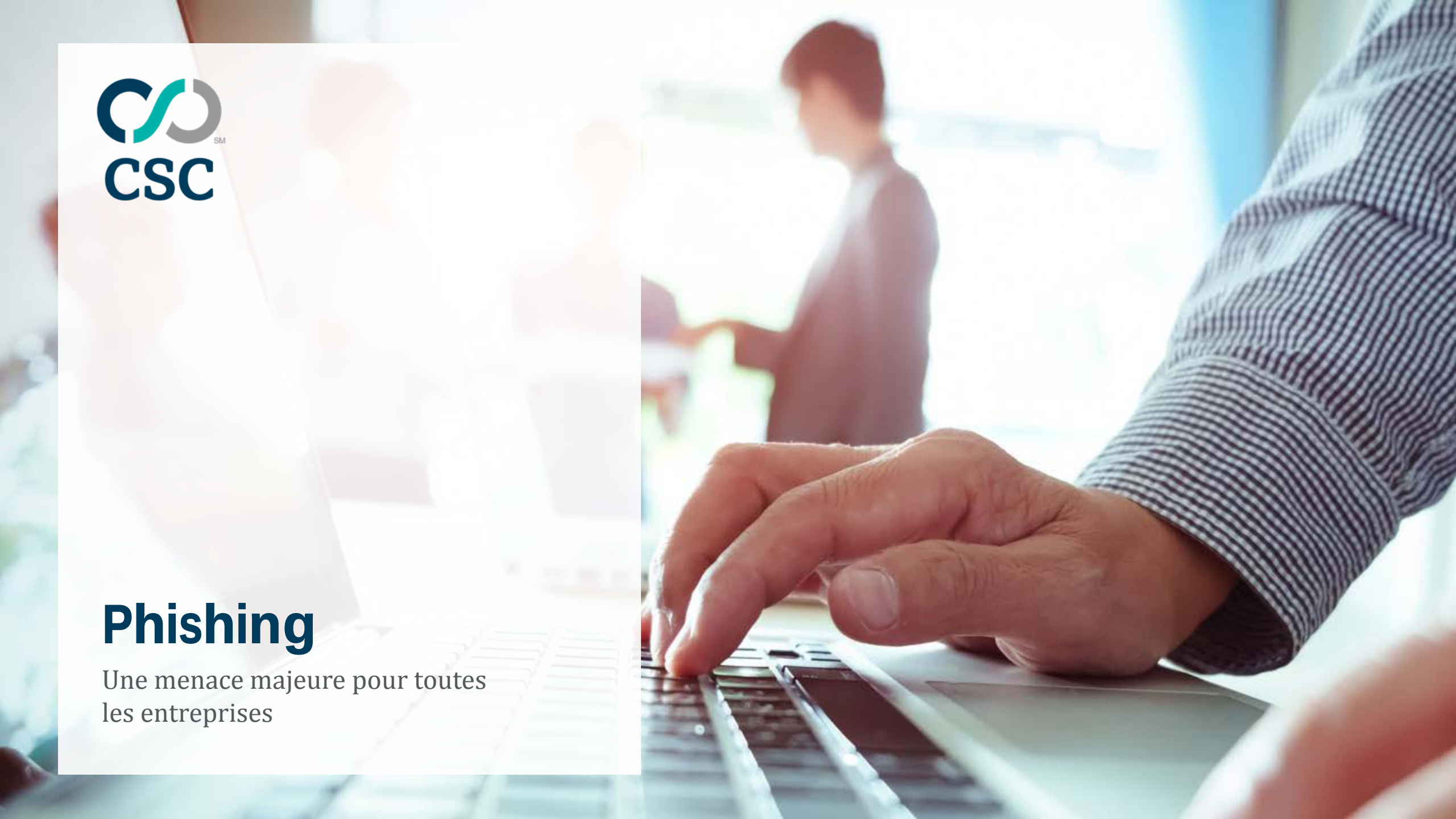
Kit d’outils de cyber-sécurité

Se défendre contre le phishing, sécuriser les actifs de la société et créer des mots de passe solides



Phishing

Une menace majeure pour toutes les entreprises

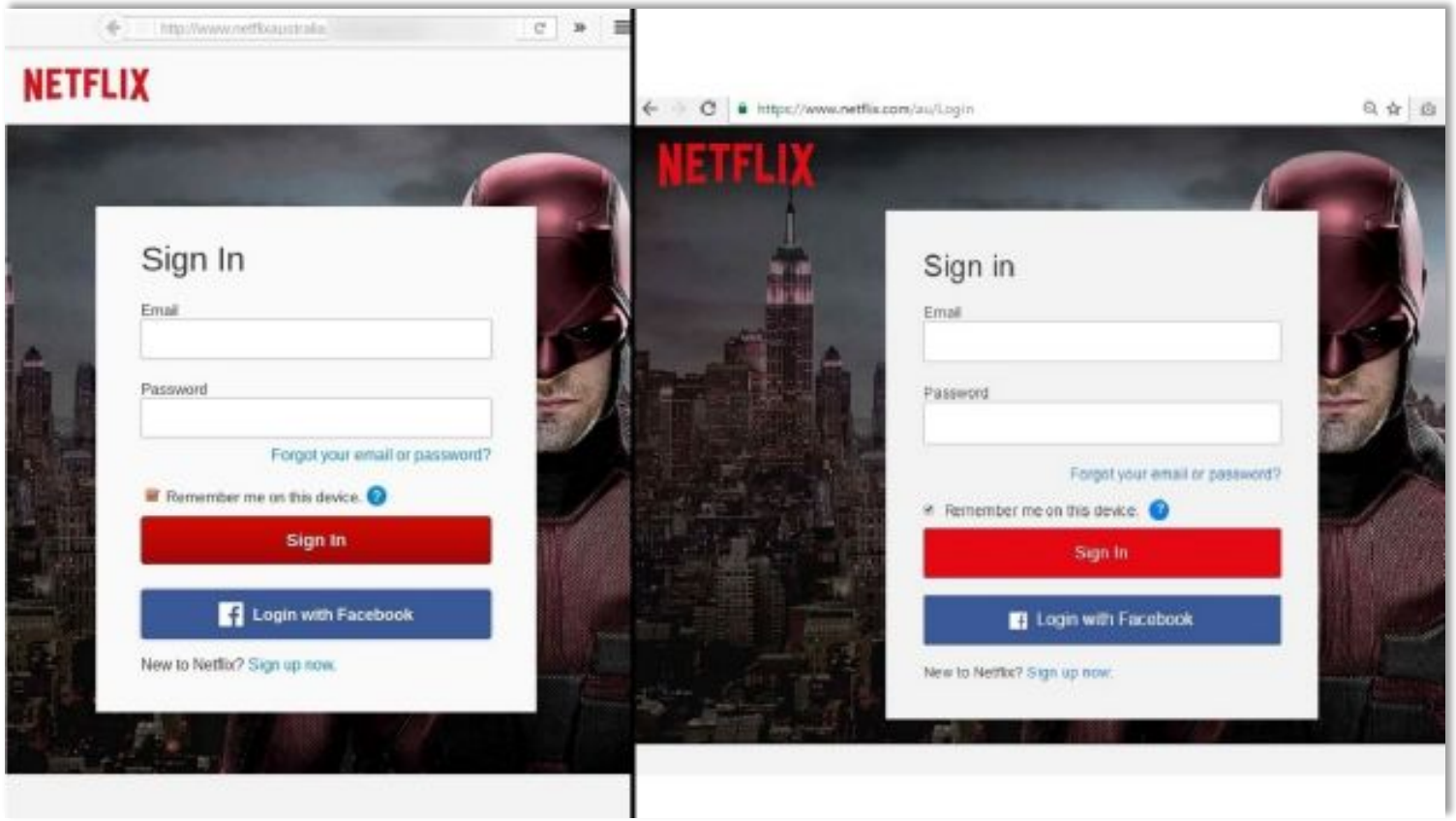
Qu’est-ce que le phishing ?

« Le **phishing** est un mécanisme frauduleux reposant à la fois sur l’ingénierie sociale et le subterfuge technique, qui a pour but de voler les données d’identification personnelle d’un utilisateur et les authentifiants de ses comptes financiers. »

- En 2016, les campagnes de phishing ont cumulé 1 220 523 attaques – soit 65 % de plus qu’en 2015.

- Chaque jour, ce sont quelques 190 000 nouveaux logiciels malveillants qui sont trouvés.

Site de phishing : lequel est contrefait ?



Source de l'image : http://www.theage.com.au/business/consumer-affairs/phishing-emails-and-other-online-scams-on-the-rise-as-australians-lose-millions-of-dollars-20161115-gspnar.html

CSC

Impact : Le coût d’une intrusion

48 % de l’ensemble des intrusions ont été causées par des attaques malicieuses ou criminelles.

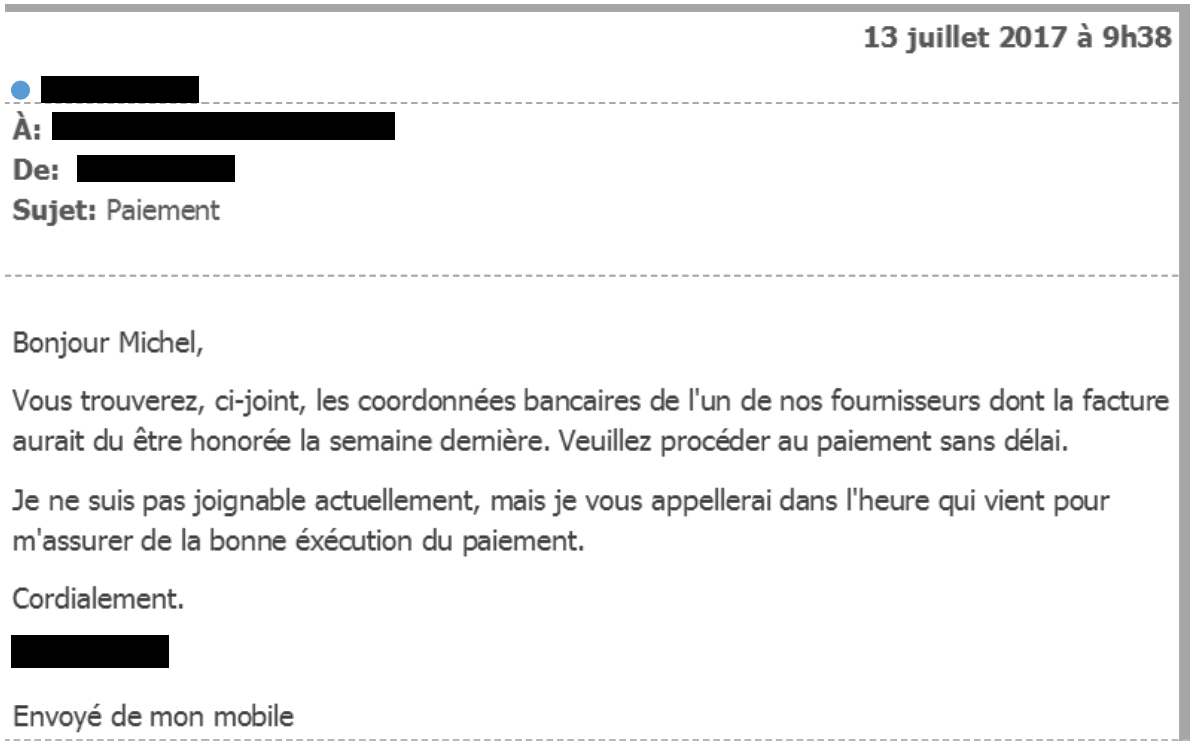
Phishing par e-mail a causé au moins 3,1 milliards $ de pertes totales dans le monde entre 2013 et 2015.

Le mode opératoire

- Les cybercriminels utilisent les graphiques, le style linguistique et les mots clés utilisés par la marque copiée.
- Les messages qu'ils envoient suscitent la peur et appellent généralement une réponse immédiate.
- Pour être plus convaincants, les cybercriminels endossent le rôle d'une personne investie d'une autorité.

Les attaques par phishing sont plus sophistiquées, plus invasives et plus convaincantes que nous le pensons.

Exemple d’e-mail urgent émanant d’une autorité



13 juillet 2017 à 9h38

[redacted]

À: [redacted]

De: [redacted]

Sujet: Paiement

Bonjour Michel,

Vous trouverez, ci-joint, les coordonnées bancaires de l'un de nos fournisseurs dont la facture aurait du être honorée la semaine dernière. Veuillez procéder au paiement sans délai.

Je ne suis pas joignable actuellement, mais je vous appellerai dans l'heure qui vient pour m'assurer de la bonne éxécution du paiement.

Cordialement.

[redacted]

Envoyé de mon mobile

Source de l’image originale : http://www.mailguard.com.au/blog/whaling-ceo-fraud-business-email-compromise-targeted-spear-phishing-attacks-continue-to-trouble-businesses

CSC

Les différents types de phishing : Phishing par e-mail

Actuellement, la plus grande menace pour les entreprises réside notamment dans le spear-phishing et les e-mails frauduleux émanant prétendument d'un Pdg ; ce type de phishing utilise l'identité d'une personne ou une ressemblance avec une entreprise.

- 30 % des e-mails de phishing sont ouverts et 12 % des cibles vont au-delà de l'ouverture en cliquant sur le lien ou la pièce jointe fournis.

- 97 % des gens dans le monde ne sont pas en mesure d'identifier correctement un e-mail de phishing sophistiqué.

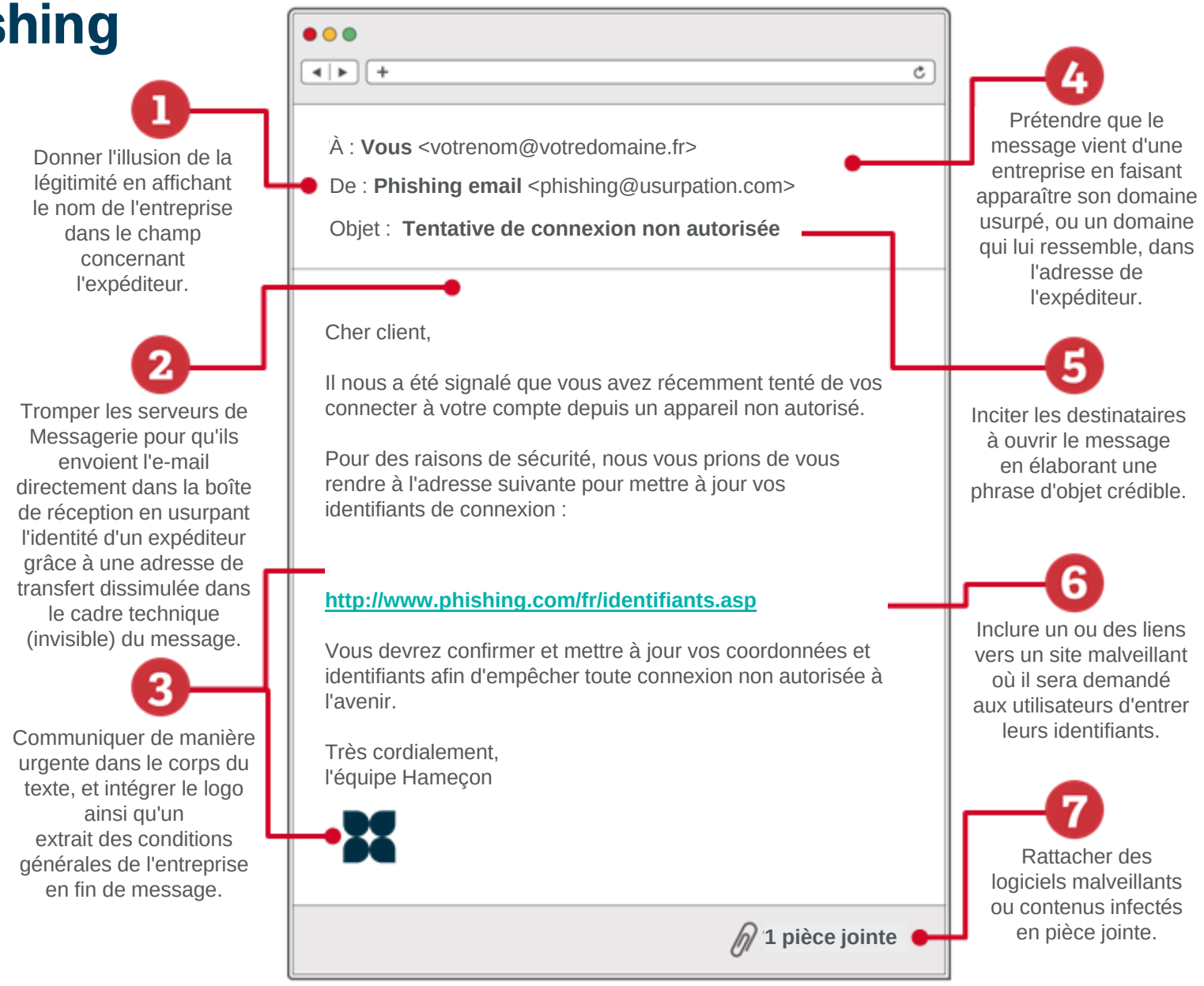
Les différents types de phishing : Phishing par e-mail

En outre :

- Les cybercriminels font évoluer leurs tactiques de phishing par e-mail afin de contourner les filtres de courrier indésirable.
- La disponibilité des informations sur les réseaux sociaux facilite les recherches effectuées lors de la création d'un e-mail de spear-phishing.
- À l'époque où tout le monde est connecté en permanence à son smartphone, les e-mails sont consultés régulièrement, ce qui signifie que les e-mails de phishing sont lus plus tôt, ouvrant ainsi une autre porte vulnérable par laquelle s'engouffrent les cybercriminels—en particulier, lorsqu'un salarié pense recevoir un e-mail de son Pdg à 21h00.

Analyse d'un e-mail de phishing

97 % des gens dans le monde ne sont pas en mesure d'identifier correctement un e-mail de phishing sophistiqué.



Liste des 5 premiers types de leurres par e-mail qui amènent les destinataires à cliquer dessus

Restitution au mot près du contenu fourni par Proofpoint—une entreprise de cyber-sécurité de nouvelle génération

« Veuillez trouver votre facture ci-jointe »

« Cliquez ici pour ouvrir votre document numérisé »

« Votre paquet a été expédié »

« Je veux passer commande pour la liste jointe »

« Veuillez vérifier cette transaction »

E-mail : À faire et à Ne pas faire

- Faites preuve de prudence vis-à-vis de toutes les pièces jointes, quelle que soit la personne qui semble les avoir envoyées. Surtout celles qui présentent des formats suspects, tels que .zip, .exe.

- Survolez les liens avec le curseur de la souris (sans cliquer) afin de vérifier qu'ils dirigent bien vers les bonnes URL d'un site web. Assurez-vous ainsi qu'il s'agit bien du site web que vous souhaitez visiter. C'est là que vous pourrez voir si la page d'accueil vers laquelle dirige le lien correspond bien à celle de la marque du site sur lequel vous entendez vous rendre et qu'il ne s'agit pas d'une copie de ce site (laquelle copie inclura généralement une série de mots, lettres et caractères non identifiables). En cas de doute, ne cliquez pas.

E-mail : À faire et à Ne pas faire

- Lorsque vous cliquez sur « répondre » à un e-mail, vérifiez toujours les adresses e-mail des destinataires. De même qu'il est conseillé de vérifier les URL d'un sites web comme décrit précédemment, vous pouvez aussi saisir manuellement les adresses des destinataires ou les insérer à partir d'un répertoire.

- Utilisez des filtres de courrier indésirable et des protections à jour. Une solution à jour contre les virus, le phishing et les courriers électroniques malicieux est incontournable en protection de base. Assurez-vous que ces protections soient régulièrement mises à jour.

- Lorsque vous visitez des sites web, vérifiez la barre verte et le « S » à la fin de HTTP. Cela vous permet de vérifier les certificats SSL (Secure Sockets Layer) du site web—une indication selon laquelle la connexion à des pages et formulaires web où vous pouvez être amené(e) à saisir des informations personnelles permettant votre identification est sécurisée.

CSC

E-mail : À faire et à Ne pas faire

- Si vous ne reconnaissez pas l'expéditeur, méfiez-vous des liens et pièces jointes. Même lorsque vous connaissez l'expéditeur, restez PRUDENT(E). Vérifiez le contenu de l'e-mail en appelant l'expéditeur ou contactez directement l'entreprise—surtout si quelque chose vous semble suspect.

- Ne répondez jamais à des e-mails vous demandant de fournir des informations permettant votre identification ou un accès quelconque, surtout lorsque la demande semble urgente. Et ce, même si la demande semble émaner de votre Pdg ou de votre directeur financier. Même si vous faites partie des personnes avec lesquelles les dirigeants de votre entreprise communiquent régulièrement. Il n'y a aucun mal à vérifier au préalable auprès de l'expéditeur supposé, par téléphone ou en personne.

CSC

E-mail : À faire et à Ne pas faire

- Ne cliquez pas sur les menus contextuels qui pourraient vous rediriger vers un site frauduleux ou lancer le téléchargement d'un logiciel malveillant.

- Soyez également prudent(e) avec les fenêtres de dialogue en direct, surtout lorsqu'on vous y demande des informations personnelles.

Les différents types de phishing : Par téléphone

Également connu sous le nom de phishing vocal ou « vishing », il s'agit d'un appel téléphonique ayant pour but de recueillir des informations personnelles.

Le numéro d'appel de l'émetteur de l'appel peut être falsifié sachant que des systèmes téléphoniques automatisés et complexes sont utilisés pour amener les gens à croire que l'appel provient de leur banque—et qu'il concerne leur carte bancaire ou tout autre mouvement de compte—et bien entendu : il s'agit toujours d'une urgence !!!

Les textos (phishing par SMS ou « smishing ») sont également utilisés. Ils incitent généralement à agir immédiatement via un lien sur lequel cliquer ou un numéro à appeler afin de « confirmer » des informations personnelles.

Si vous cliquez sur le lien ou appelez le numéro fourni, des logiciels malveillants spécialisés dans le vol de mots de passe pourront s'installer automatiquement sur votre téléphone.

Téléphone : À faire et à Ne pas faire

- Vérifiez toujours l'identité de l'appelant. Si vous répondez à l'appel, demandez un numéro et une ligne directe à rappeler, ou bien des informations que l'appelant est supposé connaître à votre sujet.

- Recherchez sur Internet d'éventuelles plaintes au sujet de ce numéro. Un format inhabituel de numéro d'appel ou de code pays peut indiquer qu'il s'agit d'un appel VoIP (effectué via Internet) ou d'un texto provenant de systèmes automatisés.

- Recherchez le numéro du service client de l'entreprise. Plutôt que de rappeler le numéro communiqué lors de l'appel ou dans le texto, vérifiez que ce numéro soit correct en vous reportant à votre carte bancaire, vos relevés de compte, et en dernier ressort, en faisant une recherche en ligne.

CSC

Téléphone : À faire et à Ne pas faire

- Ne répondez jamais aux textos de phishing par SMS. Et ne cliquez jamais sur les liens fournis, surtout s'ils sont courts et n'indiquent pas vers quoi ils redirigent.

- Ne communiquez jamais vos données bancaires personnelles. Préservez la confidentialité de votre code de carte bancaire et de son numéro de vérification CVV. Aucune banque ne vous demandera jamais de telles informations vu qu'elle les détient déjà.

CSC

Les différents types de phishing: Les réseaux sociaux

Les réseaux sociaux possèdent peu de contrôles de sécurité, ce qui rend facile—et gratuit—la mise en place par des pirates de faux comptes imitant de véritables entreprises, avec des logos, un contenu et des offres semblant plus que réalistes. Ces pirates prétendent aussi parfois être des employés de l'entreprise copiée et insèrent un lien dirigeant vers la véritable entreprise afin de gagner la confiance des utilisateurs de réseaux sociaux.

- 1 tentative de phishing sur 5 se fait désormais via les réseaux sociaux.
- En effet, un tweet demandant une assistance adressé à *@customerservice* peut facilement être intercepté et faire l'objet d'une « réponse » provenant d'une adresse telle que *@customer-service*.

Réseaux sociaux : À faire et à Ne pas faire

- Faites attention aux réponses et commentaires reçus sur les réseaux sociaux suite à une réclamation de votre part. Ils peuvent provenir de comptes frauduleux. Choisissez plutôt de contacter une entreprise par des voies officielles.

- Faites attention aux sites web et applications vers lesquels pointent les profils des réseaux sociaux.

Réseaux sociaux : À faire et à Ne pas faire

- N’ajoutez pas de contacts non vérifiés à votre liste de contacts sur le réseau social que vous utilisez, même si ledit contact prétend être de votre entreprise. Et faites attention à l’ajout d’inconnus, notamment de recruteurs, tant que vous ne vous êtes pas renseigné(e) à leur sujet.

- Ne cliquez pas sur les liens provenant de sources non fiables. Nombre de canaux sociaux utilisent des liens raccourcis qui masquent la véritable URL. Or, le lien peut diriger vers un courrier indésirable ou un logiciel malveillant.

Réseaux sociaux : À faire et à Ne pas faire

- Ne répondez pas aux e-mails ou messages suspects. Même s'ils proviennent d'amis, car s'ils vous semblent suspects ou inhabituels, cela peut signifier que le compte de l'ami en question a été piraté. Informez immédiatement l'ami concerné par un autre moyen de communication.

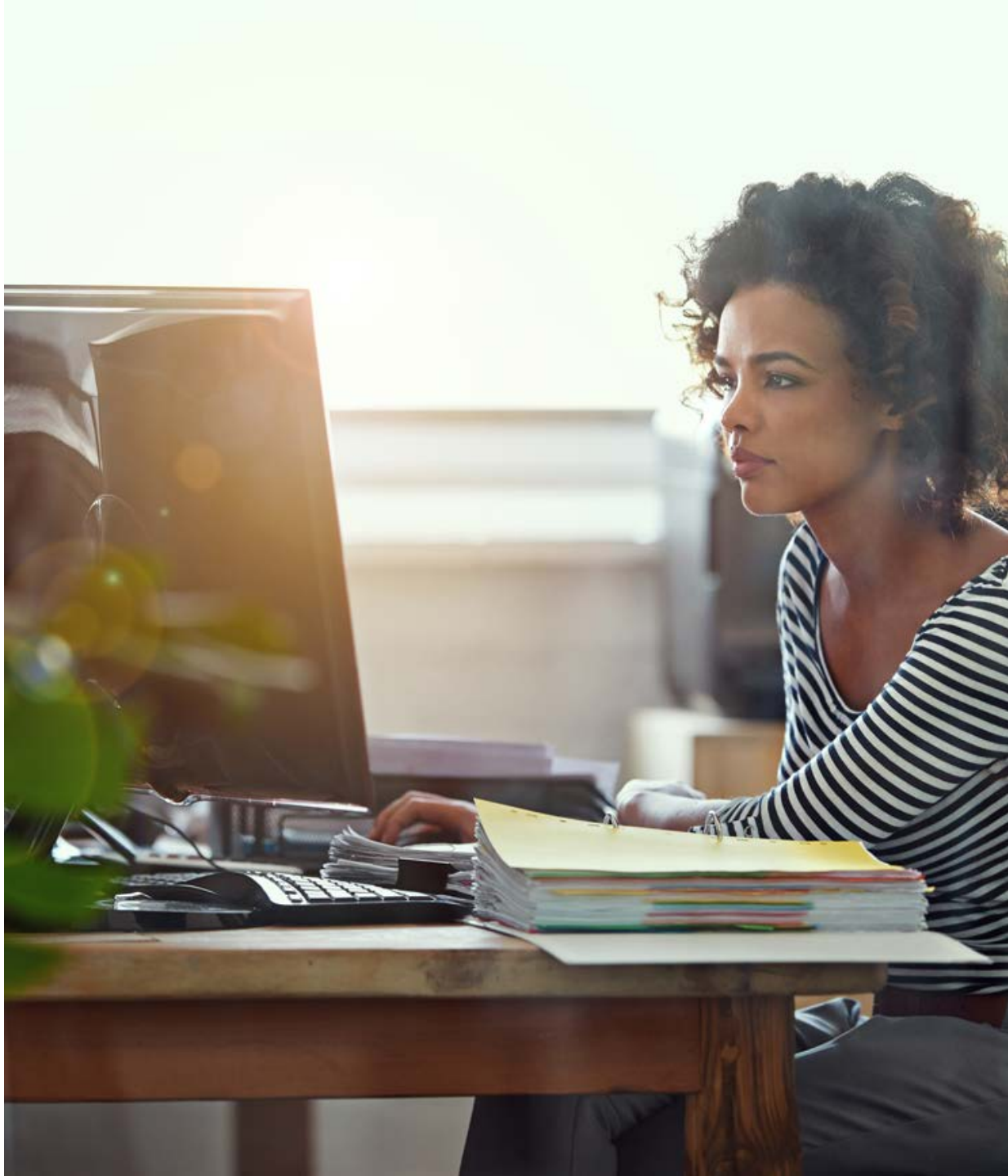
- Ne communiquez jamais d'informations confidentielles ou financières. Même lorsqu'une conversation semble privée, ne communiquez pas d'informations confidentielles sur les réseaux sociaux. Pas même de photos susceptibles de reproduire un relevé de compte ou une facture.

Sécuriser les ressources de l’entreprise

Réduire les risques inhérents

Des effectifs mobiles

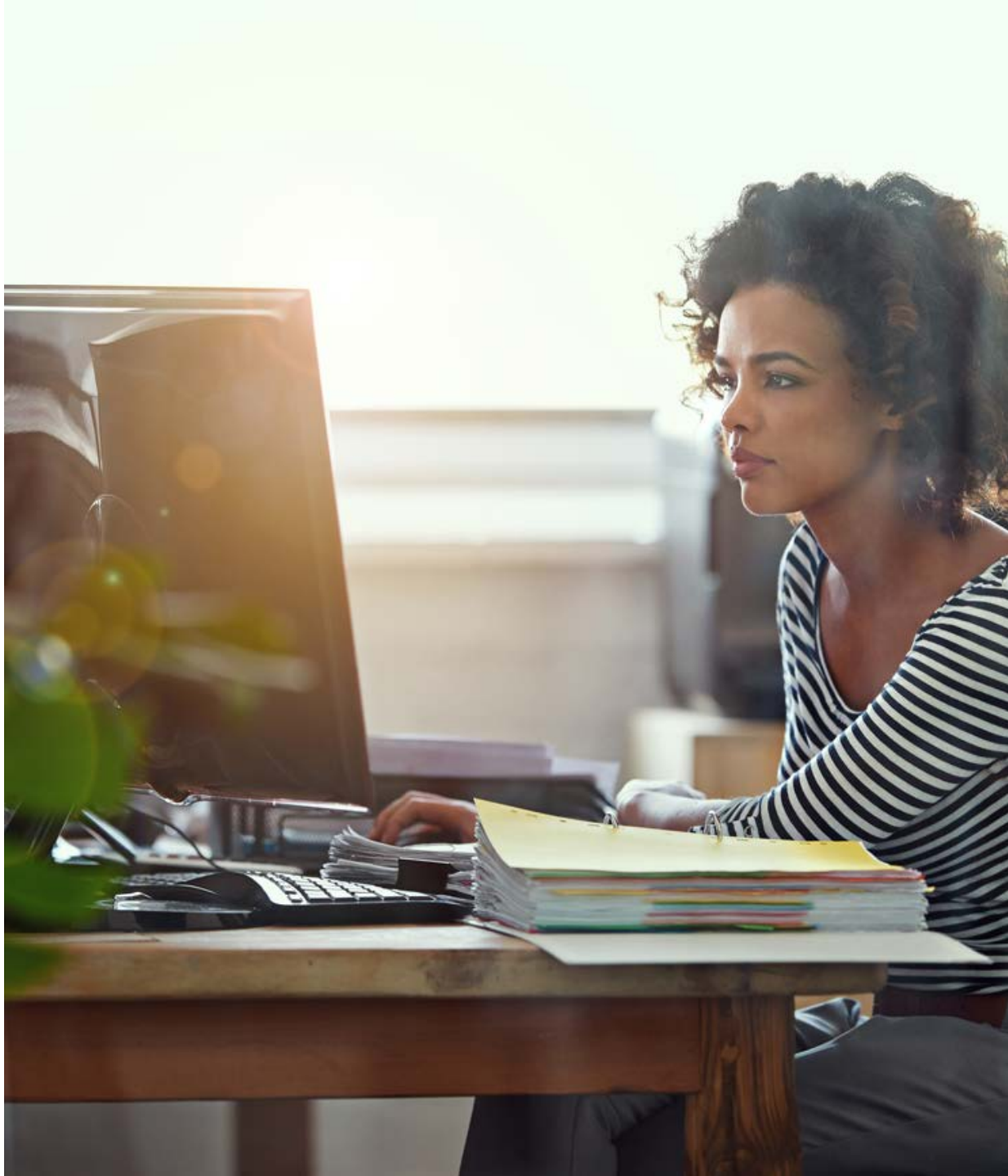
- Près des ¾ de l'ensemble de la population active des États-Unis devraient adopter la mobilité d'ici 2020.
- 12,1 milliards d'appareils mobiles devraient être en circulation d'ici 2018.
- Les prédictions de Gartner anticipent que d'ici à fin 2017, plus de la moitié des entreprises du monde demanderont aux employés d'apporter leur propre appareil.
- Les applications les plus populaires téléchargées sur les appareils mobiles des employés sont dédiées à la gestion des e-mails, des agendas et des contacts (84 %), viennent ensuite les applications de documentation et d'édition (45 %), puis intranet (43 %).



Les risques inhérents en termes de sécurité

Les connexions constantes engendrent des risques :

- 1 entreprise sur 5 a déclaré avoir été victime d'une faille de sécurité liée à la connexion des appareils mobiles des employés, à des téléchargements ou à des WiFis infectés.[2].
- 39 % des entreprises sondées ont indiqué que les appareils utilisés dans le cadre du programme BYOD comme ceux appartenant à l'entreprise ont, à un moment ou un autre, téléchargé des logiciels malveillants[2].
- L'employé moyen porte en permanence plus de 2 appareils sur lui, et pratiquement personne n'utilise plus les connexions Ethernet, ce qui rend le WiFi incontournable[3].
- Un pourcentage élevé de points d'accès WIFI sont dotés d'une sécurité obsolète, voire, d'aucune sécurité[4].



Mobiles : À faire et à Ne pas faire

- Visitez des sites sécurisés—vérifiez que l'URL contienne bien le protocole sécurisé HTTPS ; il s'agit d'une URL de couleur verte, ainsi qu'un cadenas de chiffrement—et limitez vos transactions financières sur les réseaux publics.

- Utilisez un réseau privé virtuel pour chiffrer votre trafic en ligne, en particulier lors d'une connexion à un réseau d'entreprise.

- Sécurisez votre appareil avec des mots de passe forts.

- Autorisez l'authentification bifactorielle pour plus de sécurité.

CSC

Mobiles : À faire et à Ne pas faire

- Maintenez vos logiciels à jour avec des correctifs de sécurité, une protection antivirus, des bloqueurs de spam et une détection des logiciels espions.

- Lors de la réception d'e-mails, restez conscients des risques d'escroquerie au phishing par des liens malveillants.

- Lors de la synchronisation de votre téléphone ou de votre ordinateur portable avec un dispositif Bluetooth®, assurez-vous de ne pas vous trouver dans un espace public dans lequel le code PIN de votre appareil pourrait être compromis et mettez le périphérique Bluetooth à utiliser en mode caché (non détectable).

CSC

Mobiles : À faire et à Ne pas faire

- Ne vous connectez pas à des points d'accès WiFi ouverts non sécurisés (vérifiez la protection par mot de passe ; il s'agit d'un indicateur selon lequel le chiffrement a été activé).

- Ne téléchargez pas de programmes ou d'applications qui ne vous inspirent pas confiance.

Sécurité du mot de passe

La dernière ligne de défense

L’importance de la sécurité du mot de passe

Un bon mot de passe est un moyen gratuit et facile de vous prémunir contre les atteintes aux données.

- 80 % des effractions aux données analysées se sont révélées avoir été effectuées pour en tirer un gain financier

- …tandis que 63 % d’entre elles ont été causées par des mots de passe trop communs, faibles ou volés.

Compromission des mots de passe

Les mots de passe peuvent être considérés comme la dernière ligne de défense avant qu'un cybercriminel ne fasse main-basse sur vos données. Les mots de passe peuvent être compromis par :

- La fraude par phishing, visant à s'emparer des données personnelles d'une personne, telles que son nom d'utilisateur et son mot de passe, ses références bancaires, etc.
- Les attaques frontales par des pirates qui essaient systématiquement toutes les phrases de mot de passe et séquences possibles.
- Une faille de sécurité dans le système informatique ou sur le site web d'une entreprise qui a été piratée, ce qui a pour résultat de compromettre des millions de comptes.

Défaillances courantes des mots de passe

Avant comme après une atteinte aux données, un mot de passe fort reste la meilleure protection. Créez un mot de passe dont vous puissiez vous souvenir, sans qu'un cybercriminel ne soit en mesure de le deviner pour autant—donc, évitez le nom de votre chien ! Voici quelques mots de passe fréquemment piratés que vous devrez éviter :

- Les 3 mots de passe les plus populaires sont : *Password1*, *Welcome1* et *P@ssword*.
- Les mots clés les plus fréquemment utilisés dans les mots de passe sont des noms de bébés, d'animaux domestiques et de villes.
- Environ 30 % des séquences à 10 caractères les plus courantes se présentent sous le format suivant : Lettre majuscule (U) suivie d'une série de lettres minuscules (l) et se concluant par des chiffres (#), comme suit : *Ullllll##.* Par exemple : *Hello11*.

Des mots de passe : À faire et à Ne pas faire

- La complexité est importante, mais c'est la longueur du mot de passe qui est fondamentale. L'utilisation de longs mots de passe (au moins 10 caractères) rend leur décodage difficile par les pirates.

- Les mots de passe à 8 caractères sont « craqués » en une journée seulement à l'aide de techniques brutales ; les mots de passe de 10 caractères requièrent environ 591 jours—soit près de 600 fois plus d'efforts ! Utilisez des suites d'initiales qui forment une phrase dont vous pourrez vous souvenir, mais qui sembleront aléatoires à d'autres personnes. Par exemple : *TW2gsi2QT&bd* = citation de Walt Disney : « The way to get started is to quit talking and begin doing. » (« La meilleure façon de se lancer, c'est d'arrêter de parler et de commencer à faire. ») Utilisez toujours un mot de passe-maître et un gestionnaire de mots de passe.

- Outre des mots de passe sûrs, l'authentification bifactorielle peut contribuer à réduire les compromissions. Les pirates préfèreront s'en prendre à une cible plus facile plutôt que de se démener pour compromettre deux modes d'authentification.

CSC

Des mots de passe : À faire et à Ne pas faire

- Évitez d'utiliser des séquences prévisibles, de type *Ullllll##*, ou des clés de sécurité adjacentes, telles que « *azerty* » et « *qsdf* ».

- N'utilisez pas de définitions du dictionnaire dans votre mot de passe ni les noms de membres de votre famille ou de vos animaux domestiques, pas plus que votre adresse ou d'autres d'informations personnelles telles que votre date de naissance, votre numéro de sécurité sociale ou votre numéro de téléphone.

- N'utilisez pas le même mot de passe pour plusieurs sites. En cas d'atteinte à vos données sur l'un ou l'autre de vos comptes, même le plus complexe des mots de passe deviendrait inutile après avoir été réutilisé pour plusieurs comptes. N'utilisez jamais le mot de passe de votre compte e-mail pour d'autres site web.

- Ne conservez pas votre mot de passe rédigé en texte clair sur un ordinateur, quel qu'il soit.

CSC

Merci !