# GUIDE DE L'INGÉNIERIE SOCIALE

## Comment prendre les bonnes mesures

Digital Security
**Progress. Protected.**

# Table des matières

# Pourquoi les PME devraient se préoccuper de l'ingénierie sociale

**Les PME sont de plus en plus conscientes qu'elles sont des cibles pour les cybercriminels, selon une enquête de 2019 menée par Zogby Analytics pour le compte de l'Alliance nationale de cybersécurité des États-Unis. Près de la moitié (44 %) des entreprises comptant entre 251 et 500 salariés ont déclaré avoir subi une fuite de données au cours des 12 derniers mois. L'enquête a révélé que 88 % des petites entreprises estiment être au moins une cible « assez probable » pour les cybercriminels, dont près de la moitié (46 %) estiment être une cible « très probable ».**

Les dommages sont réels et étendus, comme l'illustre bien le Rapport annuel de l'Internet Crime Complaint Center (IC3) du FBI. En 2020, l'IC3 a reçu 19 369 plaintes pour usurpation de messagerie, avec des pertes ajustées se montant à plus de 1,8 milliard de dollars. Pour ceux qui ne le savent pas, l'usurpation de messagerie, également appelée BEC/EAC, est une escroquerie sophistiquée qui vise à la fois les entreprises et les particuliers effectuant des transferts de fonds.

33 % des intrusions étaient dues à des attaques d'ingénierie sociale, qui est la tactique la plus utilisée après le piratage, indique le rapport Data Breach Investigations de 2019.

## Une fois les PME victimes d'une faille de sécurité

| 37 % | 25 % | 10 % |
|---|---|---|
| subissent une perte financière | déposent le bilan | cessent leur activité |

Source : NCSA

# Introduction

**L'objectif de ce guide est de présenter l'ingénierie sociale et ses risques pour chaque collaborateur de l'entreprise. Les humains sont des êtres émotionnels, et l'ingénierie sociale est un moyen très efficace d'exploiter cette caractéristique. De plus, les attaques d'ingénierie sociale ne nécessitent généralement pas de compétences techniques poussées de la part de l'attaquant. Forcer des milliers d'utilisateurs à divulguer des informations confidentielles ou effectuer des actions nuisibles s'est avéré jusqu'à présent plutôt facile ! Ne vous laissez pas berner. Vous pourriez facilement vous aussi devenir une cible.**

Les pages suivantes comportent une vue d'ensemble des tendances de l'ingénierie sociale, ainsi que des exemples des types d'attaques les plus courants qui peuvent affecter la façon dont les collaborateurs agissent en ligne. Vous apprendrez également à reconnaître ces attaques pour vous en protéger, vous et votre entreprise.

Les solutions de sécurité devraient protéger contre les attaques techniques. Cependant, les techniques d'ingénierie sociale reposent davantage sur la psychologie. Elles profitent de la confiance, de la peur et de l'inattention des gens.

# Types de techniques d'ingénierie sociale

**Spear phishing**
Une forme d'hameçonnage ciblant un individu ou une entreprise spécifique. Les campagnes d'hameçonnage classiques ne ciblent pas les victimes individuellement, mais sont envoyées à des centaines de milliers de destinataires.

**Vishing**
Une méthode similaire à l'hameçonnage mais utilisant des appels téléphoniques frauduleux au lieu d'emails. Les cybercriminels se font souvent passer pour un représentant d'une banque ou d'une compagnie d'assurance.

**Smishing**
Une tentative d'attaque d'ingénierie sociale via SMS. Le plus souvent, elle a pour objectif de rediriger les destinataires vers un site web récoltant leurs données. Il peut également s'agir de campagnes invitant les victimes à envoyer des données sensibles par réponse directe au SMS.

**Sextorsion**
Il s'agit d'une escroquerie de chantage qui existe depuis longtemps, au moyen d'emails comportant des affirmations et des accusations sans fondement.


**Usurpation d'identité**
La technique d'usurpation d'identité est la même que dans le monde physique. Des cybercriminels contactent des employés, généralement en se faisant passer pour leur PDG, et tentent de manipuler les victimes pour les amener à agir, par exemple pour commander et approuver des transactions frauduleuses.

**Scareware**
Un logiciel qui utilise différentes techniques anxiogènes pour forcer les victimes à installer d'autres malwares sur leurs appareils. Par exemple, un faux produit antivirus incite les utilisateurs à installer un logiciel spécifique pour traiter une infection, mais le programme est généralement dangereux.

**Escroquerie au support technique**
Des attaquants tentent de vendre de faux services, de résoudre des problèmes inexistants ou d'installer une solution d'accès à distance dans les appareils des victimes, et d'obtenir un accès non autorisé à leurs données.

# Hameçonnage

**Vous avez probablement déjà, à un moment de votre vie, été confronté à une situation dans laquelle vous avez reçu un email semblant provenir d'une banque ou d'un service en ligne populaire vous demandant de confirmer vos identifiants ou votre numéro de carte bancaire. Il s'agit d'une technique d'hameçonnage courante. Ces pièges évoluent cependant constamment et sont parfois difficiles à reconnaître.**

L'hameçonnage est une forme d'attaque d'ingénierie sociale dans laquelle un criminel tente d'accéder à des identifiants de connexion, d'obtenir des informations confidentielles ou transmettre des malwares. Les campagnes d'hameçonnage peuvent cibler un grand nombre d'utilisateurs anonymes, une victime spécifique ou un petit groupe de victimes associées, à l'aide d'escroqueries personnalisées (spear phishing). Les attaques visant des personnes spécifiques, le plus souvent des cadres supérieurs ou des propriétaires d'entreprise, sont qualifiées de « chasse à la baleine » (les pirates ciblent les « gros poissons »).

Les escrocs savent qu'il y a de fortes chances que tout message soit analysé par le logiciel de sécurité de votre messagerie puis placé dans le dossier des emails indésirables. C'est pourquoi le contenu des messages frauduleux change si souvent.

Selon Google, les escrocs ont envoyé 18 millions d'emails d'hameçonnage en période de COVID-19 chaque jour de mars 2020 aux utilisateurs de Gmail.

# Hameçonnage

Depuis le début de la pandémie de COVID-19, les fraudeurs n'ont pas perdu de temps pour tenter de tirer profit de l'incertitude, de la peur et des pénuries d'approvisionnement liées à la crise. En mars 2020, nous avons constaté un déluge d'emails de spam sur le thème de COVID-19, diffusant des malwares, essayant d'obtenir des informations sensibles ou proposant des produits factices, comme le révèle le Rapport ESET sur les menaces du 1er trimestre 2020.

Il n'est pas surprenant que la pandémie soit devenue l'un des principaux appâts utilisés par les attaquants. L'apparition de toute crise entraîne de nouvelles circonstances qui offrent aux cybercriminels un environnement idéal pour innover.

94 % des malwares sont diffusés par email.

17 700 dollars sont perdus chaque minute en raison des attaques d'hameçonnage.

Environ 14,5 milliards d'emails de spam sont envoyés chaque jour.

Sources : CSO, hostingtribunal.com

# Attributs de base de l'hameçonnage

Digital Security
Progress. Protected.

1 Si vous ne reconnaissez pas l'adresse email, faites preuve de prudence.

2 Attendez-vous au pire avec les fichiers joints ou les liens inconnus. Ils peuvent contenir un malware ou vous envoyer vers une destination web malveillante.

3 Trop effrayant ou trop beau pour être vrai ? C'est probablement une arnaque. N'oubliez pas que l'ingénierie sociale tente d'exploiter les faiblesses humaines.


4 L'objet diffère du message

5 Lorsque la salutation est trop générale, ce peut-être le signe qu'elle ne s'adresse pas seulement à vous, mais également à un certain nombre d'autres personnes.

6 Une urgence suspecte ? L'escroc veut que vous paniquiez.

7 Les fautes d'orthographe et de grammaire sont fréquentes dans les emails d'hameçonnage qui ont été traduits depuis une autre langue.

8 Les attaques homoglyphes consistent à remplacer les caractères d'une adresse par des caractères similaires appartenant à des alphabets différents (par exemple, « ạ » plutôt que « a » dans paypal.com).

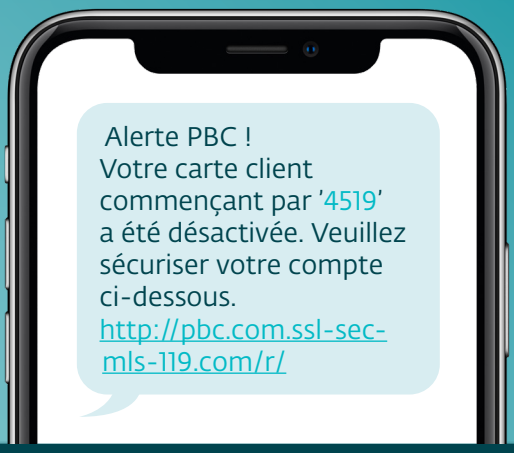
# Smishing


Le **smishing** est un type de cyberattaque qui utilise le service de messagerie texte, ou SMS. Cette méthode s'est également répandue au cours des premiers mois de la pandémie de COVID-19. En période trouble, les gens ont par exemple reçu des SMS prétendant être des messages officiels de leurs autorités locales.

L'objectif de ces attaques est similaire à celui de l'hameçonnage (de l'anglais « phishing ») : les cybercriminels peuvent **tenter de vous soutirer des informations personnelles ou vous forcer à cliquer sur un lien menant à site web malveillant**. Une autre technique s'appuie sur notre compassion. Les cybercriminels envoient des SMS avec une demande de don pour les personnes en situation désespérée, comme un fonds pour les victimes d'ouragans ou un autre type d'organisation caritative, en demandant généralement les informations de votre carte bancaire.

Beaucoup de gens ont été surpris que des pirates puissent obtenir leur numéro de téléphone à leur insu. Mais comme l'ont souligné de nombreux experts en cybersécurité, **il est plus facile d'obtenir le numéro de téléphone d'une personne que son adresse email, car les numéros de téléphone existent en quantité limitée et leur structure est connue**. Il est plus difficile de deviner des adresses emails car elles autorisent davantage de caractères.

## Pouvez-vous dire ce qui est suspect dans ce SMS ?




Une banque ne vous enverrait probablement jamais un lien direct comme celui-ci. Si vous n'êtes pas sûr, vous pouvez vous rendre sur votre banque en ligne et vérifier si vous avez reçu le même message. Il est toujours plus sûr de se rendre sur un site officiel plutôt que de cliquer sur un lien suspect.

# Vishing

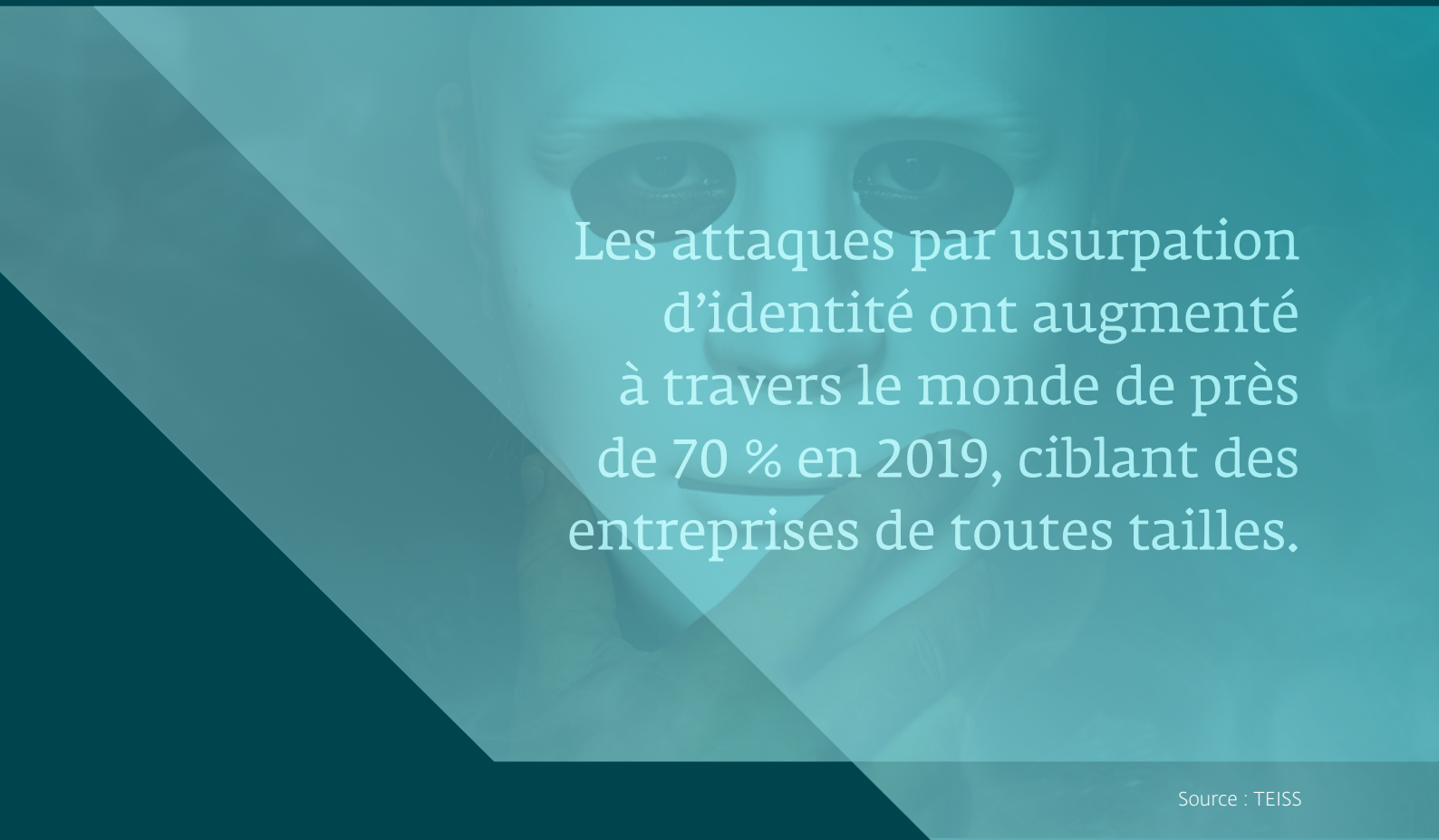
Le **vishing** exige d'être encore meilleur acteur que pour les autres types d'escroquerie, et se déroule généralement comme ceci : un escroc vous appelle au téléphone et **se fait passer pour un représentant d'une institution officielle**. Il vous informe que votre compte bancaire est compromis, ou d'une offre de prêt non sollicitée, dans le but d'obtenir vos informations personnelles et vos données financières. Trop beau ou trop effrayant pour être vrai ? Demandez-lui plus de détails, et **ne communiquez pas immédiatement de données sensibles**. Vous pouvez également mettre fin à l'appel et contacter vous-même le service clientèle de votre banque en expliquant la situation.

# Usurpation d'identité : quand un cybercriminel se fait passer pour un PDG

**Examinons l'usurpation d'identité, une autre méthode d'attaque non technique utilisée par les cybercriminels pour se faire passer pour des personnes dignes de confiance tout en essayant de manipuler les gens. Comment reconnaître que vous êtes contacté par un cybercriminel plutôt que par un collègue ?**

L'usurpation d'identité est définie comme étant une pratique consistant à se faire passer pour quelqu'un d'autre, dans ce cas, **afin d'obtenir des informations ou l'accès à une personne, une entreprise ou un système informatique**. Pour atteindre ces objectifs, les cybercriminels ont recours, entre autres, à des appels téléphoniques, des emails ou des applications de messagerie. Dans de nombreux cas, ils choisissent des noms parmi les cadres supérieurs de l'entreprise et créent un email qui semble avoir été rédigé par ces derniers.

La quantité d'informations disponibles sur les entreprises, sur des plateformes comme LinkedIn qui révèlent la structure de l'entreprise et les noms de ses employés, est assez incroyable. Un pirate peut utiliser ces données pour tenter de contacter plusieurs employés de l'entreprise, **et leur demander d'effectuer des transferts d'argent, de payer des factures ou d'envoyer des données importantes**. C'est pourquoi l'usurpation d'identité est si dangereuse pour les entreprises, car elles peuvent entraîner des fuites de données et des pertes financières.

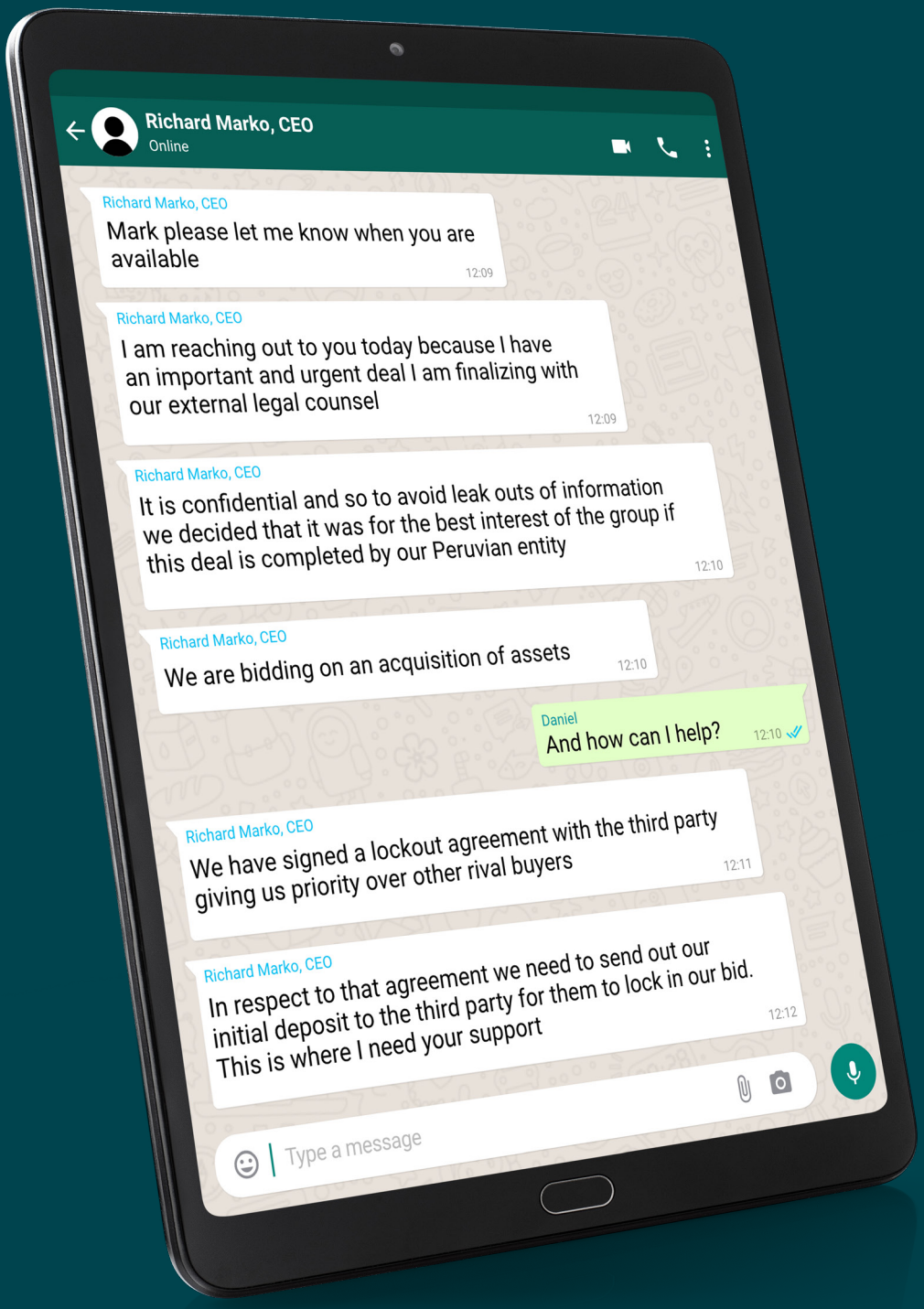


Les attaques par usurpation d'identité ont augmenté à travers le monde de près de 70 % en 2019, ciblant des entreprises de toutes tailles.

Source : TEISS

# Histoire vraie : attaque par usurpation d'identité contre ESET

Toute entreprise peut être victime de cyberattaques. En 2020, ESET a été confronté à des tentatives d'usurpation de l'identité de son PDG via des messages WhatsApp. Le but de cette tentative était de simuler l'existence d'une offre commerciale importante nécessitant un dépôt d'argent.



# Comment détecter les attaques par usurpation d'identité

**N'oubliez pas que la sensibilisation est essentielle. Plus nous en savons sur les attaques par usurpation d'identité, mieux nous pouvons les éviter. Voyons comment fonctionnent les emails d'usurpation. Beaucoup essaient d'instiller un sentiment d'urgence et de peur chez leurs cibles. Ce sentiment incite les victimes à accomplir la tâche souhaitée. Il peut s'agir de quelque chose que vous trouverez inhabituel et suspect, comme des achats qui ne sont pas liés à votre activité, avec des clients que vous ne reconnaissez pas. Les cybercriminels essaient également d'imposer un délai court pour les tâches requises.**

Les messages frauduleux contiennent souvent des erreurs grammaticales ou une utilisation incorrecte de la marque de l'entreprise. Ce ne sont cependant que les plus faciles à repérer. Les pirates adeptes de l'usurpation d'identité avancée peuvent concevoir un message qui semble très réel, avec une photo ou la signature officielle d'un employé à la fin du message. Ainsi, même si la forme semble légitime, faites preuve de prudence si vous trouvez que la demande est étrange.

## PENSEZ AU CONTEXTE

Parfois, nous sommes trop occupés et nous prenons des décisions sans trop réfléchir. Cela peut prendre quelques secondes de plus, mais vous devez toujours vous demander si l'email a un sens. Pourquoi ce collègue ne me demande-t-il d'effectuer que cet achat, ou de lui fournir des informations personnelles sensibles ? **Tout élément inhabituel qui s'écarte des processus traditionnels devrait être un avertissement**. Même si l'email provient apparemment d'une personne digne de confiance, comme le PDG, il peut s'agir d'un faux. Restez vigilant et vérifiez toute demande auprès d'autres collègues.

## PAS AU BUREAU ?

Les cybercriminels peuvent parfois savoir que quelqu'un est absent du bureau et faire semblant de le remplacer. Dans ce cas, vérifiez les informations en question auprès de leur supérieur ou de leurs collègues. Comme le dit le proverbe, il faut « regarder avant de sauter. »

# Comment détecter les attaques par usurpation d'identité

### VÉRIFIEZ L'ADRESSE EMAIL

Vous avez reçu un email professionnel à partir d'un compte personnel ? L'adresse email pourrait sembler appartenir à quelqu'un que vous connaissez, et il est toujours préférable de lui répondre à son adresse email officielle. Les pirates peuvent parfois utiliser une adresse email qui ressemble presque à l'adresse officielle d'une entreprise, avec seulement un petit écart, par exemple en remplaçant la lettre « m » par les lettres « rn ».

## Implémentation de la balise « EXTERNE »

La sécurité interne d'ESET a récemment introduit une fonctionnalité qui libelle les emails provenant de l'extérieur du domaine de l'entreprise avec la mention « EXTERNE ». Cela ne permettrait pas d'identifier un imposteur envoyant un email à partir de l'adresse personnelle du PDG, mais cela permettrait d'identifier les emails qui tentent de falsifier le domaine (par exemple en substituant « m » par « rn »).

### VALIDEZ L'INTERLOCUTEUR PAR UN AUTRE CANAL DE COMMUNICATION

Si vous avez reçu un message suspect sur WhatsApp, vous devez écrire à la personne concernée par l'intermédiaire de son adresse email d'entreprise, ou la rappeler. Vous pouvez également simplement **discuter directement avec la personne en face à face**. Ne craignez pas de déranger quelqu'un, même s'il est occupé. Par exemple, vous pourriez être réticent à l'idée de déranger votre PDG. C'est naturel, car plus le poste d'un collègue est élevé, plus nous hésitons à le joindre, surtout lorsqu'il n'est pas au bureau. Dans ce cas, **consultez un autre collègue ou un supérieur**. Par exemple, votre directeur financier ou votre directeur de l'exploitation serait (ou devrait être) certainement au courant d'une facture impayée importante et urgente, alors vérifiez auprès d'eux. N'oubliez pas que la vigilance porte ses fruits.

« Bonjour mon ami. Vous ne me connaissez pas, mais je vous connais très bien. Mieux que ce à quoi on peut s'attendre. C'est bien votre mot de passe ? »

**Des emails comme celui-ci peuvent apparaître dans la boîte de messagerie de n'importe qui. Le mystérieux maître chanteur prétend généralement avoir espionné le destinataire via sa webcam alors qu'il regardait un contenu pour adultes, l'obligeant à payer pour se tirer d'affaire, faute de quoi le pirate contactera sa famille et ses collègues. Pour prouver le piratage réel du PC, un mot de passe utilisé par la victime est fourni. Mais les escroqueries de sextorsion sont exactement cela, des escroqueries.**

## NOUS SOMMES À L'ÂGE D'OR DES ESCROQUERIES DE SEXTORSION

La pandémie de COVID-19 est un exemple frappant de la façon dont les pirates utilisent la technologie et les crises pour diffuser des escroqueries. À mesure que de nombreuses entreprises se sont tournées vers le télétravail et les bureaux à domicile, les collaborateurs n'ont plus été protégés par le réseau de l'entreprise et le nombre de menaces web a augmenté. Des cybercriminels, par exemple, menaçaient d'infecter des victimes et leur famille avec le coronavirus en cas de non-paiement.

---

En payant la somme demandée, vous ne faites que perdre de l'argent et alimenter l'activité des criminels, les aidant à propager d'autres escroqueries.

---

## COMPRENEZ CE QUE VEUT L'ATTAQUANT

Vous devriez savoir que le principal objectif des emails de sextorsion est de vous faire payer, de préférence en bitcoins, ce qui permet aux pirates de collecter l'argent de manière anonyme. Les escroqueries sont un excellent business : Selon l'Internet Crime Complaint Center du FBI, les attaques de sextorsion par email ont causé des pertes d'environ 70,9 millions de dollars en 2020.

## SACHEZ COMMENT RÉAGIR AUX ESCROQUERIES DE SEXTORSION

N'envoyez pas d'argent, ne répondez pas et ne cliquez pas sur des liens ou des pièces jointes. Si vous êtes victime d'une escroquerie de sextorsion, informez toujours les services informatiques ou de sécurité interne de votre entreprise. Et si cela est possible dans votre pays, l'incident devrait être signalé aux autorités (par exemple, si vous êtes au Royaume-Uni, vous pouvez le signaler en ligne à Action Fraud, et aux États-Unis, vous pouvez déposer une plainte sur le site du FBI).

---

La meilleure prévention consiste à créer un mot de passe renforcé ou une phrase de passe. La vente de mots de passe est exactement la raison pour laquelle tout le monde doit modifier son mot de passe de temps en temps, ou doit utiliser des facteurs de protection supplémentaires (authentification multifacteur).

---

## SI LE MOT DE PASSE EST VRAI, NE PANIQUEZ PAS

La mention d'un véritable mot de passe n'est qu'une autre technique pour rendre le destinataire nerveux. Les attaquants peuvent connaître votre mot de passe, mais c'est probablement tout ce dont ils disposent. Ils ont probablement acheté le mot de passe sur le dark web, ou celui-ci a pu être divulgué lors d'une fuite de données.

## NE SOUS-ESTIMEZ PAS LES DÉFIS DE SÉCURITÉ DU TRAVAIL À DISTANCE

Les lieux de travail et les bureaux flexibles sont formidables, mais seulement s'ils sont bien sécurisés et si vous savez comment vous y prendre. Les réseaux wifi sont très exposés aux attaques. Pour veiller à la protection de la connexion et des données de l'entreprise, utilisez de préférence un réseau privé virtuel (VPN), qui vous permet de créer une connexion sécurisée au réseau de l'entreprise.

# Comment les pirates s'introduisent dans votre ordinateur et votre webcam

Lorsqu'elles sont traitées avec précaution, les escroqueries de sextorsion ne font aucun dommage. Néanmoins, vous devriez savoir qu'il existe un moyen pour les pirates d'accéder à votre webcam. Ils utilisent souvent des malwares, par exemple un cheval de Troie, pour infecter votre appareil avec un logiciel d'accès à distance. Mais pour ce faire, ils ont besoin de votre aide. Parfois, il suffit de télécharger un logiciel inconnu. Alors que vous pensez avoir obtenu ce que vous recherchiez, un malware peut se cacher dans le fichier. Vous venez sans le savoir d'aider les pirates à infecter votre appareil. Et ne vous attendez pas à ce que le témoin lumineux de la webcam s'allume dès qu'ils commencent à vous espionner. Ils ne seraient pas incognito si c'était le cas.

Si votre ordinateur est infecté, le pirate peut non seulement voir les moments intimes de votre vie, mais également capturer des données et des documents confidentiels, ou enregistrer des discussions s'ils ont pris le contrôle de votre microphone.

# Sachez comment réagir à un message de sextorsion

**1. Agissez lentement et délibérément, et évitez les actions irréfléchies.**
Les escroqueries de sextorsion ciblent les faiblesses humaines et tentent de vous manipuler pour vous pousser à agir de manière préjudiciable. Donc si vous recevez un message qui a pour but de vous effrayer, prenez du recul et envisagez la possibilité qu'aucun élément de l'email ne soit vrai. En cas de doute, consultez le service informatique ou l'assistance du prestataire de sécurité.

**2. Ne payez pas les escrocs.**
Les emails de sextorsion ne sont généralement que des escroqueries. Cela signifie que les affirmations des criminels ne sont pas fondées. Il est presque certain qu'ils n'ont pas de vidéo de vous ou de ce que vous avez regardé, qu'ils ne font pas partie des forces de police, et qu'ils n'ont pas commandité quelqu'un pour vous espionner.

**3. N'interagissez pas avec l'email.**
Ne répondez pas à l'escroquerie, ne téléchargez pas ses pièces jointes, ne cliquez pas sur les liens intégrés et n'interagissez pas avec les contenus, car ces éléments peuvent conduire à des malwares ou d'autres menaces.

**4. Changez votre mot de passe.**
Dans certains cas, les criminels testent des identifiants fuités, et en cas de réussite, utilisent le compte piraté au moins pour diffuser leurs messages. Par conséquent, si un pirate indique posséder l'un de vos mots de passe réels, changez-le immédiatement et activez l'authentification multifacteur.

**5. Envoyez l'email à votre service informatique.**
Si votre entreprise ne dispose pas de personnel informatique, le moins que vous puissiez faire est d'analyser l'ordinateur et le réseau avec une solution de sécurité fiable, et de vous assurer qu'aucun de vos mots de passe n'a été divulgué ou compromis.

**6. Sécurisez votre webcam.**
Pour éviter tout détournement de la webcam intégrée, utilisez un logiciel de protection ou mettez au moins un morceau de ruban adhésif opaque sur la caméra. Ainsi, vous pouvez être certain que les criminels n'ont aucun moyen d'enregistrer une vidéo de vous assis devant l'appareil.

**7. Utilisez une solution antispam.**
Une solution de sécurité fiable dotée d'une fonction antispam peut également contribuer à empêcher les escroqueries de sextorsion d'atteindre votre boîte de messagerie à l'avenir.

# Autres types de techniques d'ingénierie sociale que vous devez reconnaître

Les **scarewares** sont un type de malware qui tente d'inciter les victimes à acheter et télécharger des logiciels potentiellement dangereux. C'est une méthode qui attire très rapidement l'attention des gens et... les effraie. Des fenêtres popup difficiles à fermer, des éditeurs de logiciels dont vous n'avez jamais entendu parler et des analyses non autorisées de votre ordinateur à la recherche de virus, sont des caractéristiques typiques des scarewares.

Ces programmes affichent généralement une liste de dizaines ou de centaines de faux virus. Mais les programmes d'alerte n'analysent pas votre ordinateur, et les résultats prétendument découverts sont faux. Les avertissements concernant une infection ne font que vous manipuler pour ouvrir la porte à une véritable infection. Ces escroqueries s'appuient souvent sur de faux logiciels de sécurité, tels que Advanced Cleaner, SpyWiper ou System Defender.

## Utilisez des logiciels connus, testés et à jour

Vous saurez ainsi qu'une invitation à télécharger un logiciel gratuit peut être une escroquerie. Il est également très utile d'utiliser des bloqueurs de fenêtres popup sur vos appareils professionnels et des filtres d'URL. Mettez en place des outils de sécurité web et des pare-feux pour stopper les attaquants.

**Les arnaques au support technique** sont étroitement liées aux scarewares. Mais à la différence des scarewares, elles prétendent provenir d'une société établie telle que Microsoft. Elles ne commenceront pas automatiquement à analyser votre ordinateur. Au lieu de cela, elles peuvent vous demander d'ouvrir certains fichiers, et vous informer ensuite que ces fichiers présentent un problème... qui n'existe pas. Selon la Commission fédérale du commerce (FTC), les escroqueries liées au support technique ne sont pas rares. En 2019, la FTC a reçu plus de 100 000 signalements d'escroqueries de ce type.

# Checklist pour les admin. informatiques :

## 5 façons de protéger votre entreprise des attaques d'ingénierie sociale

**1.** Formation régulière de tous les collaborateurs à la cybersécurité, y compris les cadres supérieurs et le personnel informatique. N'oubliez pas que cette formation doit montrer ou simuler des scénarios réels. Les éléments appris doivent être concrets et, surtout, testés activement à l'extérieur de la salle de formation.

**2.** Recherchez les mots de passe faibles qui pourraient ouvrir une brèche dans le réseau de votre entreprise pour les attaquants. Protégez également les mots de passe par une couche de sécurité supplémentaire en implémentant l'authentification multifacteur.

**3.** Mettez en œuvre des solutions techniques pour lutter contre les communications frauduleuses afin que les spams et les messages d'hameçonnage soient détectés, mis en quarantaine, neutralisés et supprimés. Des solutions de sécurité, dont plusieurs fournies par ESET possèdent une partie ou la totalité de ces fonctionnalités.

**4.** Créez des politiques de sécurité compréhensibles que les collaborateurs pourront utiliser et qui les aideront à identifier les mesures à prendre en cas d'exposition à une attaque d'ingénierie sociale.

**5.** Utilisez une solution de sécurité et des outils d'administration, tels qu'ESET PROTECT Console pour protéger les endpoints et les réseaux de votre entreprise. Elle fournit aux administrateurs une visibilité totale, et la possibilité de détecter et d'atténuer les menaces potentielles sur le réseau.

Depuis plus de 30 ans, ESET® développe des logiciels et des services de sécurité informatique pour protéger le patrimoine numérique des entreprises, les infrastructures critiques et les consommateurs du monde entier contre des cybermenaces. Nous protégeons les terminaux fixes et mobiles, les outils collaboratifs, et assurons la détection et le traitement des incidents. Établis dans le monde entier, nos centres de R&D récoltent et analysent les cybermenaces pour protéger nos clients et notre monde numérique.
Pour plus d'informations, consultez le site www.eset.com/fr/
ou suivez-nous sur LinkedIn, Facebook et Twitter.



Digital Security
**Progress. Protected.**