LES DOSSIERS TECHNIQUES

Sensibilisation du collaborateur

Le maillon essentiel de la cybersécurité

Mars 2023

CLUSIF

Table des matières

Remerciements

Le Clusif tient à mettre ici à l'honneur les personnes qui ont rendu possible la réalisation de ce document, tout particulièrement :

Le responsable du groupe de travail :

Grégory	**ADROT**	ARMAND THIERY
Michaël	**JACQUES**	CSB School

Les contributeurs :

David	**BLONDEAU**	SESAN SERVICE NUMÉRIQUE DE SANTÉ
Marc-Henri	**BOYDRON**	CYBER COVER
Emmanuel	**DOREAU**	INOVIE
Raphaël	**DUVEAU**	NEO CONSULTING FOR YOU
Éric	**EGEA**	NTT FRANCE
Benoit	**FUZEAU**	CASDEN BANQUE POPULAIRE
Michel	**GERARD**	CONSCIO TECHNOLOGIES
Christophe	**GIRAULT**	IRP AUTO
Marc-Éric	**LEBRUN**	ILEX INTERNATIONAL
Thomas	**LE COZ**	ARSEN
Hervé	**MAFILLE**	UVU GROUP
Thomas	**MERLY**	ELIADE
Philippe	**SOLA**	AUCAE
Anne-Catherine	**VIE**	ALL4TEC
Philippe	**WURTHEISER**	HUAWEI

Le Clusif remercie également les adhérents ayant participé à la relecture.

1 Introduction

Ce document a été rédigé pour vous fournir des pistes et des points clés à prendre en compte dans la mise en œuvre d'une campagne. La sensibilisation doit s'adapter en fonction de la taille, de la maturité, de la culture de l'organisme et du budget disponible. Dans ce document, et du point de vue de la sensibilisation, le responsable de la sécurité des systèmes d'information (RSSI) est vu comme la personne qui s'occupe de la démarche de sensibilisation. Ce n'est pas forcément lui qui anime les sessions.

Les RSSI le répètent souvent : la sécurité est l'affaire de tous.

Dans un environnement numérique et totalement interconnecté, les cyberattaques sont en constante augmentation. L'hameçonnage reste, selon l'IC3[1], le vecteur d'infection le plus courant. En effet, la messagerie électronique n'est plus un outil réservé au monde de l'entreprise. Quasiment chaque particulier en possède une. Les attaques par rançongiciel ont augmenté de 255 % selon l'Agence nationale de la sécurité des systèmes d'information (ANSSI[2]), passant de 54 incidents signalés en 2019 à 192 en 2020… Toujours selon l'IC3, l'usurpation d'identité en entreprise, qui se matérialise par la fraude au président, n'est pas la menace la plus importante pour une organisation, mais reste l'une des attaques les plus rémunératrices pour les cybercriminels. Les coûts de remédiation explosent, et, dans les situations les plus critiques, provoquent des faillites.

Depuis 2020, le monde connaît une crise sanitaire qui a aussi des répercussions sur les organisations en matière de prévention des risques cyber. La pandémie de Covid-19, aidée par la massification du télétravail, a engendré une augmentation du risque. Dans un rapport publié par Verizon[3], 85 % des compromissions de données sont imputables à des comportements humains. Dans ce contexte, il devient vital et urgent pour les entreprises de sensibiliser leurs collaborateurs pour faire face à ces menaces.

En plus des mesures barrières déjà en place, il est maintenant fortement recommandé de prendre des actions de sensibilisation et de communication spécifiques aux risques de l'organisation. Elles vont permettre d'informer les collaborateurs à la fois sur les risques, mais aussi sur les moyens de s'en prémunir. Elles fédéreront les collaborateurs autour d'un sujet auquel ils seront confrontés aussi bien dans leur vie professionnelle que personnelle.

Durant la rédaction de cet ouvrage, nous avons sollicité les membres de l'espace RSSI du Clusif afin d'avoir une vision de ce qu'ils mettaient en œuvre. Trente-huit participants ont pris le temps de répondre à un questionnaire sur leur façon d'aborder et de mettre en œuvre leur sensibilisation.

---

[1] Rapport de l'IC3

https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf

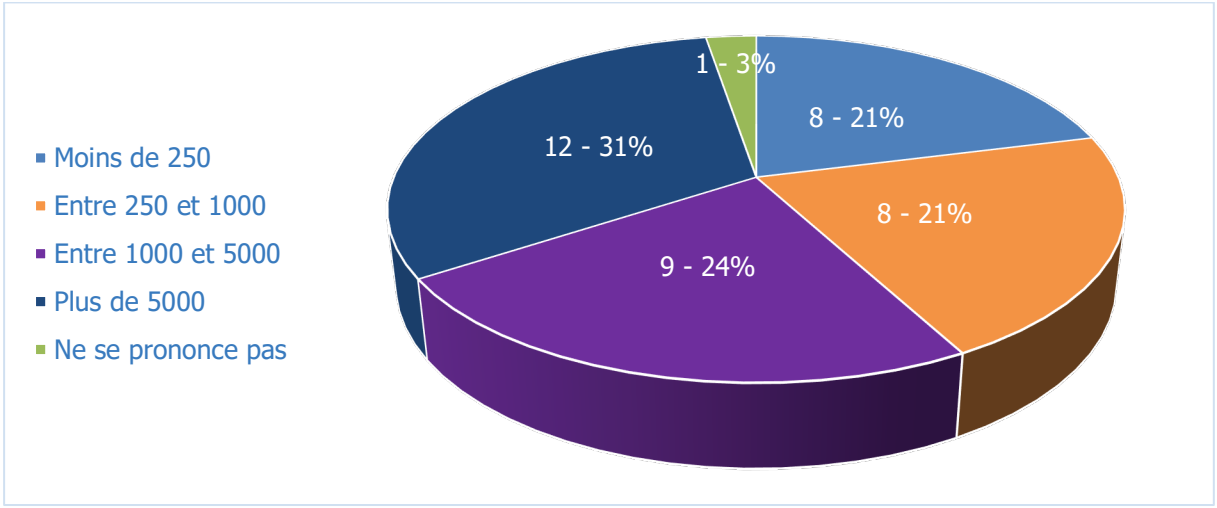
[2] Rapport du Cert-FR

https://www.cert.ssi.gouv.fr/cti/CERTFR-2021-CTI-001/

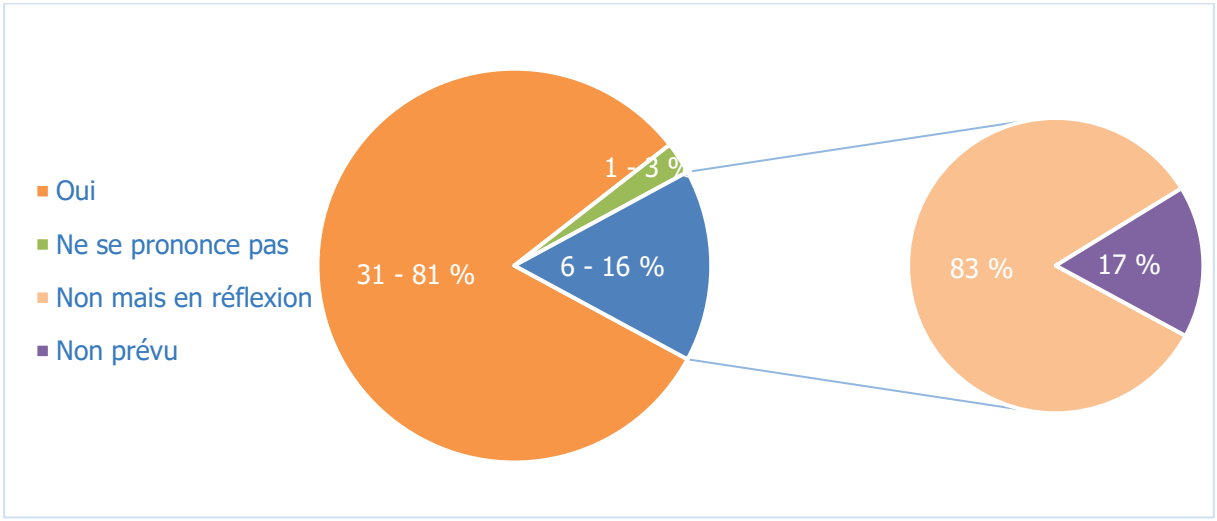
[3] Rapport Verizon

https://www.verizon.com/business/fr-fr/resources/reports/dbir

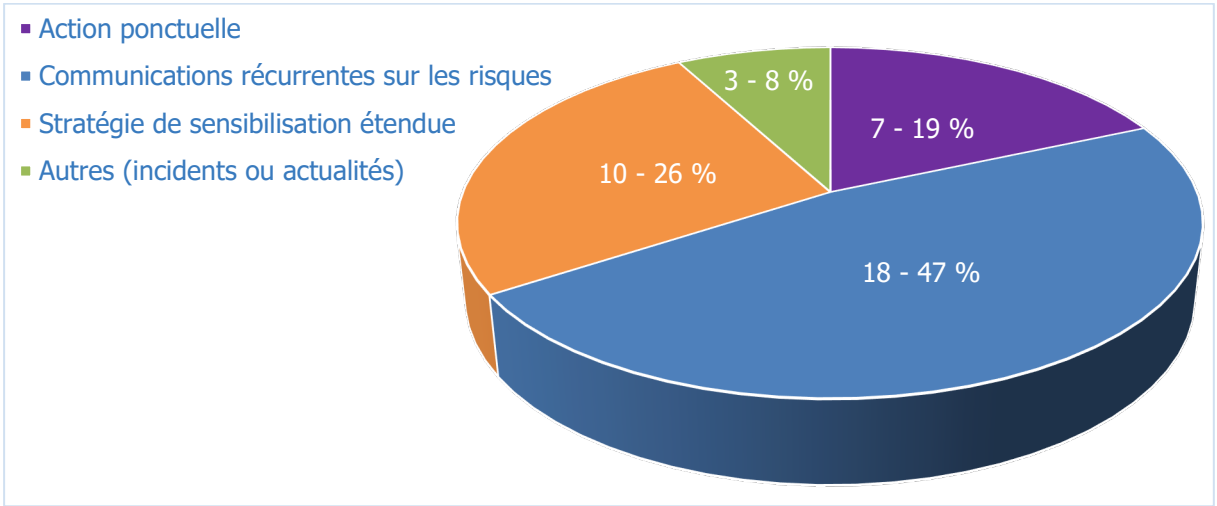
Profil des organisations



Les organisations disposent-elles d'un programme de sensibilisation ?



Quelle est la fréquence des campagnes



2 Panorama des menaces

Lors de la 22e édition du **Panorama de la cybercriminalité**, de nombreuses thématiques ont été présentées par les intervenants.

En substance, malgré une année plus singulière, la cybercriminalité n'a pas diminué. Et ce, malgré une « trêve » annoncée en mars 2021 par des groupes de cybercriminels.

Le directeur de l'ANSSI, Guillaume Poupard, a bien expliqué que « *la croissance de la cybercriminalité n'est pas uniquement liée à la pandémie mondiale. L'appât du gain reste une source de motivation intarissable* ». Les rançongiciels sont plus que toujours en augmentation, impactant les entreprises de toute taille, mais aussi les collectivités territoriales ; comme l'explique Jérôme Poggi, RSSI de la Ville de Marseille, invité à partager son retour d'expérience sur l'attaque rançongiciel qui a touché sa ville.

On constate une professionnalisation du rançongiciel permettant une meilleure rentabilité et montrant une structuration avec une chaîne d'intervenants de la création (développement d'outils spécifiques), à la revente avec un service après-vente (négociation sur la rançon, accompagnement des clients dans le paiement en cryptomonnaie, blanchiment d'argent, etc.).

Bien que moins médiatisé, l'espionnage industriel est aussi en hausse, avec des cas graves observés.

L'attaque par les tiers (« *supply chain attack* ») en est un bon exemple :

- NotPetya[4] ;
- Solarwinds[5] ;
- Vietnam, attaque de l'autorité de certificat nationale[6] ;
- logiciel de taxes préalablement infecté par le malware GoldenSpy[7].

L'Internet des objets (IoT) est devenu une cible de choix. Avec l'avènement des voitures connectées ou d'autres objets, la surface d'attaque ne fait que croître. La sécurisation de ces objets doit être intégrée dès la conception dans les projets correspondants (« sécurité dès la conception » ou « Security by Design »).

---

[4] NotPetya – Wikipédia

https://fr.wikipedia.org/wiki/Cyberattaque_NotPetya

[5] Solarwinds – US Government

https://www.gao.gov/blog/solarwinds-cyberattack-demands-significant-federal-and-private-sector-response-infographic

[6] Supplychain Attack – Vietnam – Techtribune.net

https://fr.techtribune.net/securite/lattaque-de-la-chaine-dapprovisionnement-logicielle-frappe-lautorite-de-certification-du-gouvernement-du-vietnam/66506/

[7] GoldenSpy – TrustWave

https://www.trustwave.com/en-us/resources/library/documents/the-golden-tax-department-and-the-emergence-of-goldenspy-malware/?utm_source=sl-blog&utm_medium=banner&utm_campaign=goldenspy

En parallèle, les sanctions[8] annoncées par le règlement général sur la protection des données (RGPD) se durcissent. Depuis 2020, plusieurs sociétés ont été contraintes de payer des amendes pour non-conformité, avec des montants conséquents pour certaines.

La tendance nous montre que le rançongiciel est parmi les principales menaces, largement médiatisée et très impactante. Il est important de mettre en place des actions, des contre-mesures et une gestion de crise adéquates.

Les dernières éditions du Panorama de la cybercriminalité confirment bien cette tendance.

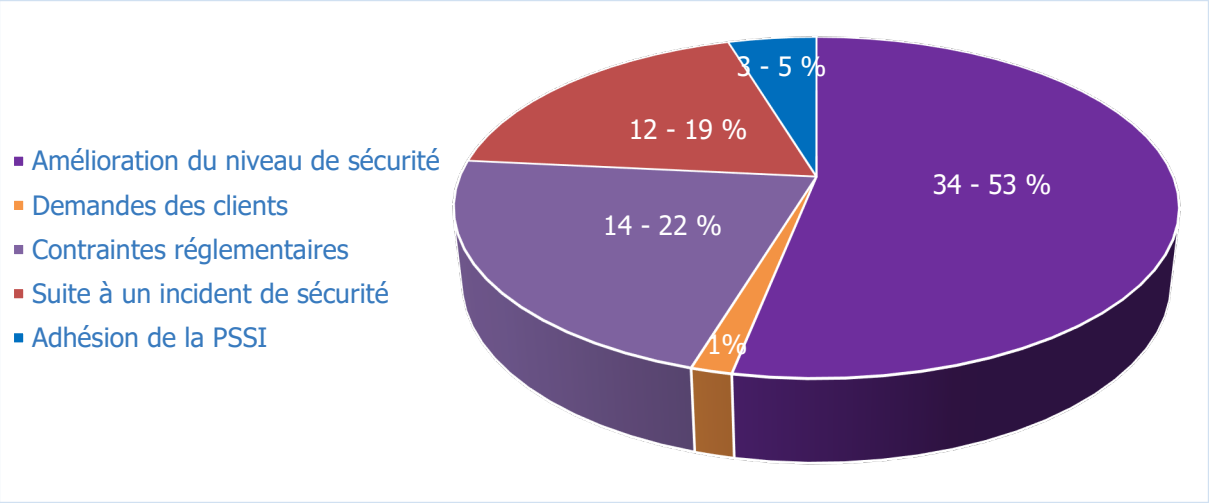
Néanmoins, ceci n'est que la partie visible de l'iceberg, de nombreux vecteurs d'attaques – parfois moins médiatisés auprès du public – nécessitent également d'être vigilants et prêts, car les dégâts peuvent être importants tant en termes d'image que financiers. La sensibilisation est une manière d'éduquer et de faire progresser les collaborateurs, qui sont souvent le premier rempart.

[8] CNIL – Bilan 2022 de son action répressive
https://www.cnil.fr/fr/sanctions-et-mesures-correctrices-la-cnil-presente-le-bilan-2022-de-son-action-repressive

3 Pourquoi sensibiliser ?

Lors de la mise en ligne du questionnaire, nous avons sollicité les membres de l'espace RSSI du Clusif pour connaître les principaux objectifs de leurs campagnes de sensibilisation.

La majorité souhaite ainsi voir une amélioration de son niveau de sécurité, mais aussi faire face à des contraintes réglementaires et, malheureusement, à postériori, réagir à la suite d'un incident de sécurité pour ne plus que cela se reproduise.



La sensibilisation est un travail de fond qui nécessite une récurrence des messages pour améliorer la transmission, l'apprentissage et l'assimilation des bonnes pratiques et des exigences parfois sectorielles de la sécurité. Le collaborateur est d'abord un citoyen, le manque de sensibilisation à la cybersécurité dans le parcours éducatif scolaire oblige les entreprises à développer des contenus pédagogiques pour leurs collaborateurs.

Amélioration du niveau de sécurité

Le respect obligatoire de certains référentiels de cybersécurité inclut des actions de sensibilisation (ISO 27001, *Guide d'hygiène informatique* de l'ANSSI, etc.). De plus, certaines compagnies d'assurance imposent la mise en œuvre de campagnes régulières de sensibilisation comme prérequis à la souscription d'une couverture d'une cyberassurance.

- Permettre d'identifier le référent sécurité

Le RSSI est la personne dont l'une des charges principales est d'assurer l'organisation et l'animation de la sécurité du système d'information (SSI) au sein de l'organisation. La sensibilisation permet alors aux collaborateurs de l'identifier et de le positionner, lui ou le service qu'il représente au sein de l'organisation, comme point de référence en charge des questions de sécurisation et de protection du patrimoine informationnel. Il est à contacter pour toutes les questions associées à la SSI.

- Sensibiliser sur la PSSI et l'organisation SSI

La politique de sécurité du système d'information (PSSI) est le document de référence pour toutes les questions touchant à la protection du système d'information. Sa compréhension n'est pas toujours évidente pour les collaborateurs et elle doit donc être vulgarisée afin de faire connaître sa raison d'être, son contenu et son objectif pour faciliter la compréhension et l'acceptation par les collaborateurs.

Sensibiliser sur la politique de sécurité doit aussi faciliter la compréhension des enjeux et des risques pour amener le collaborateur à une prise de conscience et ainsi en faire un contributeur/acteur de la SSI dans l'organisation. Le collaborateur, quels que soient son service et son niveau hiérarchique, peut être la cible de diverses tentatives d'approche (ingénierie sociale, hameçonnage) afin de collecter de l'information sur lui, ses collègues ou, plus globalement, l'environnement au sein de l'organisation.

- Sécurité de l'information dans la gestion de projet

Il convient de transmettre aux chefs de projet, les bonnes pratiques et les compétences de « sécurité dès la conception » pour la mise en œuvre d'un changement (transformation numérique) conforme aux exigences de sécurité détaillées dans la PSSI. Le chef de projet devient alors le relais de la sécurité auprès des équipes et doit être un interlocuteur dans les campagnes de sensibilisation pour appuyer et mettre en œuvre les messages et bonnes pratiques.

- Personne « cible »

Salarié ou service exerçant des fonctions attractives pour les cybercriminels. Il doit ou devrait faire l'objet de session de sensibilisation adaptée aux risques spécifiques à ses fonctions et/ou aux flux d'informations auxquels il a accès.

  - Sensibilisation et soutien de la direction générale et son adhésion à la sensibilisation des collaborateurs

La direction générale doit être un « sponsor » (à tous les niveaux) de la démarche de sensibilisation. Elle doit y adhérer, être un exemple et un « moteur » dans la promotion de la sensibilisation. Pour cela, il faut qu'en amont la ou les directions soient impliquées dans une campagne de sensibilisation spécifique et correspondant à leur positionnement dans l'organisation (population cible).

Co-construction des objectifs de sensibilisation avec la direction générale : c'est le « Graal » de la sensibilisation.

- Améliorer le niveau de compréhension de la SSI par les collaborateurs

La sensibilisation permet de démystifier les aspects techniques et organisationnels de la SSI, ainsi que les techniques d'attaque, afin que les collaborateurs puissent mieux déjouer ces dernières.

Certaines menaces peuvent être spécifiques au type d'organisation, c'est donc au RSSI de construire sa campagne en fonction de son environnement et son exposition. Une bonne campagne ne se livre pas clé en main, elle est le résultat d'une analyse de risque préalable.

Dans le cadre réglementaire

Il existe plusieurs lois, directives et réglementations imposant la sensibilisation des collaborateurs, en voici deux parmi les plus courantes.

3.1.1 RGPD

Avec l'entrée en vigueur en mai 2018 du règlement (UE) 2016/679, le RGPD, il incombe aux responsables de traitement de se conformer à leurs obligations, notamment en matière de sensibilisation. Bien qu'il n'y ait pas d'article spécifique consacré à la sensibilisation, cette dernière doit-être réalisée de manière à faire connaître au sein de l'organisation les obligations liées au RGPD.

Les collaborateurs manipulant des données personnelles ne devraient pas ignorer les exigences, obligations et pénalités en cas de non-conformité. La sensibilisation devient donc essentielle dans la construction de la conformité.

La CNIL précise que sensibiliser est une précaution élémentaire et qu'il faut : « *Sensibiliser les utilisateurs travaillant avec des données personnelles aux risques liés aux libertés et à la vie privée, les informer des mesures prises pour traiter les risques et des conséquences potentielles en cas de manquement. Organiser une séance de sensibilisation, envoyer régulièrement les mises à jour des procédures pertinentes pour les fonctions des personnes, faire des rappels par messagerie électronique, etc.* »

3.1.2 Loi de programmation militaire 2013

Promulguée le 18 décembre 2013, la loi de programmation militaire, par le biais d'arrêtés sectoriels, impose aux opérateurs d'importance vitale, des règles de sécurité. Parmi ces règles, la gouvernance pose des exigences en termes de sensibilisation et de formation. C'est à chaque opérateur, et en fonction de son secteur, de mettre en place la sensibilisation qui lui incombe.

Dans un cadre contractuel

3.1.3 Contrats de sous-traitance

Dans le cas d'entreprises fortement sécurisées, le sous-traitant est souvent un maillon faible exploité. En atteste la recrudescence des attaques par les tiers (Supply Chain Attack). C'est pourquoi le cadre réglementaire se renforce autour des contrats de sous-traitance.

Le RGPD, dont on a déjà parlé précédemment, encadre la sous-traitance dans son article 28,

avec, par exemple, le premier alinéa demandant de faire « *uniquement appel à des sous-traitants qui présentent des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du présent règlement et garantisse la protection des droits de la personne concernée* ».

Lors de l'établissement d'un contrat de sous-traitance, il est recommandé la mise en place d'un plan d'assurance sécurité (PAS), qui doit évoquer la sécurité des ressources humaines avec entre autres la sensibilisation et la formation aux enjeux de sécurité.

Ce dernier point est d'ailleurs mentionné dans le guide de l'ANSSI sur l'externalisation, en conseillant que le candidat à un contrat de sous-traitance indique dans sa réponse : « *[…] la fréquence et le contenu des actions de formation et de sensibilisation des personnels de l'hébergeur aux enjeux de sécurité* ».

On peut imaginer que, dans un futur proche, les contrats critiques puissent exiger la sensibilisation des collaborateurs du sous-traitant afin de se protéger des risques en cascade ou de respecter les termes de leur contrat d'assurance.

3.1.4 Cyberassurances

- La mise en place d'une démarche cyberassurance comme levier de sensibilisation de la direction de l'entreprise

La mise en place d'un contrat de cyberassurance permet, par la nature des informations attendues et collectées, d'aider la direction de l'entreprise à mieux apprécier son niveau d'exposition et les vulnérabilités potentielles auxquelles elle fait face.

Dans un premier temps, les compagnies d'assurance vont s'appuyer sur leur propre questionnaire (analyse de la gouvernance), afin de dresser un tableau exhaustif du niveau de maturité cyber de l'organisation à assurer. Ce recueil d'informations permet de comprendre l'exposition aux risques et la façon dont l'entreprise les gère, cet exercice pouvant parfois conduire à des améliorations dans leur gestion.

Les compagnies d'assurance viendront souvent compléter ce recueil d'informations par un audit technique (scan de vulnérabilité, audit de surface, etc.) avec établissement d'un « *scoring* ». L'exploitation des résultats de ce rapport se révèle être, dans de nombreux cas, un moyen de renforcer sa sécurité.

À travers cette démarche, la direction d'une entreprise pourra prendre conscience, si nécessaire, du risque financier que font peser les risques numériques. Elle comprendra le chemin réalisé en termes de gouvernance de sa sécurité informatique, et les efforts à poursuivre, légitimant encore davantage l'importance du RSSI au sein de l'organisation.

- Les assureurs et la sensibilisation des collaborateurs

Dans un contexte tendu, avec une capacité du marché de la cyberassurance limité, il est de plus en plus difficile pour les entreprises de trouver un assureur capable de couvrir leurs cyberrisques avec des niveaux de garantie élevés.

En effet, face à une sinistralité en très forte augmentation (fréquence et intensité), les compagnies d'assurance deviennent de plus en plus sélectives, privilégiant les organisations offrant le risque moindre et les mieux sécurisées. Dans ce contexte, l'assureur va encourager une organisation à adopter une bonne gouvernance de sa sécurité informatique, imposant en particulier dans les organisations importantes, une politique régulière de sensibilisation de ses collaborateurs.

Aux yeux des cyberassureurs, la composante humaine est un facteur critique de cybersécurité. La capacité d'une organisation à sensibiliser et former les équipes opérationnelles, et pas seulement les équipes informatiques, est un indicateur important du niveau de maturité de l'entreprise face aux cyberrisques.

L'assureur souhaitera en savoir davantage sur la formation des équipes en charge de la SSI et de la gestion des risques.

L'évaluation générale de l'organisation par l'assureur repose notamment sur :

- une culture d'entreprise dans laquelle la sécurité informatique est intégrée dans la sensibilisation de chaque collaborateur ;
- la capacité de l'organisation à identifier et à prévenir ces risques.

Pour les compagnies d'assurance, la sensibilisation des collaborateurs aux cyberrisques est un élément important qui permet de minimiser l'exposition d'une organisation aux cybermenaces, tandis que l'assurance vise plutôt à minimiser les dommages financiers consécutifs à une cyberattaque.

Dans la gestion des risques

La sensibilisation devient un outil complémentaire dans la gestion des risques. Sensibiliser permet de faire prendre conscience de la nature d'un risque – l'hameçonnage, par exemple – et ainsi aider les collaborateurs à sa prise en compte.

La gestion des risques ne doit pas être exclue des programmes de sensibilisation et ne doit pas être réservée à un public type. Elle intervient à tous les niveaux de l'organisation et les campagnes doivent donc être adaptées en conséquence. Une campagne de sensibilisation peut s'appuyer sur la cartographie des risques afin de mieux cibler chaque population de collaborateurs et ainsi leur faire prendre conscience des risques associés à sa fonction.

La sensibilisation doit être incluse dans l'estimation des risques financiers et dans leur réduction. Un investissement – en temps et en argent – même limité peut potentiellement en réduire l'impact.

4 Démystifier la sensibilisation

La sensibilisation n’est pas une question de budget : cela demande du temps et de la matière grise pour la constitution des supports et des campagnes adaptées au contexte de l’organisation. De plus, elle ne doit pas cibler exclusivement les équipes IT, mais l’ensemble des métiers de l’organisation. La cybersécurité n'est pas un domaine qui concerne seulement les informaticiens.

Il convient de mettre en avant l’éveil des consciences des collaborateurs, mais pas que… La direction générale, le comité de direction, et l’ensemble des services de l’organisation doivent prendre la mesure des risques informatiques et surtout, des conséquences qu’ils auront sur l’organisation.

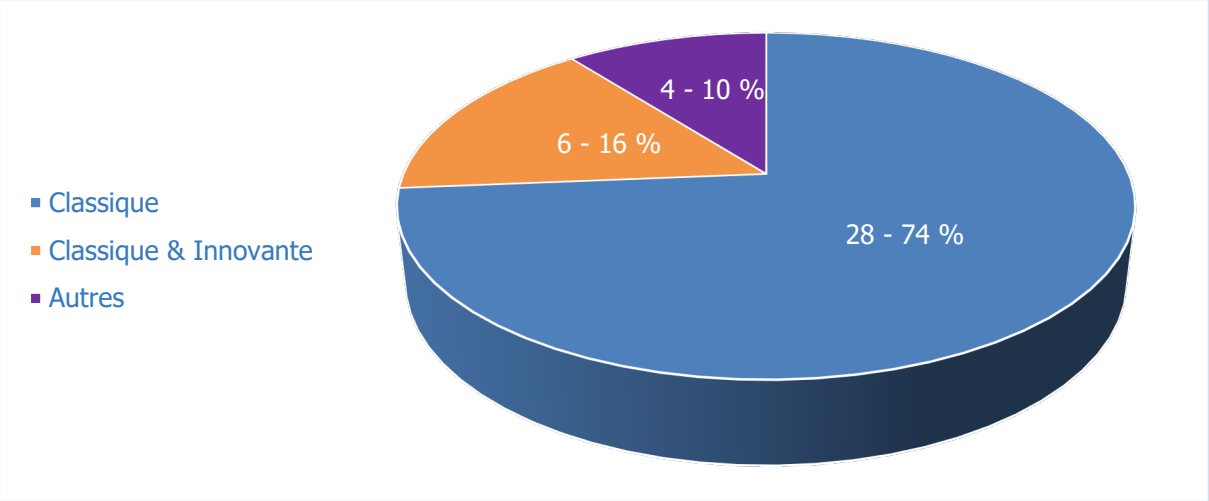
La sensibilisation doit-être prise en compte en continu car, comme l’organisation, les menaces évoluent. De ce fait, même si dans sa phase de construction, elle doit être traitée en mode projet, son maintien et son évolution devront faire l’objet d’amélioration continue.

La sensibilisation touche aux aspects professionnels, mais pas uniquement. Le collaborateur a aussi une vie numérique personnelle : messagerie, réseaux sociaux, terminaux. Les campagnes d’hameçonnage ne touchent pas que les organisations. Une mauvaise utilisation des outils personnels peut dériver vers une compromission de l’environnement professionnel si le même terminal est utilisé.

De quelques minutes à beaucoup d’euros, la sensibilisation s’inscrit dans une démarche globale pouvant aboutir à des formations qualifiantes.

5 Méthodes et outils ?

Quelles méthodes sont employées ?



L'approche par le risque permet, comme pour la construction de sa politique de sécurité, de déterminer les axes prioritaires dans les campagnes de sensibilisation et ainsi d'optimiser l'efficacité des investissements dans la sensibilisation des collaborateurs. En effet, une organisation dont le cœur de métier est la communication via des canaux numériques sera plus sensible aux risques d'hameçonnage et donc, devra orienter ses sessions sur cette thématique. À l'inverse, une organisation dont une partie des collaborateurs ne disposent que d'une messagerie interne sera sensiblement moins exposée.

Exemple : portable chiffré, mais mot de passe écrit sur un post-it collé sur le clavier : l'outil perd donc totalement son intérêt et son investissement pour un gain à zéro.

Du plus classique au plus innovant

Il existe de nombreuses méthodes pour la sensibilisation. Chacune peut correspondre à un public différent et un niveau de compétences plus ou moins élevé. Il convient donc de réfléchir au public visé pour déterminer l'approche la plus adaptée qui permettra de mieux porter les messages. La variation des outils et des messages permet de ne pas lasser l'auditoire et rend plus audibles les actions de sensibilisation. Cependant, la récurrence des messages est une des clés de l'acquisition des compétences et des réflexes de sécurité.

Il faut donc trouver un équilibre entre la nouveauté et la répétition en mixant aussi bien les techniques que les sujets afin de maintenir l'attention, et ce, pour une efficacité maximale. Il reste cependant des solutions très simples qui permettent de maintenir une régularité dans les messages fournis telles que les emails et autres supports d'affichage classiques.

Il existe des solutions pour tout type d'organisation. Quelle que soit la taille de la structure, la sensibilisation est possible ! En effet, de simples informations disponibles gratuitement et relayées régulièrement permettent de démarrer une sensibilisation. En fonction de la maturité en cybersécurité de la structure, il sera par la suite possible de créer des contenus spécifiques aux risques identifiés, voire de faire du e-learning totalement sur mesure. La question du coût et des moyens ne doit donc pas être une excuse à l'absence de sensibilisation. N'attendez pas d'avoir un budget, **vous pouvez sensibiliser les collaborateurs autour d'un café**.

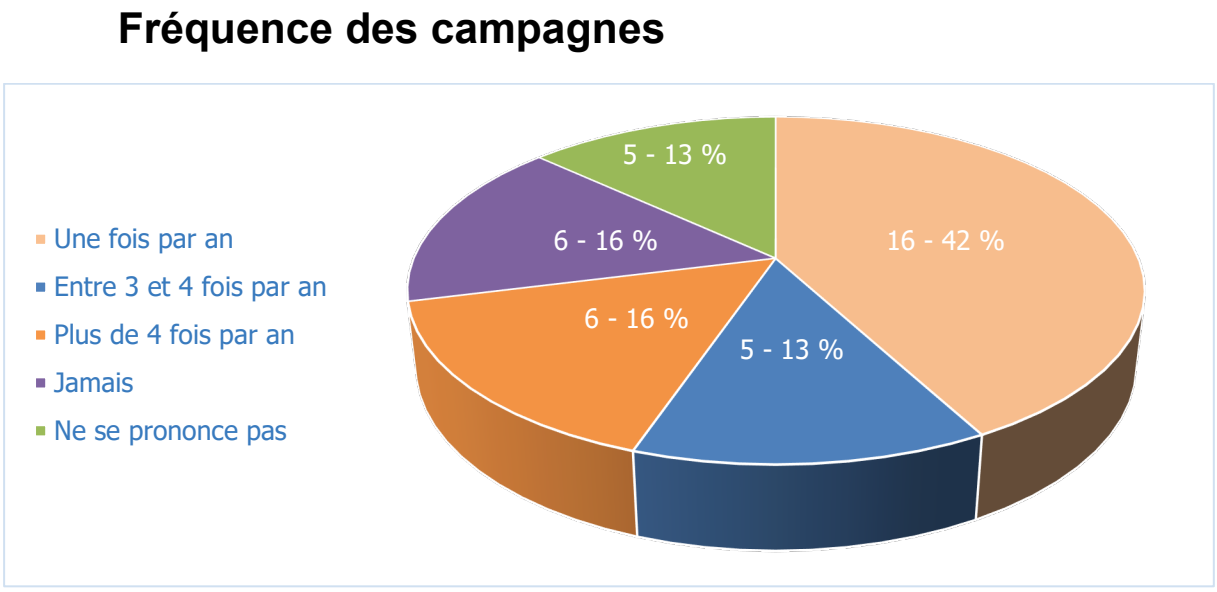
Type	Simplicité (temps)	Simplicité (compétences nécessaires)	Coût	Impact estimé
L'email ponctuel et/ou récurent	de Minutes (ponctuel) à Heures (récurrent)	Standard		- / +
Charte d'utilisation des moyens informatiques	Minutes	Standard	€	+
Les affiches papier dans les couloirs	Heures	de Standard à Moyen	€€	- / +
Le calendrier (goodies ou organismes) avec message sécurité ciblé (1/mois)	Minutes	Standard	€€€	- / +
Le e-learning, les quiz volontaires	Jours	Moyen	€€	+
E-learning et quiz imposés par les RH	Jours	Moyen	€€	++
Les campagnes de sensibilisation interactives	Semaines	Moyen	€€€	++
Outils de test et éducation aux bonnes pratiques (campagne de faux phishing) – Retour favorable des personnes qui ont été piégées	Semaines	Spécifique	€€€	+++
Les jeux sérieux (serious games), esprit d'équipe, challenge collectif. Demande une bonne maturité de l'organisation	Mois	Spécifique	€€€€	++
Les réunions, animations, webinaires (format PowerPoint) en présentiel	Heures	Standard	€	++
Les réunions, animations, webinaires (format PowerPoint) en distanciel	Heures	Standard	€	+
Formation traditionnelle (acquisition d'une compétence et moyen de mesure)	Jours	Standard	€€	+++
Les vidéos (sérieuses ou amusantes)	Jours	de Moyen à Spécifique	€€€€	++ / +++
Tous types de documents (brochures, guides rappelant les règles d'or et les pratiques) en postulant que le document est pris par les collaborateurs	Jours	Standard	€€	+

Type	Simplicité (temps)	Simplicité (compétences nécessaires)	Coût	Impact estimé
Les goodies (attention aux failles de sécurité) reprenant les messages de la campagne	Jours	Standard	€€€	++
Sensibilisation aux nouveaux personnels (accueil sécurité)	Jours	Standard	€	++
Réseau social interne et groupe de travail	Minutes	Standard	€	- / +
Simulation de crise (adaptée à l'encadrement)	Jours	de Moyen à Spécifique	€€€	+++
Témoignages et retours d'expérience (retex)	Jours	Standard	€€	++
Information sur les réseaux sociaux à destination des utilisateurs finaux	Minutes	Standard	€	- / +
Fond/économiseur d'écran, page de login personnalisée (rappel des règles)	Heures	Standard	€	++
Complément d'information dans la signature	Minutes	Standard	€	- / +
Journée sécurité avec stand d'information	Jours	Standard	€€€	++
Discussion informelle avec message sécurité	Minutes	Standard	€	+ / ++
Rappel de règles par les agents du support informatique	Minutes	Standard	€	- / +
Message sécurité sur les musiques d'attente du support informatique	Minutes	Standard	€	- / +
Démonstration en direct (possible via une vidéo pour plus de simplicité : esoin de moins de matériel) Simulation d'attaque en réalité virtuelle	Jours	de Standard à Moyen	€€	+++

Un des moyens d'impliquer les collaborateurs est d'intégrer la sécurité informatique dans leurs objectifs définis dans les entretiens individuels. Cela permet de maintenir une attention sur cet aspect sécurité et rend la sensibilisation « importante » aux yeux du collaborateur. Attention cependant à rendre l'objectif clair et accessible pour qu'il paraisse atteignable, et de s'assurer de l'investissement du collaborateur dans cet objectif.

La sensibilisation n'est pas une destination mais un chemin. Il convient de mettre en place un niveau de sensibilisation adapté à la maturité de l'organisation. Ce niveau de maturité évoluant, la stratégie de sensibilisation doit faire l'objet d'une amélioration continue. De plus, elle doit être en lien avec le domaine d'activité des collaborateurs : le « générique » est toujours moins percutant que le spécifique.

Les retex professionnels et personnels permettent de démontrer au collaborateur le bien-fondé de la démarche de sensibilisation.



La fréquence idéale de la sensibilisation et des campagnes d'informations n'existe pas : elle dépend de nombreux paramètres dont le contexte, les moyens disponibles, la maturité de la structure, sa prise en compte des risques, etc. Cependant, la régularité associée à un dosage adapté est un facteur clé de la transmission des messages. La sensibilisation doit donc être continue sans devenir répétitive, afin d'éviter « l'effet poubelle » où l'utilisateur jette directement le message sans même l'avoir consulté. La sensibilisation doit s'appuyer sur les risques à couvrir afin de maximiser son impact là où le risque est le plus important.

La variation des contenus entre chaque période de sensibilisation permet de rendre celle-ci attractive et ainsi d'éviter une lassitude de l'utilisateur. Cependant, la récursivité des thèmes est nécessaire pour optimiser l'apprentissage et améliorer, à terme, l'impact d'un message. La répétition est donc nécessaire à l'intégration des notions par les collaborateurs.

De la même façon, il est conseillé de varier les formes. En effet, un même contenu de sensibilisation ne doit pas être systématiquement présenté sous une forme identique, bien au contraire. Le public visé sera d'autant plus attentif si l'on parvient à maintenir un effet de surprise à chaque sensibilisation, ce qui maintient l'utilisateur « en mode apprentissage ».

Chaque contexte d'organisation est différent, mais les retex montrent qu'un minimum de sensibilisation une fois tous les deux mois sur l'ensemble de l'organisation est nécessaire pour entretenir une certaine habitude, voire une attente des collaborateurs. S'il n'y a pas de maximum dans l'absolu, il convient de ne pas sur solliciter les collaborateurs qui risquent de

ne plus souhaiter accorder d'attentions aux messages (effet poubelle). Dans ce contexte, la mesure de l'efficacité de la sensibilisation (cf. 7.4) et l'évaluation de la perception qu'en ont les collaborateurs peuvent fournir de précieuses indications pour optimiser la fréquence des campagnes.

Afin d'optimiser ces sensibilisations, il peut être pertinent de préparer à l'avance un plan de communication. Ce plan peut servir à préparer efficacement les sensibilisations et donc maintenir un haut niveau d'attention des collaborateurs en définissant à l'avance le niveau de mixage du fond et de la forme. En fonction des moyens et des risques à couvrir, il est possible de déterminer à l'avance : qui, quoi, comment, pourquoi et quand. Évidemment, il est souhaitable de laisser une marge de manœuvre pour adapter certaines communications à l'actualité, ou à l'apparition d'un risque critique à couvrir d'urgence.

Périmètre de la sensibilisation			
Qui	Quand	Comment	Pourquoi
Direction générale	Au plus vite	Présentiel	Démonstration du risque
Objectifs de la sensibilisation (Quoi)			
En faire un relais de communication au plus haut niveau des éléments stratégiques/ les plus importants que l'on souhaite relayer auprès des équipes			

Si la sensibilisation permanente des collaborateurs est pertinente, il ne faut pas oublier l'accueil des nouveaux collaborateurs. Il convient de définir un socle minimum d'information à délivrer à leur arrivée. Il est nécessaire d'adapter ce socle régulièrement avec les nouveaux risques ou les nouvelles règles de sécurité.

Public visé

- Utilisateurs vs administrateurs

Il est conseillé de créer pour les administrateurs ou personnes à privilèges un contenu complémentaire à la sensibilisation à destination des utilisateurs non techniques.

En effet, il ne semble jamais très pertinent de parler d'aspects trop techniques avec un collaborateur. Cette approche a tendance à développer un frein important à son intérêt, surtout s'il n'est pas spécialiste des technologies de l'information (IT). Cette distance peut devenir l'excuse pour qu'il ne s'implique pas dans la sensibilisation, voire rejette en bloc l'information et les messages. Il faut alors vulgariser les notions techniques pour le collaborateur autant que possible. À l'inverse, le collaborateur disposant de compétences spécifiques dans le domaine de la sécurité ne s'impliquera pas dans une sensibilisation générique.

Pourtant, le collaborateur disposant de privilèges doit tout autant être sensibilisé que l'utilisateur lambda. Des comportements déviants en matière de sécurité sont d'autant plus dangereux qu'une personne possède des droits élevés sur le système. Or, de façon régulière, une forme de faux sentiment de sécurité est constatée sur ce type de population *(« Moi, je ne me ferais pas avoir ! »*) ; la connaissance des risques entraînant une minimisation de celui-ci. Il est donc important de déterminer un canal de sensibilisation spécifique qui inclut l'administrateur dans la solution, en lui présentant par exemple les techniques utilisées par les pirates de façon très détaillée, éventuellement par un expert externe, voire en l'incluant dans la recherche de solutions de sécurisation pendant la sensibilisation *(« J'enfreins moins une règle que j'ai moi-même définie ! »*). La présentation de ce retex par d'autres administrateurs peut aussi avoir un impact très positif sur ce type de population.

Enfin, tous les administrateurs ne sont pas obligatoirement à la direction informatique. Certains collaborateurs disposent parfois de pouvoirs étendus sur les systèmes. Des campagnes de sensibilisation spécifiques doivent alors être envisagées. Par exemple, le responsable CRM (Customer Relationship Management) qui peut exporter la totalité de la base client, les responsables RH qui disposent des droits étendus sur l'annuaire, etc.

- Comité de direction

Les membres du top management (présidence, direction générale, comité de direction, comité exécutif, etc.) ne doivent pas être écartés des démarches de sensibilisation, bien au contraire. Il appartient cependant au RSSI d'adapter le discours et les priorités.

Même si ces personnes sont souvent conscientes des risques, certains dirigeants peuvent encore aujourd'hui sous-estimer leurs conséquences. Elles peuvent faire preuve d'une méconnaissance de l'adéquation entre le niveau réel de la menace, les moyens mis en œuvre et la charge de travail nécessaire pour atteindre le niveau de sécurité désiré.

Le canal de sensibilisation qui semble le plus adapté est l'orientation financière et les enjeux de réputation. Sur les « enjeux financiers », certains éléments comme le montant des amendes ou les coûts associés au temps d'indisponibilité du système d'information sont des éléments facilement communicables, tout comme les frais de préparation à une gestion saine de communication de crise. Au regard de ces enjeux, la mise en perspectives des coûts pour limiter ces risques devient un puissant levier d'actions, autant dans la gestion quotidienne d'une entreprise que dans les opérations de fusion-acquisition.

Le temps accordé par ce type de population étant souvent réduit, il est important de synthétiser les informations principales utiles à une prise de décision, notamment en utilisant des formats courts et des raccourcis si nécessaires.

Pour les dirigeants, le cyberrisque est devenu un des risques majeurs pour l'entreprise. Effectivement, ces dernières années, il a été de plus en plus pris en compte par les instances dirigeantes. Celui-ci demeure néanmoins un risque parmi d'autres pour lequel des instances dirigeantes doivent parfois arbitrer en fonction des informations, risques et opportunités qui lui sont transmis.

Parallèlement, une tendance de fond sur la communication et la responsabilité des dirigeants apparaît. D'une part sur la communication, les rapports annuels de sociétés cotées présentent la manière dont les entreprises adressent les enjeux de cybersécurité. D'autre part, il apparaît également certaines mises en responsabilité de dirigeants[9] après des attaques subies par les entreprises. En effet, les décisions prises d'investir ou de ne pas investir en cybersécurité peuvent parfois être regardées par les actionnaires post-incidents et engager la responsabilité des dirigeants, notamment pour négligence.

Il est important que les dirigeants soient les premiers à respecter les règles établies dans l'organisation, afin d'instaurer la culture d'entreprise nécessaire à leur application par le reste des collaborateurs. Les dirigeants et les managers doivent être les sponsors des actions de sensibilisation menées par le RSSI.

[9] « Target : le PDG débarqué à la suite de la cyberattaque de décembre »
https://www.lesechos.fr/2014/05/target-le-pdg-debarque-a-la-suite-de-la-cyberattaque-de-decembre-302478

- Cible privilégiée des attaquants (présence sur les réseaux sociaux, accès à des données confidentielles, etc.)

Certains collaborateurs sont plus exposés aux cyberattaques. En effet, les attaquants choisissent certaines cibles en fonction de leurs accès à privilège ou leur niveau d'exposition.

Ainsi, les employés des services de support sont souvent en première ligne et reçoivent des communications de l'extérieur, tout comme les responsables RH sont bien souvent habitués à recevoir des CV en pièce jointe d'emails transmis depuis l'extérieur.

Il faut donc adapter le contexte et les éléments de sensibilisation de ces populations particulièrement ciblées afin de les préparer aux tentatives d'attaques qu'elles pourraient subir.

Les collaborateurs les plus exposés devront être formés à la détection des attaques typiques que leur position risque d'attirer. Les collaborateurs avec des comptes à privilèges quant à eux devront être sensibilisés plus fortement aux conséquences d'une compromission et l'ingéniosité dont feront preuve les attaquants qui cherchent à accéder à leurs comptes.

- Manager intermédiaire

Ils peuvent être un relais des communications qui permet de varier l'origine des messages. La direction doit s'assurer qu'ils sont compétents sur le domaine pour être eux-mêmes en mesure d'agir rapidement en cas d'incident de sécurité.

- Chef de projet

Les chefs de projet disposent en général de privilèges et potentiellement de connaissances technologiques plus avancées. Il est donc possible d'aborder des aspects plus techniques lors de la sensibilisation spécifique à cette population. Par exemple, certains sujets tels que :

- les revues de sécurité dans les projets,
- les bonnes pratiques de développements,
- le chiffrement des données personnelles,
- le cloud computing,
- les dangers du shadow IT,
- l'importance de la traçabilité,
- la gestion des erreurs.

Il semble important d'aborder à minima les aspects « Security by Design » et de « Security by Default » dans la sensibilisation de ce type de population, la prise en compte de ces éléments le plus tôt possible dans le projet permettant d'optimiser la sécurité globale du système d'information.

- Contrat temporaire (intérimaire, stagiaire, etc.)

Il ne faut pas les oublier et prévoir une sensibilisation à l'accueil portée au moins par un manager de proximité : par exemple, proposer un flyer synthétique des règles de base de sécurité s'appuyant sur les thématiques de la charte informatique.

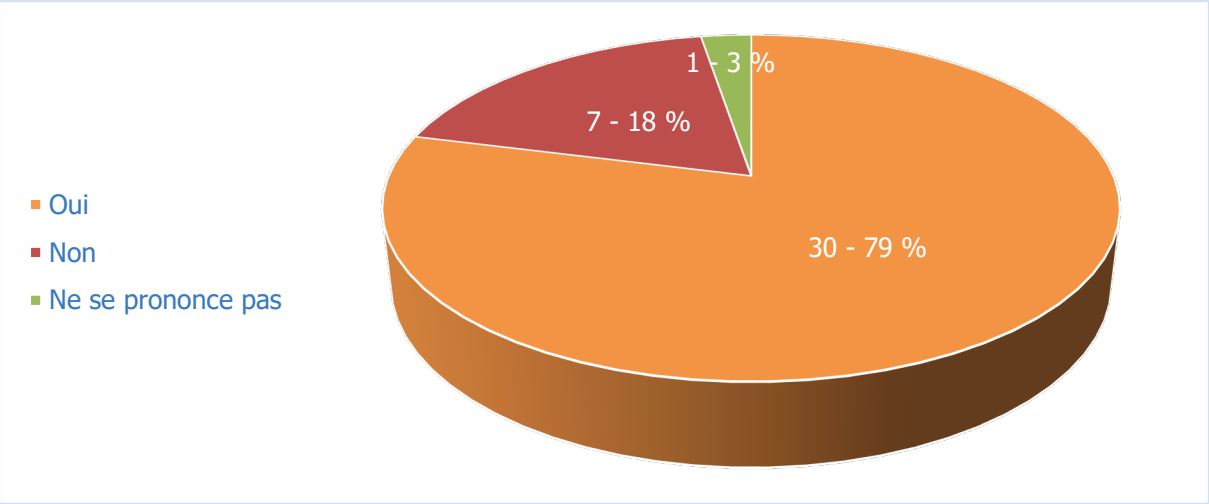
Les personnes en charge des entrées/sorties du personnel peuvent être un bon relais pour la sensibilisation au départ (risques et règles) ou la sortie (confidentialité et retour des équipements, suppression des droits, etc.).

Adaptation des messages

Dans les questions, nous avons souhaité savoir si lors des campagnes nos membres réalisent une veille pour faire évoluer leurs messages de sensibilisation. La question peut sembler

évidente mais, réaliser une veille sur les menaces ou adapter les messages en fonction des risques identifiés au sein de l'organisation demande une charge de travail complémentaire qui doit être identifiée.

Majoritairement, les campagnes font l'objet d'une veille et d'une adaptation en fonction du contexte de l'organisation de la part de la personne ou du service en charge de la sensibilisation.



Pour adapter au mieux sa sensibilisation, si elle existe, il est pertinent de s'appuyer sur la cartographie des risques afin de construire ses campagnes et ainsi les optimiser en axant les messages sur les risques critiques de l'organisation.

L'actualité est une source d'information et peut alors inspirer la création d'une campagne spécifique sur une menace touchant le secteur d'activité de l'organisation (par exemple, rançongiciels ayant touché les hôpitaux en 2020/2021). Tout comme les campagnes ponctuelles soutenues au niveau de l'État ; en octobre, le Cybermoi/s proposé par l'Agence de l'Union européenne pour la cybersécurité (Enisa) et mis en avant par l'ANSSI en France, peuvent être relayées en interne auprès des collaborateurs pour appuyer les messages de sensibilisation déjà diffusés.

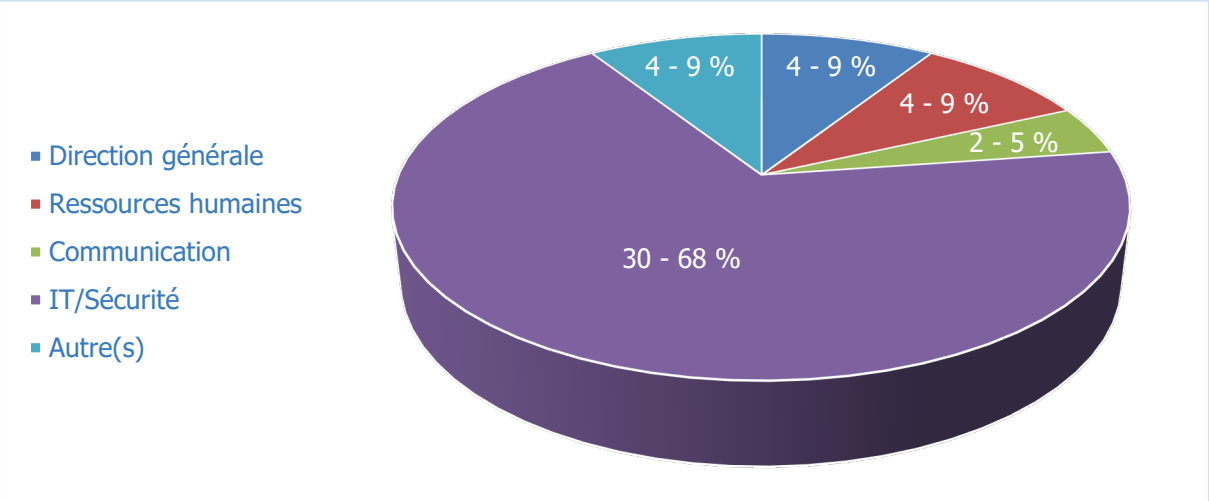
La sensibilisation peut s'appuyer sur une expérience malheureuse vécue par l'organisation pour sensibiliser les collaborateurs et ainsi appuyer le ou les messages en les associant à des faits avérés ayant eu des conséquences pour l'organisation et ses collaborateurs.

Si la sensibilisation est uniquement à la charge d'un service de communication, il est important de prêter une attention particulière à ce que les messages de sensibilisation « sécurité » ne soient pas noyés dans la communication générale de l'organisation. Cependant, impliquer le service communication ou les ressources humaines favorisera la prise en compte de la sensibilisation numérique dans la politique générale de l'entreprise au lieu de la limiter à un simple outil de la direction informatique.

6 Budget

Lors de l'élaboration du questionnaire, une question est revenue fréquemment et pour laquelle, la réponse n'est pas évidente : qui est porteur du budget ? En effet, en fonction du type, de la taille de l'organisation et de sa structure (existence d'un pôle formation ou communication), le financeur n'appartient pas forcément au même service.

Néanmoins, pour la grande majorité des répondants, le budget sensibilisation est associé à l'IT ou à la SSI. Cette tendance peut alors s'expliquer par certains aspects techniques (hameçonnage) associés à la sécurité.



L'absence de budget n'est pas un frein !

Il existe de nombreuses ressources permettant de commencer à mettre en place une sensibilisation tout en ayant un budget limité, voire inexistant. Au niveau européen, l'Enisa propose des supports de toutes natures ; au niveau national, l'ANSSI et Cybermalveillance.gouv.fr mettent à disposition pour l'un, des livrables permettant entre autres de définir la gouvernance et le pilotage de la sécurité, ainsi que le durcissement des systèmes d'information dans l'organisation ; et pour l'autre, des supports sous forme de fiches et de vidéos pour comprendre les risques et adopter les bonnes pratiques en matière de cyber.

Ces médias peuvent être réutilisés et librement diffusés au sein des organisations :

- Enisa : Supports
- ANSSI : Supports
- Cybermalveillance.gouv.fr : Supports

Ils peuvent constituer une première étape dans la construction du plan de sensibilisation des collaborateurs. Les ressources peuvent servir à la mise en place d'affiches, de communications par email ou en vidéo. En revanche, ces supports sont génériques et sans identité visuelle de l'organisation, ce qui peut nuire à l'appropriation par les collaborateurs.

La constitution d'un support, présentant les techniques classiques des cybercriminels ainsi que les moyens de s'en protéger peut-être réalisée à moindres frais. Cela demande de pouvoir réunir les collaborateurs en présentiel, à distance ou de diffuser le support, mais dans ce dernier cas, attention à valider la bonne compréhension et l'assimilation des messages.

Pour aller plus loin, il existe aussi des outils « clé en main » qui permettent de construire et de

mener des campagnes d'hameçonnage. Toutefois, ces derniers demandent quelques compétences techniques et forcément un temps de préparation pour l'identification des populations cibles, la construction du ou des scénarios, et l'analyse des résultats. Il convient aussi de prendre garde à l'utilisation de logo et marque avec laquelle vous n'avez aucun droit et accord. La sensibilisation ne doit pas devenir un risque juridique pour l'organisation.

Ces premiers éléments permettront de démarrer des campagnes avec un investissement humain et financier limité et ainsi poser les jalons des campagnes.

De quelques minutes à beaucoup d'euros

L'évolution des campagnes demandera un investissement humain et/ou financier complémentaire afin de maintenir les participants en éveil constant sur les risques. Il serait contreproductif pour l'organisation de répéter les mêmes campagnes ou de les réaliser sur les mêmes périodes ; cela risque en effet de créer un faux sentiment de sécurité et d'engendrer des comportements qui pourraient exposer le système d'information.

Pour les collaborateurs les plus exposés aux risques, il peut être pertinent de passer par une phase de formation axée sur leurs besoins spécifiques. Par exemple, pour les développeurs : une fois sensibilisés au risque – notamment ceux liés au code (XSS, injection SQL, etc.) – une formation complémentaire sur les méthodes de développement sécurisé leur permettra de faire évoluer leurs méthodes de travail et limitera la surface d'attaque de l'organisation.

Dans la stratégie de sensibilisation, il y aura plusieurs itérations. Dans les premières étapes, il n'y a pas forcément besoin d'un budget conséquent, les ressources à disposition, la volonté de transmettre auprès des collaborateurs et l'adhésion de ces derniers permettent de mettre en œuvre les premiers jalons à faible coût. Il faut monter les escaliers marche par marche, commencer par des emails d'information, puis progresser.

7 Objectifs

Ambition

L'organisation fait face à des enjeux majeurs : perte d'activité, désorganisation, confiance, sanctions juridiques et financières, sécurité/santé (risques psychosociaux) des collaborateurs et des clients.

Sensibiliser permet de réduire l'exposition aux comportements à risque et les impacts de ces derniers. Par exemple, il faut en moyenne 197 jours[10] pour détecter une violation de données. Sensibiliser les collaborateurs permet de les impliquer dans la détection des signaux précurseurs et donc de réduire les temps de réaction et d'en limiter les impacts.

Par exemple, le RGPD impose une obligation de déclaration auprès de l'autorité de contrôle dans les 72 heures après constatation d'une violation des données personnelles. Pour déclarer une violation, celle-ci doit être préalablement connue de l'organisation. La remontée par les collaborateurs permet d'obtenir ces signaux faibles bien en amont. La sensibilisation est un moyen d'initier et de faire progresser chaque personne dans sa compréhension de la sécurité informatique. Elle doit être retranscrite notamment dans la charte informatique et les contrats de sous-traitances.

La lutte contre les cyberattaques doit être collective au sein d'une organisation. Chaque individu doit prendre conscience qu'il est acteur de la cybersécurité et doit adopter les bonnes règles en termes de comportement. Cela inclut l'identification, puis le signalement à l'organisation des signes d'un comportement anormal et l'assurance qu'il peut remonter ces anomalies en toute quiétude. D'autre part, la sensibilisation peut être une obligation imposée par des clients donneurs d'ordre ou par la souscription d'un contrat de cyberassurance.

La sensibilisation doit-elle être obligatoire ? Si oui, obligation contraignante ou récompensée/valorisée ?

En dehors de certains référentiels comme l'ISO 27001, et pour lesquels la sensibilisation découle à la fois de la partie normative, une obligation de sensibilisation n'est pas nécessairement explicitée. Néanmoins, elle est vivement recommandée.

Au-delà de l'obligation réglementaire, la mise en place d'une sensibilisation permet à l'organisation de démontrer auprès des collaborateurs sa volonté d'inclure la cybersécurité comme une priorité. Le but à atteindre devrait être plutôt une démarche d'adhésion et d'engagement des collaborateurs qui découle de celle de la direction de l'entreprise : le « cyber-engagement ».

Comment ?

1- Récompenser **directement** par valorisation :

Charte « éthique » (inclut la RSE et la qualité de vie au travail) : valoriser le collaborateur dans un engagement sociétal (conformité – extension dans la vie privée = valorisation).

- Concours/challenge : collectif (service, équipe) est à privilégier / individuel.

[10] LeBigData, « Une entreprise met 6 mois pour détecter une fuite de données ».
https://www.lebigdata.fr/entreprise-6-mois-pour-detecter-une-fuite-de-donnees

- Retour explicatif équipe SI.
- Fiche retex interne, notamment faite par la mise en avant directe du collaborateur (témoignage : vidéo, mail, réseau social, etc.).

2- Récompenser **indirectement** par le maintien d'une accessibilité aux utilisateurs : ergonomie/sécurité. Rupture numérique supplémentaire…

Plus il y a de l'engagement individuel/collectif dans la cybersécurité, moins les contraintes techniques sont pesantes, plus l'ergonomie/agilité/souplesse est préservée : C'est un cercle vertueux favorisant l'adhésion.

Exemple de valorisation du collaborateur :

- les goodies,
- le cyber-champion,
- visibilité pour les collaborateurs sur leur niveau atteint.

Faire passer la sensibilisation d'un état de contrainte pour le collaborateur à un gain de compétence, tant dans sa vie professionnelle que personnelle (par exemple, la création de sauvegarde de ses photos).

L'aspect obligatoire et contraignant de la sensibilisation ne réglera que la question du respect du principe de responsabilité (« accountability ») et donc d'une éventuelle responsabilité interne de défaillance de formation, mais pas véritablement celle de la protection améliorée contre les attaques.

L'objectif n'est en aucun cas de créer des experts, mais d'engager les collaborateurs, avec un **socle minimal de connaissances** et une acquisition de comportements, dans une dynamique participative.

L'ambition peut et doit se situer, certes sur un savoir, mais aussi sur un savoir-faire et un savoir-être.

- **savoir** : posséder un socle minimal de connaissances et adapté à chaque poste et chaque responsabilité, et à l'exposition individuelle et collective aux risques ;
- **savoir-faire :** savoir détecter et savoir alerter ;
- **savoir-être :** éveiller et maintenir une vigilance constante.

En définitive, on développe une capacité comportementale de savoir réagir au bon moment en impliquant, en sollicitant les bonnes personnes. L'un des objectifs est d'éviter le silence afin de s'inscrire dans une démarche positive.

Que souhaite-t-on que le collaborateur retienne ?

Les collaborateurs doivent retenir d'une sensibilisation :

- que c'est important ;
- que la **méfiance/vigilance** est la clé ;
- quelques **réflexes** de base ;
- qu'ils sont un composant clé dans notre dispositif de sécurité : nous sommes **TOUS** concernés.

7.1.1 C’est important

Les campagnes de sensibilisation ne sont pas là pour empêcher les collaborateurs de se concentrer sur leurs tâches. Il est important que l’organisation prenne en compte les conséquences importantes, voire **vitales**, qui peuvent découler d’un geste en apparence anodin.

On retrouve principalement :

- la perte temporaire ou totale d’accès aux données, potentiellement sur tous les équipements,
- le positionnement face à la concurrence remis en question,
- la réputation de l’entreprise touchée,
- la perte d’argent avec des cas réguliers de redressement judiciaire ou de faillite,
- des conséquences désastreuses quand un établissement de santé est touché.

Il est très important que les utilisateurs se sentent en confiance et valorisés quand ils remontent des anomalies. La sensibilisation à l’accueil des remontées d’incidents par les équipes support ne doit pas être négligée.

7.1.2 Il faut se méfier

Le piratage s’est professionnalisé avec un modèle économique très lucratif (et non imposable), calqué sur le crime organisé (voir Panocrim 2020/2021).

Cela signifie que les pirates disposent de temps, de moyens, et cherchent en permanence comment s’améliorer et augmenter les bénéfices. Il ne s’agit plus seulement d’un acteur isolé dans son garage, mais aussi de véritables organisations criminelles très structurées.

Les méthodes évoluent très vite et s’adaptent. Toutes les organisations sont concernées. C’est encore plus vrai quand la menace est ignorée ou minimisée.

Il n’y a plus de cibles privilégiées, toutes les organisations peuvent être victime d’une cyberattaque :

- demande de rançon directe par opportunisme : un gain financier potentiellement conséquent pour quelques minutes ou heures d’effort ;
- accès indirect à des entreprises plus importantes (attaque du sous-traitant).

Les collaborateurs doivent être acteurs et non plus spectateurs dans la cybersécurité de l’organisation.

7.1.3 Les réflexes de base

Les réflexes de base ne s’acquièrent qu’à travers des phases telles que l’enseignement et l’entraînement.

Une fois ces réflexes acquis, il est important qu’il y ait une récurrence dans les messages et de la diversité des supports de transmission. Il faut entretenir les connaissances (Ebbinghaus, lutter contre la courbe de l’oubli) par la répétition des messages.

7.1.4 Les messages de conclusion

Afin d’entretenir les actes réflexes, il est nécessaire de rappeler aux collaborateurs lors de ces sensibilisations les messages clés de l’entreprise tels que :

- Comment rendre compte ?
- À qui ?
- Où trouver la base de connaissance de l'entreprise ?

Une proposition pourrait être de :

- disposer d'interlocuteurs via un email générique et connu de tous,
- mettre à disposition d'une base de connaissance,
- un numéro de téléphone unique,
- des référents bien identifiés,
- une voie hiérarchique, un management.

7.1.5 Rappel

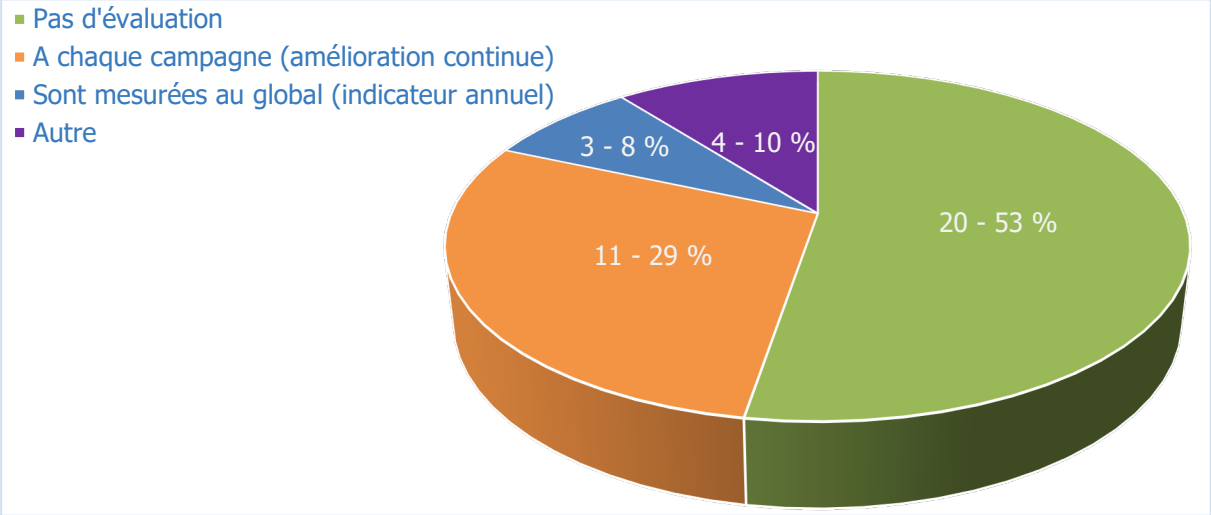
Lors des sessions de sensibilisation, il faut garder en tête que la quantité des informations retenues reste faible et varie selon les vecteurs de transmission. Il faut cibler le média à utiliser en fonction des messages que l'on souhaite transmettre.

Modalités de mise en œuvre

Définir un plan de sensibilisation qui ne soit pas trop ambitieux, qui correspond à la disponibilité des collaborateurs et des moyens mis à disposition par l'entreprise. Ce plan doit inclure :

- la fréquence,
- la durée,
- la population cible (adaptation de la sensibilisation à la fonction),
- les thèmes et objectifs de la sensibilisation.

Mesure d'efficacité/suivi



L'efficacité d'une campagne est mesurée en fonction des objectifs, définir les indicateurs qui permettront de mesurer les résultats obtenus afin d'apprécier l'efficacité des moyens mis en œuvre pour atteindre ces objectifs.

Attention à la mesure d'efficacité sur l'acquisition de savoirs théoriques. Beaucoup d'attaques reposent sur l'ingénierie sociale qui manipule les émotions et les schémas de réponse des collaborateurs. Ces derniers risquent de ne pas pouvoir mobiliser les connaissances acquises en parcourant des contenus théoriques. Il faut donc prendre les résultats de quiz et d'évaluations de connaissances avec prudence.

Attention également à l'excès de confiance[11-12] que peuvent engendrer des résultats flatteurs lors d'une évaluation ponctuelle. Les résultats peuvent drastiquement varier d'un test à l'autre en fonction de nombreux paramètres (effectif testé, scénario employé, heure de la campagne, etc.). Il est donc nécessaire de ne pas se satisfaire d'un seul bon résultat.

Ces scores évoluent d'ailleurs dans le temps en raison de l'évolution des menaces elles-mêmes et de la courbe de l'oubli. C'est pourquoi on ne peut se satisfaire d'un test annuel pour évaluer le niveau de vigilance du collaborateur et de résilience de l'organisation.

Amélioration continue

- Ne pas rester sur ce qui fonctionne, considérer que les menaces évoluent et que les campagnes doivent s'adapter.
  - moduler les campagnes pour limiter la perte d'efficacité ;
  - prendre en compte les nouveaux risques/scénarios ;
  - adapter les campagnes en fonction du niveau évalué et/ou des résultats des campagnes précédentes (« adaptive learning ») ;
  - ne pas négliger les retours des collaborateurs, qu'ils concernent une campagne spécifique ou la stratégie globale de sensibilisation ;
  - valoriser les actions de sensibilisation.
- Du point de vue du collaborateur :
  - améliorer sa connaissance « cyber » qui pourra être valorisée durant son évolution au sein de l'organisation ;
  - adopter des actes réflexes qui pourront lui servir aussi bien dans sa vie professionnelle que personnelle ;
  - créer une reconnaissance interne pour les « cyber-champions ».
- Pour l'organisation en générale :
  - améliorer le niveau de sécurité et de résilience de l'organisation, ce qui est quasiment devenu un incontournable dans la souscription d'une garantie « cyber » ;
  - améliorer son score auprès des agences de notation cyber.

Pour les dirigeants, cela peut être vu comme une obligation de moyen, ainsi qu'une justification d'avoir à mener des actions pour l'organisation, les employés et eux-mêmes. Cela fait partie des moyens à mettre en œuvre pour se protéger et ainsi limiter les risques de poursuites potentielles dans le cadre de leurs fonctions.

---

[11] 76 % des salariés se considèrent formés en cybersécurité.
https://www.ey.com/en_us/news/2022/10/gen-z-and-millennials-less-serious-about-cybersecurity-on-work-issued-devices-than-personal-according-to-new-ey-consulting-survey

[12] 80 % des entreprises considèrent que leurs employés sont à même de déjouer les cyberattaques.

https://www.eset.com/fr/about/newsroom/press-releases/enquete/enquete-eset-cybersecurite

8 ANNEXE

Quelques exemples

- Gestion de ses mots de passe, car la divulgation de ceux-ci ouvre l'accès au système d'information de l'entreprise :
  - Utiliser des mots de passe qui ne peuvent pas se deviner facilement. Éviter donc les prénoms familiers, les dates de naissance, l'année en cours, les séries de chiffres ou de lettres telles que « 456 » ou « azerty », des astuces éculées comme « M0tDeP@sse123! », etc.
  - Savoir que les pirates volent les identifiants sur des sites peu protégés et les réutilisent ensuite sur d'autres. Il existe des bases de plusieurs milliards d'identifiants aujourd'hui disponibles[13].
- Se méfier de son port USB quand :
  - On y branche une clé, un disque dur externe ou une cigarette électronique qui ne vient pas d'une source fiable. En cas de besoin ou de doute, contacter le RSSI.
  - On copie des données confidentielles non chiffrées sur un support amovible. Ce type de support se perd, se vole, s'oublie…
- Verrouiller son PC :
  - même pour deux minutes ;
  - même chez soi.
- Usage des WiFi publics (gare, hôtel, restaurant, etc.) :
  - Ces réseaux ne sont pas sécurisés « By Design » (par conception). Cela signifie que pour celui qui sait écouter, les informations transitent en clair.
  - Si une information sensible doit être consultée ou transmise, il faut soit utiliser un VPN, soit attendre de disposer d'un réseau plus fiable (3G/4G/5G).
- Sécuriser les échanges et identifier un phishing/vishing :
  - Ne jamais donner ses codes et identifiants après être arrivé sur une page au travers d'un lien que l'on n'a pas explicitement demandé. Les entreprises, les banques, les assurances ou les organismes étatiques ne demandent jamais ce type d'informations. Alors si ce n'est pas eux, qui est-ce ?
  - Éviter de cliquer sur des liens dans des emails. Toujours préférer se rendre directement le site web.
  - Ne pas ouvrir une pièce jointe quand on ne l'attendait pas ou que l'on ne connaît pas l'expéditeur. En cas de doute, transmettre au RSSI.
- L'ingénierie sociale :
  - Technique assez vicieuse qui consiste à créer un climat de confiance pour obtenir de l'information. Il faut conserver sa méfiance vis-à-vis d'inconnus, surtout s'ils proposent un gain facile, vous flattent ou partagent vos convictions. Personne ne vous reprochera de respecter les procédures, notamment celles de vérification et de contre-appel.

[13] https://haveibeenpwned.com

- Ne pas oublier le papier :
  - j'imprime, je me lève et je vais chercher et je vérifie que je n'ai pas oublié une page ;
  - j'imprime le moins possible ;
  - j'appose des affiches autour des imprimantes, sans oublier celles visibles quand on a le dos tourné à l'imprimante.

Tour Eria
5, rue Bellini
92821 Puteaux cedex
France
✆ Tél. : +33 1 53 25 08 80
clusif@clusif.fr

clusif.fr