FORTRA

Ipsos

DE LA PROTECTION DES DONNÉES À LA CULTURE CYBER

La sensibilisation des collaborateurs au cœur des enjeux de cybersécurité

TABLE DES MATIÈRES

4 Introduction

6 Le mot de Dalila Ben Attia, Directrice Générale de Terranova Security France

7-12 Sensibilisation à la cybersécurité : état des lieux

- Présentation des résultats de l'enquête IPSOS
  - Un niveau élevé de connaissance des risques cybers
  - Des défis grandissants liés au télétravail
  - La question du besoin en sensibilisation
  - La responsabilité face aux risques
  - La société est-elle favorable à une culture cyber partagée entre tous ?
  - Alors, quelles sont les clés d'une généralisation de la culture cyber ?

13-16 Les fondations et l'émergence d'une culture de la cybersécurité : où en sommes-nous ?

- L'illectronisme, mal du siècle ?
- L'éducation au service de la culture numérique
- Une association tripartite : pouvoirs publics, entreprises et individus

17-18 Le besoin urgent d'une base commune de connaissances sur la technologie numérique

- Technophiles, technophobes : des freins à la culture de sécurité ?

19 Conclusion

Introduction

Ce rapport a pour objectif d'ouvrir le débat autour de l'acculturation des personnes aux risques numériques, en dressant un état des lieux du niveau de sensibilisation à la cybersécurité de la population active en France, au Canada, aux États-Unis, au Royaume-Uni et en Australie. En préambule, il est nécessaire de bien circonscrire notre sujet : quand peut-on affirmer qu'un individu, ou un groupe, est sensibilisé aux risques cyber ? On parle de culture de la cybersécurité dès lors que les individus sont capables d'identifier, de citer différentes typologies d'attaques, qu'ils ont également connaissance des outils de protection existants, ainsi que des méthodes permettant d'éviter et/ou de signaler une tentative d'intrusion.

Depuis plus de deux ans et demi maintenant, les mots « cyberattaques », « ransomwares », « cybersécurité » ou encore « phishing » n'ont eu de cesse de s'inviter dans les médias, les communications internes et externes des entreprises, les discours des politiques et les réseaux sociaux. La crise sanitaire liée au virus de la Covid-19 semble avoir ainsi fait de la "conscience cyber" une réalité enfin tangible, quoique discrète. Les attaquants quant à eux n'ont eu de cesse de se professionnaliser. En 2021, le rapport des menaces de l'ANSSI mettait en exergue une hausse de 37 % du nombre d'intrusions actées, passant la barre des 1000 attaques, par rapport à 2020. Et, au regard des dernières unes médiatiques, il est très probable que le rapport 2022 témoigne prochainement d'une nouvelle augmentation des risques. À cette augmentation continue des attaques, une cause a été présentée dans plus de 90 % des cas : l'erreur ou l'inattention humaine. Car si les attaques sophistiquées telles que les DDoS existent bel et bien, la vaste majorité des attaques usent et abusent de procédés dits d'ingénierie sociale, qui se fondent à la fois sur le manque de culture cyber des individus et sur des stratagèmes de pression psychologique, pour voler des données, de l'argent, voire l'identité des particuliers comme des professionnels.

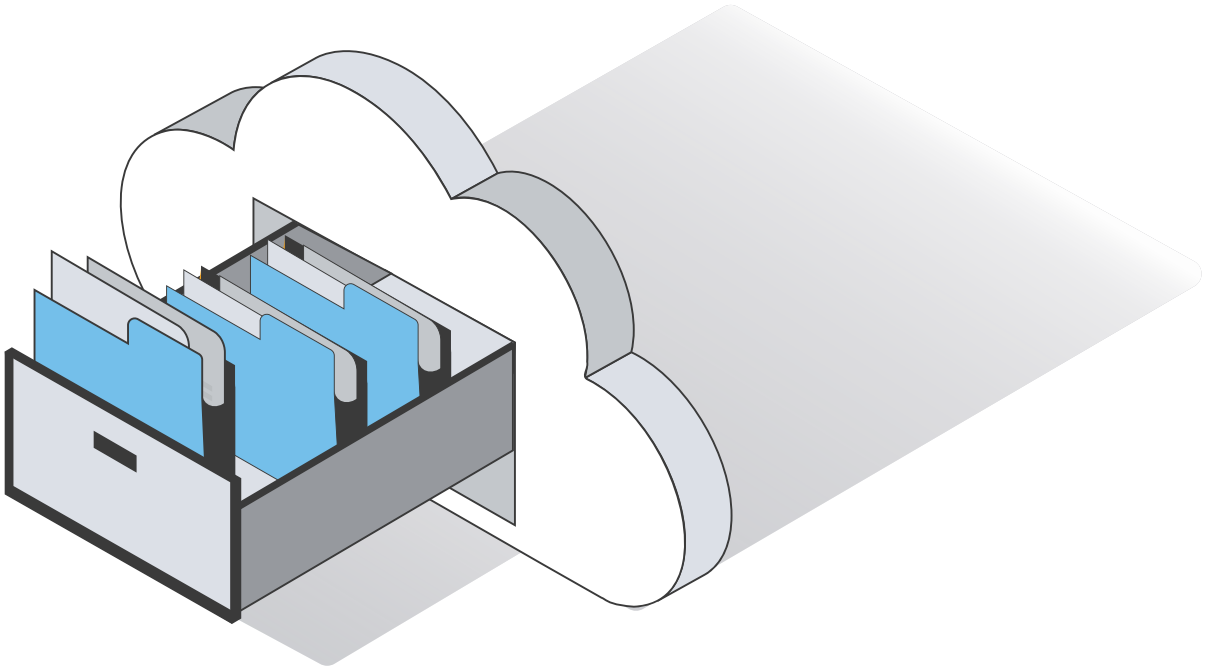
Le paysage des cybermenaces s'est également élargi depuis l'avènement des modes de travail hybrides, dont les modalités ne sont pas encore stabilisées, ouvrant la voie à un phénomène récemment identifié et nommé : le « Shadow IT ». Ce terme désigne l'utilisation de technologies matérielles et logicielles par les employés de l'entreprise sans l'accord du département informatique. Si en 2020 le passage au 100 % télétravail avait mis à rude épreuve les politiques de sécurité informatique et fait la lumière sur le manque de connaissances en sécurité des collaborateurs, la situation ne semble aujourd'hui pas encore résolue.

L'une des questions à se poser est alors la suivante : la visibilité des risques cyber auprès de l'ensemble de la population est-elle synonyme de connaissance ou de savoir ?

Pour y répondre, il est utile de rappeler que chaque être humain peut être un bouclier efficace contre ces cyberattaques, dès lors qu'il en est informé, qu'il y est préparé et qu'il bénéficie des outils et du soutien nécessaires. En effet, des études et rapports de simulation d'attaques comme le *Gone Phishing Tournament Report* mettent en lumière une étroite corrélation entre la mise en place de programmes de sensibilisation à la cybersécurité et la conscience « cyber » des individus. D'après l'édition 2021, seules 29 % des institutions dans le secteur de l'éducation avaient par exemple mis en place des actions de sensibilisation et de simulation aux attaques ; 27,6 % des personnes ayant reçu l'e-mail de la simulation de phishing ont cliqué sur le lien contenu dedans (contre 19,8 % en moyenne sur l'ensemble des répondants).

Aussi, alors que la sensibilisation à la cybersécurité a été décrétée enjeu prioritaire par le gouvernement français et a fait l'objet de la création d'un groupe de travail dédié opérant depuis novembre 2021, la question du niveau minimal de connaissance nécessaire à la protection des données des entreprises comme des particuliers continue à se poser ?

À mesure que la société toute entière se numérise, progresse dans la dématérialisation de ses services, de ses objets, et tend même vers l'émergence de nouvelles réalités virtuelles, il est grand temps de songer à « s'armer », en s'acculturant aux risques du numérique. Cela ne peut se faire sans une sensibilisation de l'ensemble de la société, avec, en tête de proue de ce mouvement, les entreprises, les pouvoirs publics et le secteur de l'éducation.



Le mot de Dalila Ben Attia, Directrice Générale de Terranova Security France

Depuis 20 ans, les équipes de Terranova Security et sa fondatrice, Lise Lapointe, travaillent sans relâche pour donner toujours plus de sens et d'intérêt à leur programme de formation en sensibilisation à la cybersécurité. Sensibiliser ne réside pas uniquement dans l'apprentissage de méthodes, mais dans une capacité à faire émerger chez l'autre une prise de conscience. Délaissant les formats d'apprentissage trop classiques qui ne permettent pas nécessairement de retenir et de mettre en application les connaissances, Terranova Security mise sur des enseignements dont le format d'apprentissage est ludique et qui engagent le collaborateur.

Il est nécessaire de rappeler que la majorité des individus dans notre société et en entreprise ne sont pas des experts informatiques. Différentes générations se côtoient et n'ont pas la même culture ni la même sensibilité face au numérique. C'est là tout le défi que pose l'évolution de notre quotidien de plus en plus dématérialisé. Les actions de sensibilisation à la cybersécurité et, de manière plus générale, la sensibilisation au numérique doivent constituer des piliers éducatifs essentiels de nos sociétés. On parle depuis quelques mois déjà d'illectronisme, un défi adressé de plus en plus souvent par les collectivités territoriales et les associations qui doit être l'affaire de tous les acteurs : école, entreprise, cercle familial et amical.

C'est à cet enjeu que nous souhaitons répondre, en favorisant la création et l'établissement durable d'une culture de la cybersécurité afin d'accompagner la société dans le développement harmonieux des nouvelles technologies. Car aujourd'hui, aucun individu et aucune entreprise n'est à l'abri d'une attaque et d'un vol de données. S'acculturer à la cybersécurité est aussi le point de départ pour minimiser ces risques au quotidien.

C'est ainsi que nous nous sommes associés à Ipsos afin d'analyser le niveau de connaissance et d'acculturation à la cybersécurité des individus, le regard qu'ils posent sur les « dangers » du numérique, leurs aspirations et leurs besoins pour mieux se prémunir des attaques. L'étude **« Phishing, malwares, arnaques : état des lieux de la sensibilisation à la cybersécurité des collaborateurs »** à découvrir dans ces pages en est le reflet.

Cette étude est le point de départ d'un débat que nous souhaitons riche et pluriel, pour que chaque acteur y prenne part et puisse contribuer à ce que l'on cimente cette culture de la cybersécurité.

Sensibilisation à la cybersécurité : état des lieux

PRÉSENTATION DES RÉSULTATS DE L'ENQUÊTE IPSOS

Menée à l'été 2022, l'enquête a interrogé 4000 individus âgés de 18 à 75 ans dans 5 pays que sont la France, les États-Unis, l'Australie, le Canada et le Royaume-Uni. L'objectif était de mesurer le niveau d'intérêt et d'adhésion des répondants à des questions concernant la sensibilisation à la cybersécurité.

Avec l'essor du travail à distance depuis le début de la pandémie, les pratiques de cybersécurité ont-elles évolué en conséquence ? Dans quelle mesure les employés sont-ils désireux d'en savoir plus sur les meilleures pratiques et de les mettre en œuvre au travail ? Et dans leur vie personnelle ?

Un niveau élevé de connaissance des risques cybers

L'enquête révèle ainsi que près de 76 % des salariés de France, du Royaume-Uni, du Canada, d'Australie et des États-Unis déclarent avoir déjà été personnellement visés par une cyberattaque ou connaître quelqu'un qui l'a été. En ligne avec cette visualisation du « danger », un grand nombre de répondants rapportent avoir été personnellement victimes de cyberattaques : 72 % en Australie, 61 % aux États-Unis. En France, où l'actualité, professionnelle comme du point de vue du particulier a été spécialement marquée par les cyberattaques, 54 % des sondés sont d'accord avec cette affirmation.

L'étude met également en avant la « faiblesse » des Français face aux attaques : ils sont 27 % à admettre avoir été personnellement victimes d'une arnaque ou d'une intrusion contre 14 % des sondés outre-Manche. Et qu'en est-il des entreprises ? De leurs collègues, amis, familles ?

Plus d'un répondant sur trois, estime que le niveau de connaissances de l'entreprise en matière de cybersécurité est moyen à bon (34 %). Ils sont en revanche plus durs avec eux-mêmes et leurs collègues : 30 % évaluent leur niveau personnel comme bon, et 22 % déclarent que leurs collègues ont un « bon » niveau de connaissance ce qui laisse supposer un manque de formation sur le sujet et peut-être aussi d'intérêt. Moins de 10 % des répondants interrogés dans le monde considèrent que le niveau de leur entreprise, de leurs collègues et de leur propre personne est excellent (note de 10 sur une échelle de 1 à 10). Ce pan de l'enquête dénote ainsi la marge de progression réelle existant entre l'appréhension du sujet « cyber » et sa véritable connaissance.

« Ces résultats soulignent l'importance d'une formation éducative et actuelle sur la sensibilisation à la sécurité », **a déclaré Theo Zafirakos, RSSI chez Terranova Security.** « Les résultats de l'enquête indiquent que, si la plupart des gens sont conscients des cybermenaces et de leur prévalence, quel que soit la région ou le secteur d'activité, on suppose que le niveau de connaissance global est inférieur à la moyenne. La seule façon de combler ce fossé est de créer une culture organisationnelle soucieuse de la sécurité et de mettre en place une formation de sensibilisation permettant aux collaborateurs de détecter et de signaler systématiquement les cyberattaques. »

Des défis grandissants liés au télétravail

Selon l'étude, 54 % des salariés travaillent à distance, dont 34 % davantage depuis la crise du Covid-19. Et si les pays anglophones sont nombreux, notamment dans les grandes entreprises à avoir adopté cette pratique, la France se pose quant à elle en figure de résistance au changement de paradigme professionnel : 56 % des Français interrogés ne pratiquent jamais le télétravail. Pour ceux qui, toutefois, expérimentent cette situation, la majorité mondiale (54 % — 58 % en France) déclare avoir besoin d'un support informatique plus important en situation de télétravail pour éviter les problèmes de cybersécurité. Une proportion non négligeable (37 %) déclare aussi moins se soucier de cybersécurité lorsqu'ils télétravaillent.

Ils s'accordent en revanche sur la question de la montée des attaques : 58 % d'entre eux estiment que le phishing et les escroqueries sont en augmentation depuis 2020.

Selon Anselme Laubier, directeur de compte chez Ipsos, « L'accélération du télétravail lié à la crise du Covid-19 renforce la notion de responsabilité partagée concernant la cybersécurité : au niveau de l'infrastructure IT des entreprises, mais surtout au niveau des employés, qui savent identifier les risques, mais ont encore trop peu de réflexes adaptés. »

La question du besoin en sensibilisation

En ce qui concerne les formations de sensibilisation à la cybersécurité proposées par leur entreprise, les résultats sont assez surprenants compte tenu de l'état d'urgence actuel déclaré dans tous les pays interrogés en matière de cyber-risques. En effet, rappelons que l'ANSSI et Cybermalveillance.gouv par exemple en France travaillent de concert depuis 2019 pour alerter et sensibiliser la population aux risques encourus dans leur utilisation du numérique et ont même mis en place des guides d'utilisation et un numéro d'urgence pour faire face aux intrusions.

Mais qu'en est-il du côté des entreprises ? L'état d'urgence a-t-il fait bouger les lignes ?

D'après l'étude, à peine plus d'un tiers (38 %) des personnes interrogées dans le monde déclarent que leur entreprise a mis en place un programme de sensibilisation à la cybersécurité obligatoire pour tous. Si ce chiffre est plus élevé dans les pays anglophones et de culture anglo-saxonne, il est très faible en France, où seuls 25 % des répondants travaillent au sein d'entreprises ayant entrepris ce type d'actions.

45 % des entreprises françaises, selon les répondants, ne proposent aucun type de formation de sensibilisation à la cybersécurité, quand, outre-Manche, ce n'est le cas que pour 31 % des répondants britanniques. Cette donnée est ensuite très liée au début et à l'achèvement des cours de formation : seulement 29 % des répondants français annoncent avoir terminé un module quand la médiane entre tous les autres pays interrogés est de 49 %. L'Australie est le meilleur élève, avec 51 % des répondants ayant terminé leurs modules, 50 % au Canada et au Royaume-Uni.

Pour rappel: les niveaux d'achèvement de la formation de sensibilisation à la cybersécurité varient considérablement selon les pays et les entreprises...

...par pays et par tailles d'entreprises :

Par pays	Total	UK (n=500)	FR (n=500)	CA (n=1000)	AU (n=500)	US (n=1500)	1-49 salariés (n=931)	50-500 salariés (n=1271)	500+ salariés (n=1798)
Ont suivi et terminé une formation à la cybersécurité	45%	50%	29%	50%	51%	48%	22%	45%	59%

Mais comment expliquer que les formations, lorsqu'elles sont proposées par l'entreprise, ne soient pas suivies dans leur intégralité par les collaborateurs ?

« Les trois facteurs influençant la motivation des employés à participer à une formation de sensibilisation à la sécurité sont l'accessibilité, la qualité du contenu et le renforcement interne », a ajouté **M. Zafirakos.** « Proposez-vous votre formation de sensibilisation à la sécurité dans plusieurs langues ? Votre contenu d'apprentissage est-il digeste et éducatif, mais aussi attrayant ? Renforcez-vous continuellement l'importance de la sensibilisation à la cybersécurité en interne par le biais d'outils de communication ? Ce ne sont là que quelques-unes des questions que les responsables de la sécurité devraient se poser s'ils constatent des niveaux de participation à la formation ou d'achèvement des cours peu élevés. »

Pour les personnes n'ayant jamais participé à des formations de sensibilisation à la cybersécurité, deux raisons majeures apparaissent dans l'enquête : le fait qu'elles ne soient pas obligatoires a tendance à ne pas mobiliser les gens sur ces formations, ce qui laisse à penser que ce n'est pas une priorité (30 % au niveau mondial le déclarent) sauf pour la France, où seulement 11 % des répondants expliquent leur manque de participation de cette manière.

Le motif premier de cette non-sensibilisation, pour plus de la moitié des répondants (53 %) réside dans le simple fait qu'ils ne se sont pas vu offrir de formation de ce type. Un chiffre qui culmine en France avec 70 % des répondants en accord avec cette affirmation.

La question qui se pose maintenant est la suivante : le fait que de nombreuses entreprises ne proposent pas encore de formation à la cybersécurité entraîne-t-il un désintérêt des individus ?

La réponse est non : plus des deux tiers des personnes interrogées (79 %) estiment intéressante la formation en sensibilisation à la cybersécurité, même si leur entreprise ne la propose pas. Toutefois, la formation de sensibilisation à la cybersécurité ne semble pas être une priorité : 1 répondant sur 4 en moyenne dans le monde pense que la formation n'est pas nécessaire, notamment au Canada (27 %), en Australie (29 %) et aux États-Unis (27 %). Aussi, malgré un intérêt grandissant, qui peut s'expliquer par la visibilité de plus en plus importante des problématiques de sécurité numérique, les entreprises intègrent-elles la sensibilisation à leurs projets pour ces prochains mois et années ? Et surtout, comment suscitent-elles l'intérêt des plus « désengagés » ?

Pour Anselme Laubier d'Ipsos, « La part du télétravail en France reste plus basse qu'en Amérique du Nord, Royaume-Uni et Australie. Logiquement, les Français sont plus attachés aux formats en présentiel ».

Toutefois, s'ils sont intéressés, ils ne se déclarent pas ouverts à tous les formats. Dans le cadre de l'enquête, les répondants ont aussi affiché leurs préférences en matière de transmission du savoir cyber : les activités pratiques telles que les simulations de phishing (37 % des répondants dans le monde), les cours en ligne (37 %), les supports ludiques de format court (32 %) et les sessions avec instructeur (virtuelles ou en personne) semblent avoir la préférence de plus de 30 % des répondants dans le monde ; la France se distingue sur ce plan puisque ce dernier type d'apprentissage y est cité en première position, fédérant 37 % des répondants.

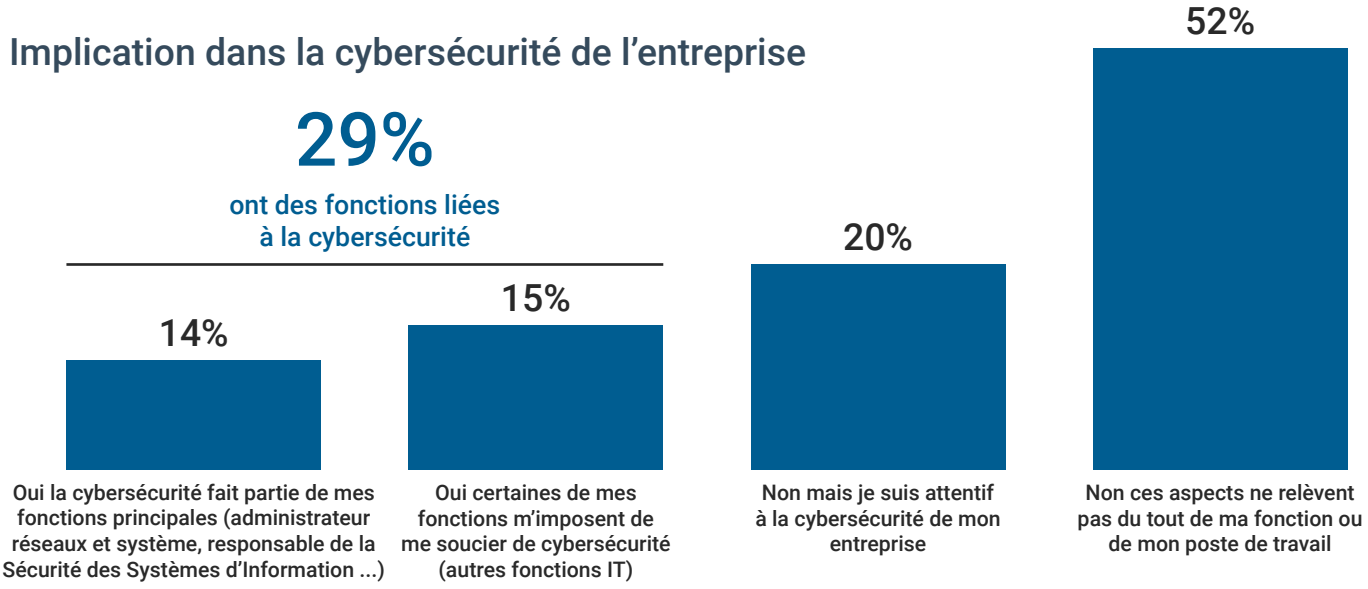
« Il est clair que les employés ont besoin d'une formation de sensibilisation à la sécurité qui soit éducative, ludique et alignée sur la culture existante de l'organisation », indique **Théo Zafirakos.** « Même un public qui préfère les sessions dirigées par un instructeur, virtuelles ou en personne, ne s'engagera pas dans un contenu de sensibilisation à la sécurité qui n'apporte pas de valeur ajoutée à ses activités quotidiennes. »

La responsabilité face aux risques

Pour plus des deux tiers (78 %) des personnes interrogées, il est du ressort de l'entreprise d'assurer la sécurité de tous ses salariés, même si la plupart d'entre elles (59 %) reconnaissent également qu'il leur incombe de protéger leur entreprise dans leurs tâches et missions quotidiennes.

52 % des salariés n'interviennent pas sur le support informatique pour des questions liées à la cybersécurité

Implication dans la cybersécurité de l'entreprise

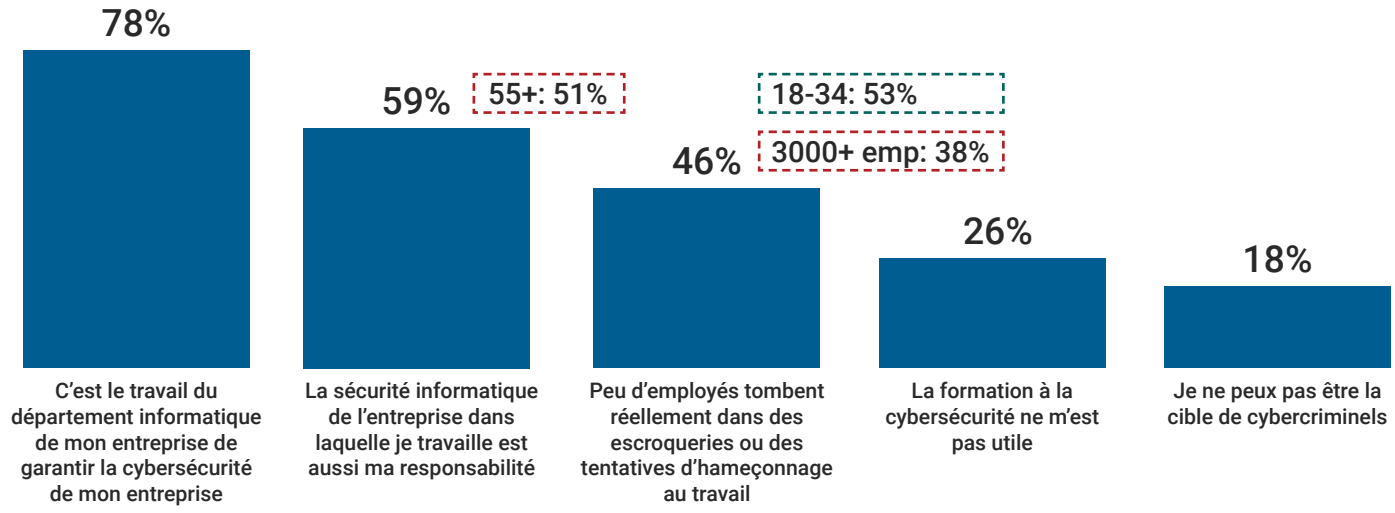


Au sein de votre entreprise, intervenez-vous sur le support informatique pour les questions liées à la cybersécurité ?

4000 répondants. Aucun filtre appliqué.

La notion de responsabilité concernant la cybersécurité est ambigüe, 3 salariés sur 4 estiment que la cybersécurité doit être garantie par le département informatique et pourtant, 6 salariés sur 10 estiment qu'elle relève aussi de leur responsabilité

% d'accord sur la responsabilité en matière de cybersécurité



Dans quelle mesure êtes-vous d'accord ou non avec chacune des affirmations suivantes ?

4000 répondants. Aucun filtre appliqué.

Toutefois, aucune autre solution ne semble envisagée. Serait-ce dû à une maîtrise très élevée des fondamentaux du numérique ? Si en France, plus de 1 personne sur 10 (19 %) souffre d'illectronisme, ce chiffre est similaire à celui étudié aux États-Unis par la National Skills Coalition. A contrario, les dernières enquêtes réalisées au niveau mondial sur le sujet par l'OCDE ont permis de mettre en lumière la très bonne maîtrise des problématiques numériques (digital literacy) en Australie, par comparaison aux marchés étudiés incluant la France, les États-Unis ou encore le Royaume-Uni.

En 2020, le sujet de l'illectronisme avait notamment été débattu au Sénat afin de pousser les pouvoirs publics et les collectivités territoriales à prendre part à l'action pour mettre fin non seulement à la fracture numérique (évoquée pour la première fois en 1996) et à l'illectronisme. Celui-ci est d'ailleurs à comprendre comme un ensemble de savoirs numériques dont les « basiques » (allumage d'un ordinateur, recherches sur Internet) sont aussi complétés de missions plus poussées (utilisation de logiciels de traitement de texte, de tableur, paramétrage d'un ordinateur, réglages Wi-Fi, etc). Un défi qui, pour reprendre l'expression du sénateur Raymond Vall, « ne s'effacera pas d'un coup de tablette magique ! ».

La société est-elle favorable à une culture cyber partagée entre tous ?

Mais, bien que tous les répondants n'aient pas été formés aux risques et aux questions de cybersécurité, ont-ils pour autant déjà mis en place certaines bonnes pratiques ? La réponse est oui, ce qui confirme l'idée qu'une culture de la cybersécurité se construit lentement, et peut être renforcée par des actions de formation. Au travail, un grand nombre de personnes interrogées connaissent les cinq principes de base pour prévenir toute attaque :

- Créer des mots de passe uniques pour chaque compte (50 %, mais seulement 38 % en France).
- Analyser minutieusement les e-mails pour détecter les signes d'hameçonnage (47 %)
- Être prudent lors de la réception d'e-mails/textes (59 %)
- Ne jamais cliquer sur les liens et les pièces jointes des e-mails et des textes non sollicités (61 %)
- Signaler les e-mails suspects aux équipes informatiques (45 %)

Le seul obstacle semble être la communication et le rôle que les individus s'attribuent en tant qu'aide potentielle pour les autres : moins d'un quart (24 %) des personnes interrogées ont déclaré partager leurs meilleures pratiques et parler des problèmes de cybersécurité avec leurs pairs, dans l'entreprise. Or, sans cela, les connaissances sont moins utiles, car c'est le nombre de personnes sensibilisées qui permettra de commencer à enrayer à la cybercrise actuelle.

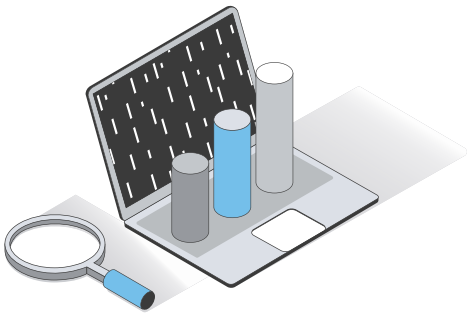
« Bien que la sensibilisation à la cybersécurité ait beaucoup progressé à l'échelle mondiale en si peu de temps, il est important d'élaborer et d'optimiser les programmes en tenant compte du présent et de l'avenir », a déclaré **M. Zafirakos.** « La complexité, les angles et les thèmes exploités par les cybermenaces courantes changent constamment à mesure que les pirates tentent de prendre le dessus. Pour cette raison, les organisations et les responsables de la sécurité doivent s'assurer que le contenu de la formation en sensibilisation à la sécurité évolue en permanence afin d'inclure les informations et les conseils les plus récents que les employés peuvent absorber et partager. »

Lorsqu'il s'agit de leur sphère personnelle, les personnes interrogées semblent un peu plus bavardes : 29 % d'entre elles disent parler des principes de cybersécurité avec d'autres personnes. Et leur connaissance des meilleures pratiques est également assez étendue, voire meilleure qu'au travail, à l'exception notable de la dimension signalement : la possibilité, pour chaque individu, de signaler une escroquerie à son fournisseur de services de messagerie, par exemple, semble être méconnue, alors qu'il s'agit potentiellement d'une mesure très efficace. Les meilleures pratiques semblent davantage observées dans la sphère privée, la question est donc de savoir pourquoi. Cet écart est-il dû au fait, précédemment mentionné qu'une majorité d'individus ne se sent pas dépositaire de la protection des données de l'entreprise et pense que c'est là le travail de l'équipe informatique ? Sont-ils, à l'inverse, plus prudents avec leurs données personnelles parce qu'ils s'en sentent naturellement responsables ?

Cette différence d'attitude entre les sphères privée et professionnelle ne peut être attribuée à une différence dans la nature des menaces, qui sont les mêmes (vol de données, virus, escroqueries et phishing), bien que les chiffres soient un peu plus élevés en ce qui concerne la cybersécurité personnelle. Ce léger écart peut s'expliquer, comme déjà mentionné, par la relative incapacité des équipes de support informatique à aider, en cas de besoin, les collaborateurs en situation de travail distanciel.

Alors, quelles sont les clés d'une généralisation de la culture cyber ?

Si cette étude a permis de mettre en lumière plusieurs pistes d'amélioration, passant en premier lieu par la généralisation des actions de sensibilisation dans le monde professionnel, il est aussi essentiel de considérer les franges de la population qui n'ont pas encore intégré (ou ont quitté) cet univers. Étendre le savoir et le mettre à la portée de tous doit faire partie des plans d'action des gouvernements, au même titre que les actions en cours pour l'indemnisation des cyberattaques, sujet largement débattu en France depuis 2021. En effet, si ces polices d'assurance aideront certainement les entreprises, il reste que les particuliers sont soumis au même danger.



Trois clés sont essentielles pour faire émerger cette culture de la cybersécurité :

- Connaître son public et en déterminer les objectifs
- Déterminer les risques propres à chacun
- Motiver l'ensemble des individus à acquérir les fondamentaux et partager leur savoir

Les fondations et l'émergence d'une culture de la cybersécurité : où en sommes-nous ?

Créer ou participer à la création d'une culture de la cybersécurité et du numérique en 2022 peut sembler anachronique. Avec la généralisation du numérique dans tous les aspects de notre quotidien, il est facile de s'imaginer que le public, dans sa vaste majorité, en détient les clés et comprend les risques sous-jacents. Pourtant l'étude menée avec Ipsos a permis de mettre en lumière, si ce n'est une totale méconnaissance, au moins une légèreté coupable dans l'appréhension du sujet. L'étude semble par ailleurs indiquer que les efforts visant à résoudre cette situation ne peuvent se limiter aux actions de formation et de sensibilisation à la cybersécurité en entreprise. Il est essentiel de les étendre à tous, et de faire de chaque individu un ambassadeur de la sécurité.

Pour y parvenir, il s'agit en premier lieu de s'attaquer à une barrière de nature socio-économique à savoir l'illectronisme.

L'ILLECTRONISME, MAL DU SIÈCLE ?

Selon une étude menée par l'Insee en 2019, 17 % de la population française n'aurait pas accès à Internet ou ne saurait pas utiliser les outils numériques. Outre-Atlantique, ce niveau se situe aux alentours des 20 % sur le continent nord-américain, un chiffre également observé au Royaume-Uni d'après les études de l'OCDE. Seule l'Australie, qui ressortait déjà comme le « bon élève » de l'étude menée par IPSOS se situe au-dessus du niveau de connaissance défini comme « bon » par l'organisation internationale.

Le travail pour lutter contre l'illectronisme ou améliorer le niveau de connaissance numérique de la population (digital literacy) est entrepris depuis peu par chaque pays, à marche forcée le plus souvent du fait de l'évolution des métiers et donc des connaissances nécessaires. On parle souvent alors de « nouvelle révolution industrielle », qui doit nécessairement s'accompagner d'une radicale révolution dans le domaine de la formation, de l'économie du savoir, de la maîtrise de certains outils indispensables, de l'accès de chacun à la culture, ces trois derniers points incluant désormais presque systématiquement le numérique.

Lors de son dernier discours officiel au Forum International de la Cybersécurité en juin 2022, Guillaume Poupard, ex-directeur de l'ANSSI abordait la question de la sensibilisation à la cybersécurité comme le grand défi de l'ANSSI aujourd'hui et demain, plus généralement de la société pour répondre à l'augmentation du poids de la vie numérique :

« Le premier sujet à mettre en œuvre, c'est celui d'une véritable sensibilisation à grande échelle sur les enjeux de cybersécurité. Si nous pouvions avoir cinq minutes de temps de cerveau de chaque Français pour passer quelques messages sur la sécurité numérique, ce serait idéal. »

Ainsi, la cyber-culture, ou culture du numérique au sens large, semble s'imposer comme LE moyen de lutter efficacement contre l'illectronisme. Mais quels en sont les pré-requis ?

La cyber-culture s'inscrit autour de quatre grands piliers, au sein de l'entreprise comme pour la société dans son ensemble :

1. Un cadre et des règles strictes pour définir les bons comportements à avoir pour se protéger des dangers numériques
2. Une éducation, une formation aux risques du numérique et un apprentissage visant à l'acquisition de compétences dans le domaine pour tous
3. Un cadre légal et réglementaire fixe sur les devoirs et droits du citoyen, comme de l'entreprise, dans l'usage du numérique
4. Une standardisation et une explication des outils technologiques pour faciliter leur accessibilité

Enfin, le dernier pilier, moins aisé à classifier demeure l'être humain. Chaque individu doit être mobilisé, ciblé par ses actions. Ce n'est que par l'intégration de tous, et ce dès le début de leur « vie numérique » que la société permettra l'émergence réelle de cette cyber-culture. Et c'est justement à l'école que cela commence…

L'ÉDUCATION AU SERVICE DE LA CULTURE NUMÉRIQUE

En France, les premiers cursus spécialisés en sécurité des services informatiques apparaissent à la fin des années 1980 (avec l'EPITA en 1989 d'abord), mais demeurent marginaux jusqu'au début des années 2000. Et si les STEM ont toujours tenu une place importante du cursus scolaire primaire comme universitaire, la spécialisation en cybersécurité, récente, demeure rare. Les cours de code n'ont, par exemple, été introduits au lycée que lors de sa dernière réforme, en 2019, et ne sont pour l'heure disponibles que sous la forme d'options.

Si la visibilité de ces métiers semble être devenue un sujet pour les médias comme pour les institutions, le manque d'étudiants dans ces filières et donc le manque de talents à recruter pour les métiers de la cybersécurité demeure criant. Une étude menée en décembre 2020 par l'éditeur Kaspersky[1] en France sur l'orientation des jeunes et leur attrait pour les métiers de la cybersécurité avait ainsi révélé que seuls 12 % des jeunes s'intéressant à une carrière dans le numérique portaient leur choix sur des études en sécurité informatique.

Mais alors, comment intéresser davantage les jeunes, si ce n'est pour les orienter vers les métiers de la cybersécurité, a minima pour les sensibiliser aux enjeux du numérique et leur permettre de « s'armer » au mieux face à une société de plus en plus virtualisée ?

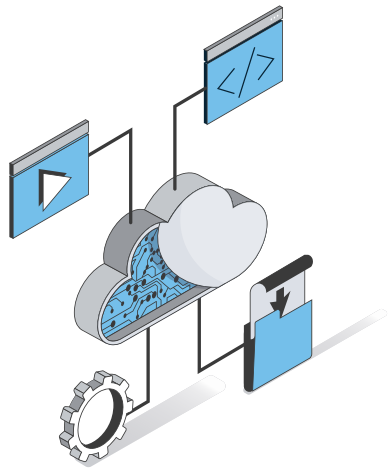
Il est dans l'ADN même de Terranova Security, de par les profils d'experts qui la composent, de penser que l'éducation joue un rôle primordial, que l'on s'éduque par le biais de l'entreprise ou dès l'entrée à « l'école ».

[1] « Préparer l'avenir numérique, c'est investir sur l'humain », Kaspersky, janvier 2021

Dalila Ben Attia, Directrice Générale France de Terranova Security est ainsi diplômée d'un Bachelor en Sciences de l'Éducation de l'Université de Lille et a suivi une préparation prédoctorale sur les sciences de l'éducation et plus particulièrement sur la manière d'engager et de motiver les apprenants par le biais de l'apprentissage en ligne. Pour elle, la « formation, la sensibilisation et les différentes actions qui en découlent doivent être portées à la connaissance de tous et doivent se faire dans la continuité ». Et pour atteindre ce mode d'apprentissage, il « est essentiel que les pouvoirs publics et les entreprises s'engagent à mettre en place des actions de sensibilisation ouvertes à tous, et communiquent sur ces initiatives. Ce dernier point est crucial : en incluant chaque personne dans le processus, et c'est d'ailleurs l'un des principaux enseignements de l'étude menée avec Ipsos, nous répondrions à l'intérêt existant et offririons une réponse aux inquiétudes grandissantes de chacun. »

UNE ASSOCIATION TRIPARTITE : POUVOIRS PUBLICS, ENTREPRISES ET INDIVIDUS

Faire émerger une cyber-culture s'apparente à la construction d'un bâtiment, dont trois composantes majeures permettent de cimenter l'ensemble : les pouvoirs publics, les entreprises et les individus. Chacun a ici son rôle à jouer, dans des registres distincts :



- Les pouvoirs publics, en assumant un double rôle : celui d'éducation et de protection des citoyens, par le biais de l'information, de réformes de l'apprentissage, de sensibilisation aux causes importantes et de mise à disposition d'outils.
- Les entreprises et les ONG, en devenant un vecteur de transmission du savoir par la mise en place de formations et de règles acculturant les collaborateurs aux problématiques et aux bons usages du numérique.
- Les individus, par leur adhésion et une attitude plus responsable dans la prise en main des outils, par l'évangélisation du numérique au sein du cercle familial, amical, utilisant les instances de socialisation comme un vecteur de partage et d'acculturation.

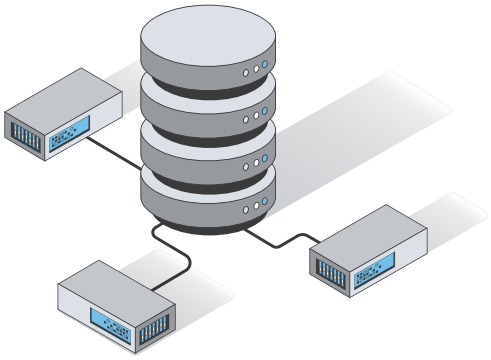
« Au niveau global, certains secteurs d'activité ont déjà largement mis en place des parcours de formation et de sensibilisation à la sécurité : les entreprises de plus de 500 employés, celles du secteur de l'information et de la communication, le secteur de la finance et de l'assurance, ou les professions scientifiques et techniques. Dans ces secteurs, les employés se sentent davantage concernés par le vol de données sensibles de l'entreprise, et sont plus enclins à se dire garants de la sécurité informatique de leur entreprise. Ils sont également plus susceptibles de partager les bonnes pratiques en matière de cybersécurité avec leur entourage, ou de signaler les attaques en cours à leur département IT. À l'inverse, les employés travaillant dans les secteurs de la distribution, des transports, et du tourisme/hospitalité, ou dans l'immobilier, se voient moins proposer ce type de formation. Il en résulte une prise de responsabilité relativement plus faible, et une moindre propension à reporter les attaques auxquelles ils font face ou à partager les bonnes pratiques avec leur entourage », **commente Anselme Laubier, Research Manager chez IPSOS.**

À l'heure où le monde, et plus particulièrement la sphère professionnelle, ne parle que des digital natives et de leur apport à la société grâce à leurs connaissances et leur maîtrise du numérique, il paraît important de rappeler qu'ils ne sont pourtant pas les seuls usagers des internets. En outre, si les jeunes générations sont hyperconnectées, elles ne sont pas nécessairement au fait des risques liés à leur utilisation des services numériques (les problématiques de cyberharcèlement, de piratage et de création de faux comptes sur les réseaux sociaux en sont la preuve). Aussi, le pilier de l'éducation, de la sensibilisation, ou même de l'éveil au numérique concerne toutes les générations, toutes les catégories socio-professionnelles et toutes les origines…

De nombreuses initiatives ont d'ailleurs vu le jour, émanant de ces trois grands « groupes » au fil des années, à l'instar d'Emmaüs Connect, qui avait mis en place « Les Cahiers de l'inclusion numérique », faisant écho à la loi de 2018 du même nom. Plus récemment, le gouvernement avait aussi mis en place des « Café Transfo », des lieux d'échange et de partage de bonnes pratiques pour accélérer notamment la transformation du service public, grande source d'inspiration et moteur du changement et de l'adhésion au numérique. Des guides d'utilisation numérique ont aussi vu le jour, et des cours d'utilisation des outils numériques sont mis en place par les collectivités territoriales pour aider tous les citoyens.

Et c'est justement parce que ces actions sont entreprises et impliquent des publics, plus ou moins « touchés » par le numérique, mais partageant des problématiques similaires que le monde se numérise, les usages aussi et il est temps de s'y accoutumer, tout en restant en sécurité. Et le progrès ne semble pas en passe de s'arrêter.

Le besoin urgent d'une base commune de connaissances sur la technologie numérique



Vivrons-nous tous dans le métavers ? Les réseaux sociaux prennent-ils le contrôle de nos vies ? D'après une enquête des grandes tendances des 25 prochaines années préparée par les analystes du cabinet Gartner, de nombreuses technologies influenceront le cours de la vie des professionnels comme des particuliers. C'est notamment le cas du Web3, du métavers, du cloud computing, voire d'un champ bien plus sulfureux et polémique, celui des technologies transhumanistes qui touchent au cœur même de l'humanité.

Le pacemaker en est une illustration, de même que la puce sous-cutanée NFC, particulièrement utilisée en Scandinavie dans le cadre du processus de numérisation du dossier patient. C'est un fait, ces objets connectés, au même titre que les montres ou téléviseurs, peuvent être la cible de cyberattaques. Or, si cela se révèle gênant dans le cadre d'un dispositif classique de type IoT (Internet des Objets), un implant connecté est évidemment nettement plus dangereux s'il peut être, par exemple, commandé à distance. Un sujet pris particulièrement au sérieux par la Commission Européenne, qui a statué mi-septembre 2022, au travers du Cyber Resilience Act, sur un durcissement des règles pour les constructeurs d'objets connectés et les développeurs logiciels, afin de prévenir les failles et intrusions potentielles.

En sus des IoT, l'intelligence artificielle (IA) peut poser des enjeux en matière de sécurité bien que ses applications et bénéfices concrets pour l'utilisateur existent déjà et soient visibles au quotidien. Une étude menée sur le sujet, aux États-Unis par Blumberg Capital révélait ainsi que l'IA et ses capacités rendent anxieux la moitié des consommateurs américains. Et si au cours des trois dernières années, les applications de l'IA adjuvante de l'humain se sont démultipliées, un article co-écrit par des chercheurs spécialisés en IA et publié par la revue AI Magazine pose toutefois de nouvelles questions sur une IA qui surpasserait l'homme, le rendant inférieur et presque dans « l'obligation » de s'augmenter pour retrouver son caractère supérieur. La possibilité d'un avenir encore plus connecté multiplie par conséquent les risques de cybersécurité et les surfaces d'attaques, d'ores et déjà étendues.

Mais, outre le déficit d'information sur les risques cyber, existe-t-il d'autres éléments pouvant freiner la cyber-culture ?

TECHNOPHILES, TECHNOPHOBES : DES FREINS À LA CULTURE DE SÉCURITÉ ?

Dans son dernier ouvrage, Homo Numericus, l'économiste Daniel Cohen, professeur à l'École Nationale Supérieure de France ouvre d'ailleurs le débat sur l'utilité du numérique, qui « éloigne les gens », les fait douter, et plus précisément sur l'impact psychologique des réseaux sociaux et autres mondes virtuels sur les individus. Si les réseaux sociaux ou même les mondes virtuels comme Roblox ou Fortnite ont conquis la quasi-totalité de la société, particulièrement chez les générations les plus jeunes, bien que cela soit plus nuancé selon les régions du monde, il apparaît clairement que cela n'est pas synonyme de culture numérique.

Les récits d'arnaques, de dérives pleuvent chaque jour à la Une des médias, et si cela fait douter certains de la fiabilité des outils, cela n'entraîne pas pour autant de prise de conscience suffisamment décisive ni, plus modestement, de modification des comportements. L'isolement qu'évoque Daniel Cohen semble être un facteur hautement perturbateur et adverse en ce qui concerne l'émergence de cette fameuse cyber-culture ou culture du numérique. Une projection trop constante dans les mondes virtuels, motivée par la recherche d'un refuge loin de la « réalité réelle », en coupant l'individu du monde, est un frein de moins en moins anecdotique à la socialisation, et donc au partage, essentiel, des savoirs.

Cette passion du virtuel et la méconnaissance de ses risques intrinsèques sont mises en évidence par les rapports d'incidents régulièrement publiés par les éditeurs d'antivirus et l'ANSSI ou encore par les dépôts de plainte effectués auprès de la CNIL ou des forces de l'ordre.

On dit souvent que, de la passion à la haine, il n'y a qu'un pas : si les technophiles ne sont pas nécessairement partie prenante de l'acculturation au numérique, les technophobes ne sont évidemment pas plus aidants. Utilisant le spectre toujours efficace de Big Brother, et de la surveillance par l'état des activités des individus, ou bien la menace de la perte d'identité ou même du sens de la vie, les technophobes sont les alliés objectifs de l'ignorance cyber. La France est d'ailleurs régulièrement singularisée pour sa technophobie supposée, souvent opposée au progressisme de ses voisins allemands ou anglais : d'après une étude menée en décembre 2020, 56 % des Français seraient de plus en plus inquiets face aux nouvelles technologies[2].

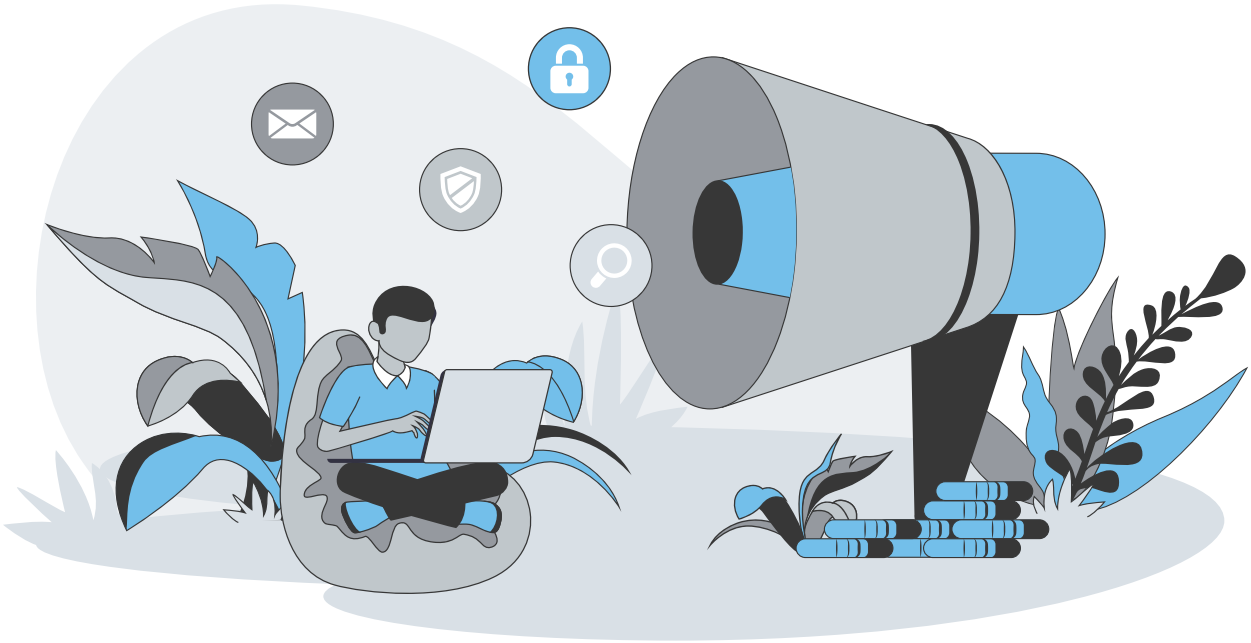
Et alors que le monde ne cesse d'intégrer davantage le numérique au quotidien de chacun, les comportements découlant de ces deux profils types posent question : comment rallier ? Est-ce là une question d'inclusion ? De communication ?

[2] Etude IFOP pour l'Académie des Technologies, **« LE REGARD DES FRANÇAIS SUR LES NOUVELLES TECHNOLOGIES À L'HEURE DES DÉBATS AUTOUR DE LA 5G »**, Décembre 2020

Conclusion

L'enquête menée avec Ipsos, présentée dans ce rapport, a été le point de départ d'une réflexion plus large : en dernière analyse, il est de la responsabilité des individus de devenir, s'ils le souhaitent, les ambassadeurs indispensables de la cyber-culture, en quelque sorte les héros de l'époque. Leur donner la parole est aujourd'hui fondamental afin de mesurer leur niveau d'intérêt pour le sujet de la cyber-protection, mais aussi, surtout, leur volonté de s'engager pour relever, collectivement, l'immense défi d'inverser le cours de l'histoire.

Nombreuses sont les questions en suspens : comment éveiller puis maintenir leur intérêt, quelles technologies ou méthodes employer, quelle reconnaissance demain pour ces nouvelles compétences ? Autant d'aspects qu'il sera nécessaire de surveiller et d'analyser dans les prochains mois et années, à mesure que les stratégies pour le numérique s'intensifient partout dans le monde.



À PROPOS DE TERRANOVA SECURITY

Terranova Security est un leader mondial de la formation et la sensibilisation à la cybersécurité et un partenaire de choix pour les entreprises. Les programmes de sensibilisation et les simulations de phishing de Terranova Security offrent aux organisations du monde entier le contenu de la plus haute qualité, la plateforme de sensibilisation à la sécurité la plus universelle, le plus grand portefeuille d'outils de formation et de communication et le simulateur de phishing le plus intuitif du secteur. Terranova Security travaille avec des organisations et des équipes de sensibilisation à la sécurité du monde entier pour concevoir des programmes, aidant à réduire considérablement le facteur de risque humain afin de contrer efficacement toutes les cyberattaques. Terranova Security est membre du groupe spécialiste mondial de la cybersécurité, Helpsystems. Pour en savoir plus, rendez-vous sur le site de Terranova Security.

Contacts presse :
Omnicom Public Relations Group pour Terranova Security
Carla Portier – 06 77 84 02 60
France.terranova-security@omnicomprgroup.com

À PROPOS D'IPSOS

Ipsos est l'un des leaders mondiaux des études de marché et des sondages d'opinion, présent dans 90 marchés et comptant plus de 18 000 collaborateurs. Nos chercheurs, analystes et scientifiques sont passionnément curieux et ont développé des capacités multi-spécialistes qui permettent de fournir des informations et des analyses poussées sur les actions, les opinions et les motivations des citoyens, des consommateurs, des patients, des clients et des employés.

Nos 75 solutions s'appuient sur des données primaires provenant de nos enquêtes, de notre suivi des réseaux sociaux et de techniques qualitatives ou observationnelles. Notre signature « Game Changers » résume bien notre ambition d'aider nos 5 000 clients à évoluer avec confiance dans un monde en rapide évolution. Créé en France en 1975, Ipsos est coté à l'Euronext Paris depuis le 1er juillet 1999.

L'entreprise fait partie des indices SPF 120 et Mid-60 et est éligible au service de règlement différé (SRD). ISIN code FR0000073298, Reuters ISOS.PA, Bloomberg IPS:FP www.ipsos.com

Notes

Notes

Notes

WWW.TERRANOVASECURITY.COM/FR-FR | WWW.IPSOS.COM

© Fortra, LLC and its group of companies. All trademarks and registered trademarks are the property of their respective owners.