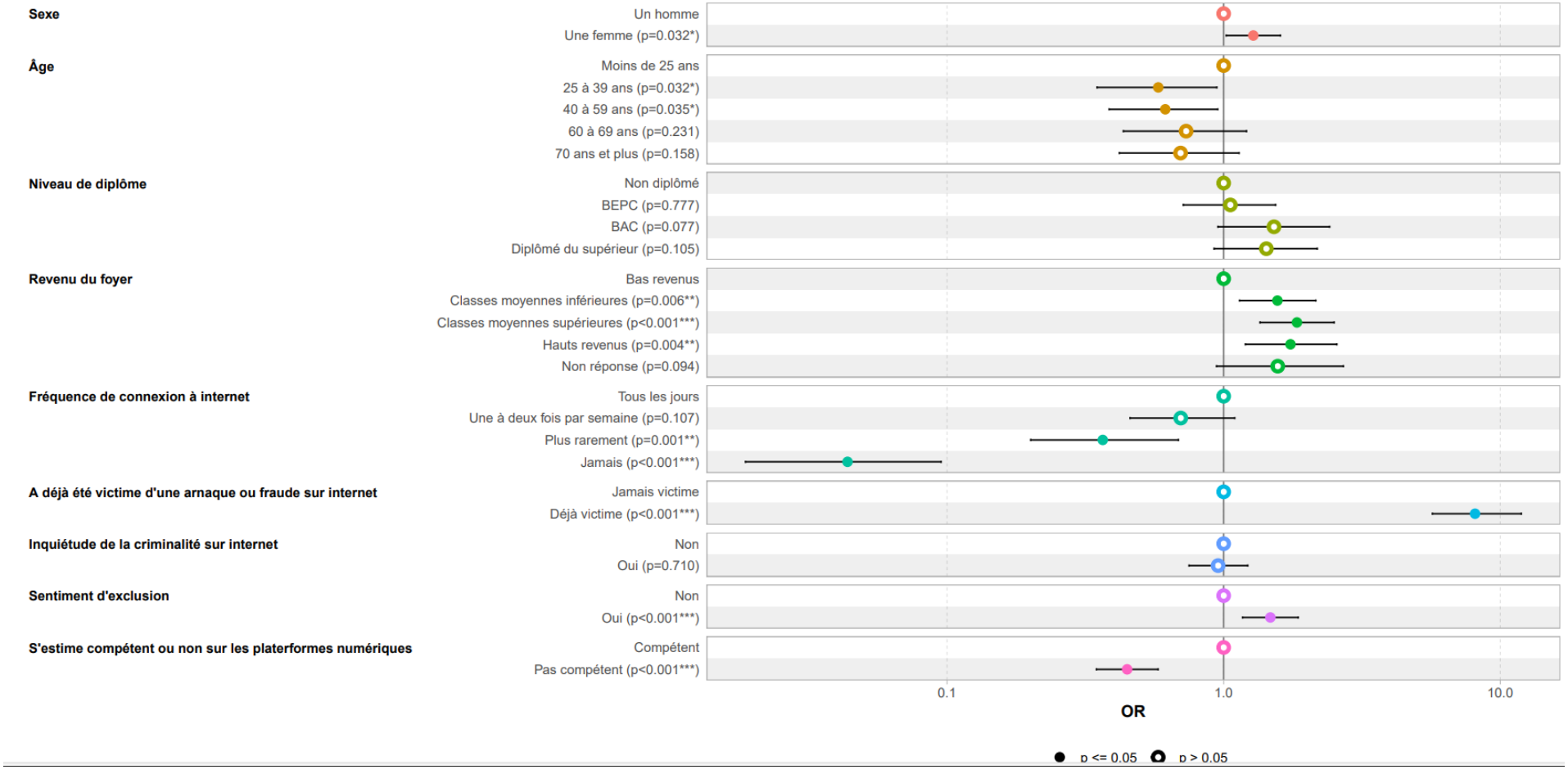


Figure A 3 - Résultats de la régression logistique « Adopte au moins un comportement de vigilance ou de renoncement sur internet » oui / non



Annexe 2 : questions posées

[A tous] INQFOR1 – INQFOR2 – INQFOR3

D1 Dans votre vie quotidienne, quels sont, parmi les faits suivants, les trois qui provoquent en vous la plus forte inquiétude ?

(Rotation aléatoire - Classez les trois premières réponses)

	1ère réponse citée	2ème réponse citée	3ème réponse citée
. Les atteintes aux biens (cambriolages, vols de véhicules, vols divers, destructions …)	1	1	1
. Les violences contre les personnes dans la rue ou les lieux publics (agressions avec ou sans armes, vols avec violences, coups et blessures…)	2	2	2
. La violence à l'école et aux abords des établissements scolaires (racket, agressions, insultes, menaces, vente de drogue …)	3	3	3
. Les violences entre proches (au sein du couple ou intra-familiales) .	4	4	4
. La violence urbaine (dégradation de biens publics, incendies de véhicules, violences contre les agents du service public, violences en bandes …)	5	5	5
. Les violences sexuelles	6	6	6
. La criminalité sur internet (messages pédopornographiques, messages violents ou à caractère raciste, utilisation frauduleuse de cartes de crédit …)	7	7	7
. Les troubles de la vie quotidienne (tapage, bruits, rassemblements inquiétants dans les halls, graffiti, petites dégradations, rodéos automobiles ...)	8	8	8
. *Ne sait pas*	*9*	*9*	*9*

[Si internaute ou si a l'usage d'un téléphone mobile1] PRECAU1 à PRECAU8

D2 Il est possible de prendre certaines précautions ou d'adopter certains comportements quand on utilise internet. Vous, personnellement, avez-vous déjà :

	Oui	Non
. Refusé d'être géolocalisé en ouvrant une page internet ou dans une application ?	1	2
. Renoncé à installer une application, afin de protéger vos données personnelles (votre carnet d'adresses, vos photos, votre agenda…) ?	1	2
. Eteint votre téléphone mobile pour éviter d'être tracé ?	1	2
. Pris des dispositions pour ne pas laisser de traces sur internet, par exemple en supprimant des cookies ou en naviguant en mode privé ?	1	2
. Renoncé à un achat parce que vous n'aviez pas suffisamment confiance au moment du paiement ?	1	2
. Souscrit à un service de sécurisation de paiement en ligne, par exemple avec un procédé qui évite de communiquer votre numéro de carte habituelle ?	1	2
. Renoncé à publier, ou supprimé, un message sur un réseau social pour protéger votre vie privée	1	2
. Arrêté votre navigation sur internet à cause de l'insuffisante sécurité d'une page internet (avertissement du navigateur, absence du https ou de l'icône cadenas dans la barre d'adresse)	1	2

[A tous] ARNAKWEB1 à ARNAKWEB8

D3 Au cours des douze derniers-mois, avez-vous été confronté aux situations suivantes sur internet ?

	Oui, j'en ai personnellement été victime	Oui, j'y ai été confronté mais j'ai pu m'en rendre compte à temps	Non	Nsp
Réception d'e-mails ou d'appels frauduleux pour récupérer des informations personnelles	1	2	3	*4*
Découverte d'un logiciel malveillant ou d'un virus sur un de vos appareils	1	2	3	*4*
Piratage d'un compte de réseau social ou d'une boîte mail	1	2	3	*4*
Escroquerie en ligne concernant l'achat d'un produit (non livré, contrefait ou non conforme)	1	2	3	*4*
Escroquerie en ligne concernant l'achat d'un service ou d'une prestation (location, voyage, etc.)	1	2	3	*4*
Escroquerie bancaire sur internet	1	2	3	*4*
Demande de paiement ou demande de rançon en échange de la récupération de données, de photos ou de contrôle de votre appareil	1	2	3	*4*
Usurpation d'identité	1	2	3	*4*

[Si un oui à ARNAK1 à 8] ACTION1 à ACTION3
NEW

D4 À la suite de ces arnaques, avez-vous réalisé les démarches suivantes ?

	Oui	Non	Nsp
Signalé les faits sur un site officiel comme THESEE, internet-signalement.gouv.fr	1	2	*3*
Porté plainte ou déposé une main courante dans un commissariat, ou en gendarmerie	1	2	*3*
Tenté d'obtenir réparation auprès de votre banque, de l'entreprise, de votre assurance	1	2	*3*

[Si un oui à ARNAK1 à 8] IMPACPSY

D5 À la suite de ces arnaques, avez-vous été affecté.e psychologiquement ?

. Oui, beaucoup 1
. Oui, un peu 2
. Non, pas vraiment 3
. Non, pas du tout 4
. *Ne sait pas* *5*

7. Bibliographie

A. Almansoori, M. A.-E. (2023). Exploring the frontiers of cybersecurity behavior: A systematic review of studies and theories. *Applied Sciences, 13*. doi:10.3390/app13095700

A. Mengin, M. A. (2020, Juin 30). Conséquences psychopathologiques du confinement. *L'Encéphale, 46*(3), pp. S43-S52. doi:10.1016/j.encep.2020.04.007

ANCT, CREDOC, Université Rennes 2 CREAD-M@rsouin. (2023). *La société numérique française : définir et mesurer l'éloignement numérique.*

Arcep, Arcom, CGE, ANCT. (2025). *Baromètre du numérique, édition 2025.* Récupéré sur https://www.credoc.fr/publications/barometre-du-numerique-edition-2025

Autorité des Marchés Financiers. (2024). *Les arnaques à l'investissement.* Récupéré sur https://www.amf-france.org/sites/institutionnel/files/private/2024-12/amf-rapport-bva_arnaques-a-linvestissement_-version-publiable_19-dec.pdf

Banque de France. (2024). *Rapport de l'Observatoire de la sécurité des moyens de paiment 2023.* Récupéré sur https://www.banque-france.fr/fr/publications-et-statistiques/publications/rapport-de-lobservatoire-de-la-securite-des-moyens-de-paiement-2023

COMCYBER-MI. (2025). *Rapport annuel sur la cybercriminalité.*

Commission Européenne. (2019). *Special Eurobarometer 499.*

Cour des comptes. (2025). *La réponse de l'Etat aux cybermenaces sur les systèmes d'information civils.*

CREDOC. (2021). *L'escroquerie en ligne et à la téléphonie en France.* Cahier de recherche.

D. Melita, E. G. (2025, Juillet 5). Inequality and Status Anxiety: Bad Allies of Health and Well-Being, but not for Everyone. The Role of Ideologies, SOcioeconomic Status, and Economic Threat. doi:10.1007/s11205-025-03656-0

Dares. (2019). *Data scientists, community managers... et informaticiens : quels sont les métiers du numérique?* Récupéré sur https://dares.travail-emploi.gouv.fr/publications/data-scientists-community-managers-et-informaticiens-quels-sont-les-metiers-du

Esmer, S. (2023). Evaluating the digital divide through Amartya Sen's capability approach. *STS Meets Ethics Conference Proceedings*, (pp. 165-175).

European Institute for Gender Equality. (2020). *Gender Equality Index 2020 : Digitalisation and the future of work.* Récupéré sur https://eige.europa.eu/publications-resources/toolkits-guides/gender-equality-index-2020-report/men-dominate-technology-development?language_content_entity=en

Eurostat. (2023). *Individuas encountering hostile or degrading online messages*.

Eurostat. (2025). *Problems experienced when buying online (isoc_ec_iprb21).* Récupéré sur https://ec.europa.eu/eurostat/databrowser/view/isoc_ec_iprb21/default/table?lang=en&category=isoc.isoc_i.isoc_iec

Fevad. (2025). *Bilan du e-commerce en France en 2024 : les ventes sur internet franchissent le cap des 175 milliards d'euros, en hausse de 9,6 % sur un an.* Récupéré sur https://www.fevad.com/bilan-du-e-commerce-en-france-en-2024-les-ventes-sur-internet-franchissent-le-cap-des-175-milliards-deuros-en-hausse-de-96-sur-un-an/

Financiers, A. d. (2024). *Les arnaques à l'investissement.*

Granjon, F. (2022). Inégalités sociales, dispositions et usages du numérique. *Education et société*(47), pp. 81-97. doi:10.3917/es.047.0081

Granjon, F. (2022). Inégalités sociales-numériques: décryptage sociologique. *Les Cahiers du Développement Social Urbain*(75), pp. 6-8. doi:10.3917/cdsu.075.0006

H. Magne, N. J. (2020, Septembre 11). La croissance post-traumatique: un concept méconnu de la psychiatrie française. *L'Encéphale, 47*(2), pp. 143-150. doi:https://doi.org/10.1016/j.encep.2020.05.021

Insee. (2021). *Sécurité et société, édition 2021.* Récupéré sur https://www.insee.fr/fr/statistiques/5763599?sommaire=5763633

Insee. (2022). *Femmes et hommes, l'égalité en question.*

Insee. (2024). *Enquête sur les technologies de l'information et de la communication par les ménages entre 2009 et 2024.* Récupéré sur https://www.insee.fr/fr/statistiques/8278698?sommaire=8278710

Insee. (2025). *Achats de produits et de services en ligne.* Récupéré sur https://www.insee.fr/fr/statistiques/8616823?sommaire=8616883

Insee. (2025, Avril 14). *Enquête sur les technologies de l'information et de la communication*.

Interstat, Service statistique ministériel de la sécurité intérieure. (2024). *Les escroqueries enregistrées par les services de sécurité entre 2016 et 2023.* Récupéré sur https://www.bnsp.insee.fr/ark:/12148/bc6p0934n7g.pdf

Interstats. (2019). *Plus de la moitié des arnaques passent par internet - Analyse N°21.*

IPSOS et cybermalveillance.gouv. (2024, Septembre). *Les Français et la sécurité numérique*.

M. Mahipal, N. S. (2025). Cybersecurity awarness among young adults: An analytical study. *International Symposium on Electronic Imaging.* doi:10.2352/EI.2025.37.3.MOBMU-312

M. Näsi, A. O. (2015, Avril 22). Cybercrime victimization among young people: a multi-nation study. *Journal of Scandinavian Studies in Criminology and Crime Prevention, 16*(2), pp. 203-210. doi:https://doi.org/10.1080/14043858.2015.1046640

Ministère de la Justice. (2025). *"Usurpation d'identité".* Récupéré sur https://www.justice.fr/fiche/usurpation-identite

Plantard, P. (2021). *La fracture numérique : mythe ou réalité ?* Education Permanente.

R. Dennehy, S. M. (2020, Février 15). The psychosocial impacts of cybervictimisation and barriers to seeking social support: Young people's perspectives. *Children and Youth Services Review*. doi:10.1016/j.childyouth.2020.104872

Rani, S. (2025). Studying the impact of anxiety, stress, and emotion on academic performance: A systematic review. *Journal of Social, Humanity, and Education, 5*(2), pp. 131-141. doi:10.35912/jshe.v5i2.2437

Raquel Lozano-Blasco, A. Q.-R.-C. (2023). Sex, age and cyber-victimization: A meta-analysis. *Computers Human Behavior, 139*. doi:10.1016/j.chb.2022.107491

Sen, A. (1997). Editorial: Human Capital and Human Capability. *World Development, 25*(12), pp. 1959-1961.

Smoreda, Z. B. (2007). *Saisir les pratiques numériques dans leur globalité.* doi:https://doi.org/10.3917/res.145.0019.

SSMSI. (2023). *Vécu et ressenti en matière de sécurité: Victimation, délinquance et sentiment d'insécurité.*

T. Moore, R. B. (2012). How do consumers react to cybercrime? *eCrime Reseachers Summit.* doi:10.1109/eCrime.2012.6489519

CRÉDOC

CENTRE DE RECHERCHE POUR L'ÉTUDE ET
L'OBSERVATION DES CONDITIONS DE VIE