Spam, phishing, ransomwares…

Adoptez tous les bons les arnaques

© adobestock.com

réflexes pour éviter

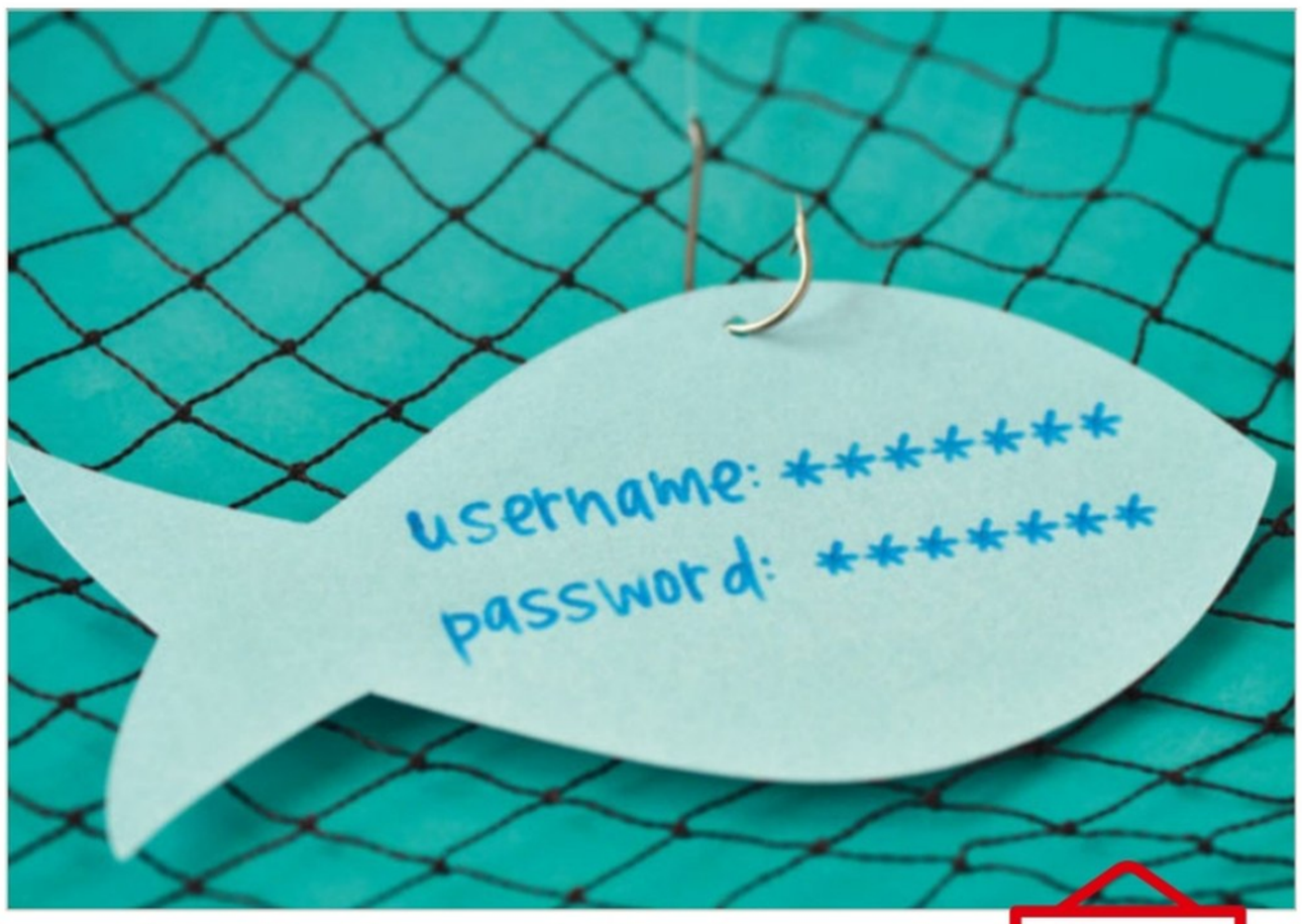
Avec le développement d'Internet, les dangers qui peuvent survenir du réseau des réseaux sont croissants. Les attaques sont de plus en plus sophistiquées pour tenter de récupérer des données, de soutirer de l'argent ou pire encore. Voici comment détecter les menaces, éviter les arnaques sur Internet et comment réagir en cas de doute ou de problème avéré.

Dossier réalisé par Sylvain Pichot

Il existe de nombreux dangers provenant d'Internet comme on peut le dire de manière usuelle, mais plus précisément, il s'agit de personnes malveillantes qui utilisent le réseau des réseaux pour tenter de se frayer un chemin jusqu'à vos données personnelles afin de les exploiter et d'en tirer un maximum de profit.
Selon une enquête publiée par le site Deloitte, fournisseur mondial de services d'audit, d'assurance et de conseil, près de 91 % de toutes les cyberattaques commencent par un email de phishing, et les techniques de phishing sont impliquées dans 32 % de toutes les failles de données à succès.

Votre confiance, vos données, votre argent…

L'hameçonnage, ou phishing en anglais, est le principal mode opératoire utilisé par les cybercriminels pour récupérer les informations personnelles et/ou professionnelles des internautes. Il s'agit d'une technique frauduleuse qui consiste à berner les utilisateurs d'un service afin de l'inciter à transmettre ses données personnelles (ou professionnelles) telles que les coordonnées d'un compte bancaire, des mots de passe, des identifiants, etc. en se faisant passer pour une personne ou un service de confiance. Le phishing peut prendre la forme d'un SMS, d'un faux message électronique, d'un appel téléphonique, d'un compte de réseau social, du site d'un fournisseur d'énergie, d'une administration, etc.
Il existe aussi d'autres types d'escroquerie basés sur l'usurpation d'identité. Ceux-ci sont assimilables à l'hameçonnage, mais consistent plus spécifiquement à tenter de récupérer directement de l'argent auprès des



© adobestock.com

victimes. Plusieurs exemples peuvent ainsi être cités comme :

- les fausses propositions d'emploi où les cybercriminels demandent un maximum d'informations personnelles afin de pouvoir monter une escroquerie ;
- les tentatives de faux ordres de virement qui consistent à se faire passer pour un responsable d'une administration ou un fournisseur afin de faire réaliser un virement frauduleux sur le compte de la personne malveillante ;
- le chantage à la webcam piratée où les malfrats font croire qu'ils ont réussi à pirater la webcam ou le smartphone d'un utilisateur afin de lui demander une rançon contre la non-divulgation des vidéos prétendument enregistrées à son insu.

Récemment, il a beaucoup été question d'escroquerie au Compte Personnel de Formation (CPF) où des personnes malveillantes usurpaient l'identité d'organismes officiels afin de récupérer le compte formation d'une victime pour en détourner les fonds.

Le spam est (aussi) un courrier électronique indésirable, c'est-à-dire une communication non sollicitée qui est envoyée à de très nombreuses personnes et qui a pour principal but d'inciter les destinataires à cliquer sur différents liens frauduleux ou sur des images intégrées, voire d'ouvrir les pièces jointes. Ces actions peuvent créer une faille dans la sécurité de l'ordinateur de l'utilisateur et permettre d'ouvrir un accès aux cybercriminels afin qu'ils puissent accéder à toutes les données enregistrées sur les disques durs de la machine, voire celles du réseau, le cas échéant. Les spams peuvent aussi servir à engendrer des coûts non prévus par les utilisateurs si, par exemple, la connexion Internet est payante au volume échangé. En outre, vu qu'il s'agit de courriers non sollicités, les victimes sont obligées de les traiter, entraînant ainsi une perte de temps et de productivité.

Les spams étaient extrêmement utilisés par les pirates informatiques, il y a encore quelques années, mais c'est une technique qui est aujourd'hui en perte de vitesse notamment face à un autre type d'attaque très tendance : le ransomware. En effet, le ransomware (en anglais) ou rançongiciel consiste à bloquer l'accès à un appareil ou à certains fichiers enregistrés sur la machine d'un utilisateur et d'exiger le versement d'une rançon en échange de pouvoir à nouveau accéder à l'appareil ou aux données bloquées. La machine peut être infectée après l'ouverture d'un lien malveillant, d'une pièce jointe frauduleuse dans un e-mail ou lors de la navigation sur des sites compromis.

COMMENT SE FAIRE REMBOURSER EN CAS DE PHISHING OU AUTRE ATTAQUE ?

En théorie, votre banque doit vous rembourser à la hauteur des sommes perdues en cas d'attaque de type phishing. Pour cela, il faut commencer par faire opposition sur la carte bancaire en contactant directement votre banque au numéro indiqué, depuis l'application correspondante ou en appelant le service interbancaire au **0 892 705 705** disponible 24h/24 et 7j/7. Contestez ensuite les potentiels débits frauduleux que vous constatez sur votre relevé de compte. Faites des captures d'écran, le cas échéant, afin de garder une trace. Les dépôts de plainte sont devenus inutiles. Aucune assurance spécifique des moyens de paiement n'est nécessaire pour être remboursé. Constituez un dossier de fraude auprès de votre banque afin de faire valoir votre droit à être indemnisé de la fraude constatée, selon la loi et plus particulièrement les articles 133-1-1 et 133-24 du Code monétaire et financier. La banque doit vous rembourser de la somme débitée et des éventuels agios dans les meilleurs délais. Il est toutefois possible que votre banque refuse de vous redonner l'intégralité de la somme mettant en avant la prise en charge de votre part d'une franchise qui peut s'élever à 50 € au maximum (selon l'article 133-19 du Code monétaire et financier).

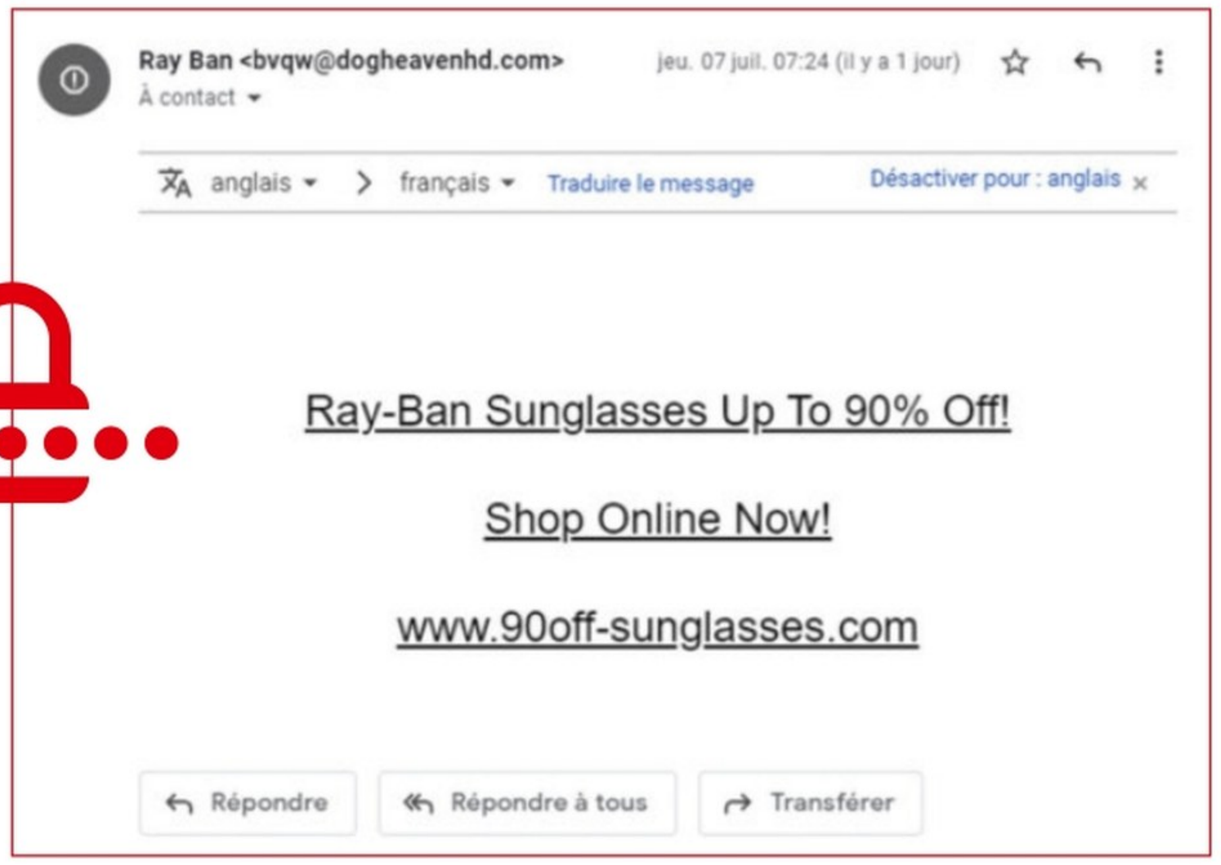
Comment repérer un e-mail de phishing ?

Les e-mails de phishing sont réalisés pour être extrêmement proches des messages dont ils usurpent l'identité, mais il est possible de les repérer grâce à quelques éléments caractéristiques communs malgré le fait que les tentatives d'hameçonnage se présentent sous diverses formes. Ainsi, une liste non exhaustive de ces indicateurs peut être établie. Si vous repérez un ou plusieurs de ces signaux d'alerte, au moindre doute, prenez contact avec l'expéditeur potentiel par une autre voie que la messagerie électronique afin de vérifier qu'il est bien à l'origine du message. Dans le cas contraire, vous pouvez signaler la tentative d'hameçonnage aux autorités compétentes (voir notre encadré : « Signalement en cas de phishing ») et prendre les mesures les plus adéquates pour limiter les problèmes.

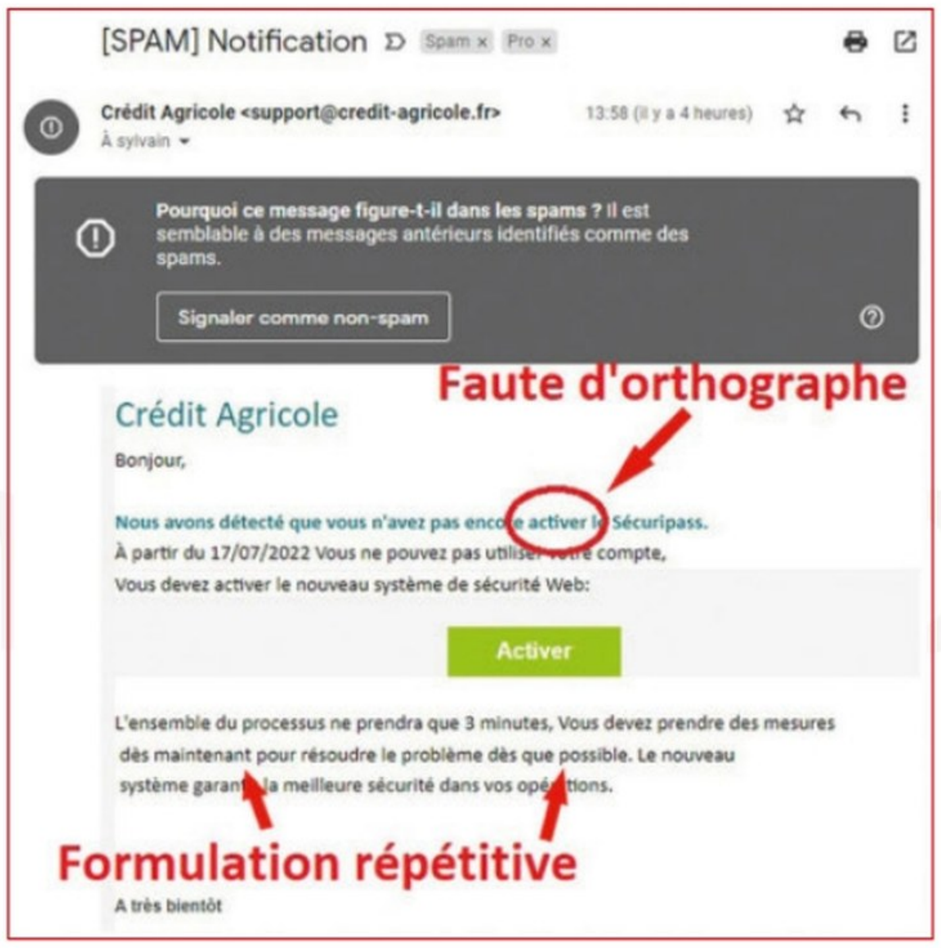
Des signes qui ne trompent pas

En premier lieu, la notification de votre messagerie ou de votre logiciel antivirus peut vous signaler la réception d'un e-mail frauduleux. Parallèlement, assurez-vous que votre solution antivirale est bien à jour. Si ce n'est pas le cas, procédez à son actualisation afin de profiter d'une

protection maximale. Méfiez-vous aussi si vous recevez un e-mail de la part d'une société ou d'un service dont vous n'êtes pas client. En effet, les cybercriminels ne ciblent pas toujours les personnes faisant partie d'une base de données de clients, mais envoient les messages électroniques de phishing au hasard. Dans le même esprit, la réception d'un e-mail inattendu de la part d'un contact, d'une personne ayant une adresse inhabituelle, que vous ne connaissez pas ou qui ne fait pas partie de vos contacts doit vous mettre la puce à l'oreille et vous devez alors faire attention, même si le message peut être potentiellement légitime. Demandez-vous si vous connaissez vraiment l'expéditeur, s'il est possible qu'il

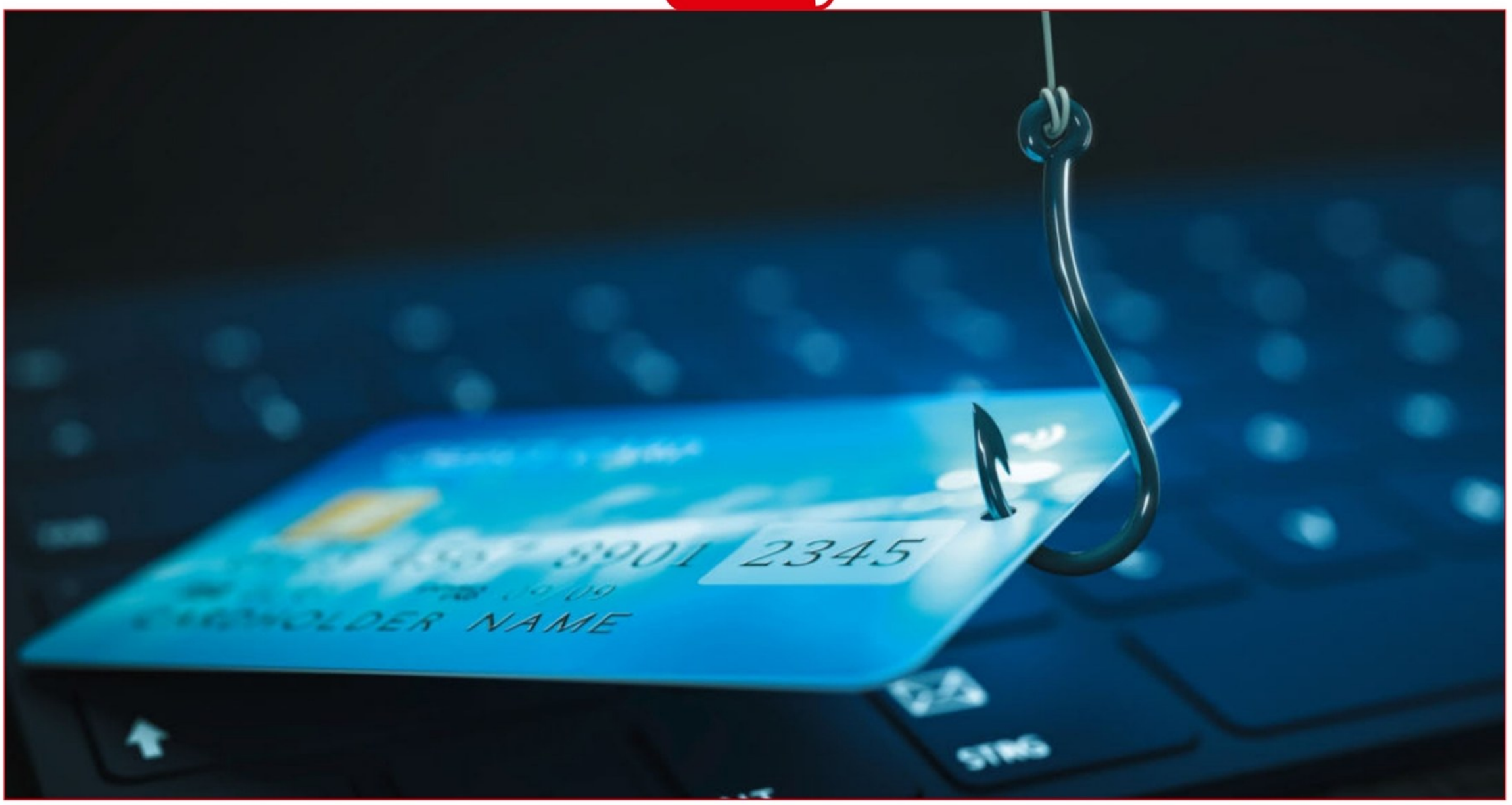


▲ **Vous y croyez, vous, à un site qui propose des lunettes de marques à -90 % ?**



▲ **Même si les mails semblent visuellement provenir d'un organisme officiel, des fautes d'orthographe, des formules étranges ou bien des onglets à cliquer doivent vous alerter…**

vous envoie un message, si le contenu du message vous est réellement destiné, si le sujet qui est abordé vous concerne et s'il est vraiment personnalisé. Toutefois, il faut aussi savoir que connaître l'adresse e-mail de l'expéditeur n'est pas un critère de confiance absolu. En effet, le cybercriminel a très bien pu usurper l'adresse de l'un de vos contacts ou d'un service que vous utilisez. Là aussi, demandez-vous si la demande contenue dans le message est bien habituelle et si vous remarquez des incohérences dans le ton employé par exemple. Restez parfaitement vigilant si le message contient des éléments suspects tels qu'un lien cliquable, vous demande des informations ou qu'une pièce jointe est attachée. De même, si l'adresse e-mail de l'expéditeur semble plutôt fantaisiste, méfiez-vous. Les messages des

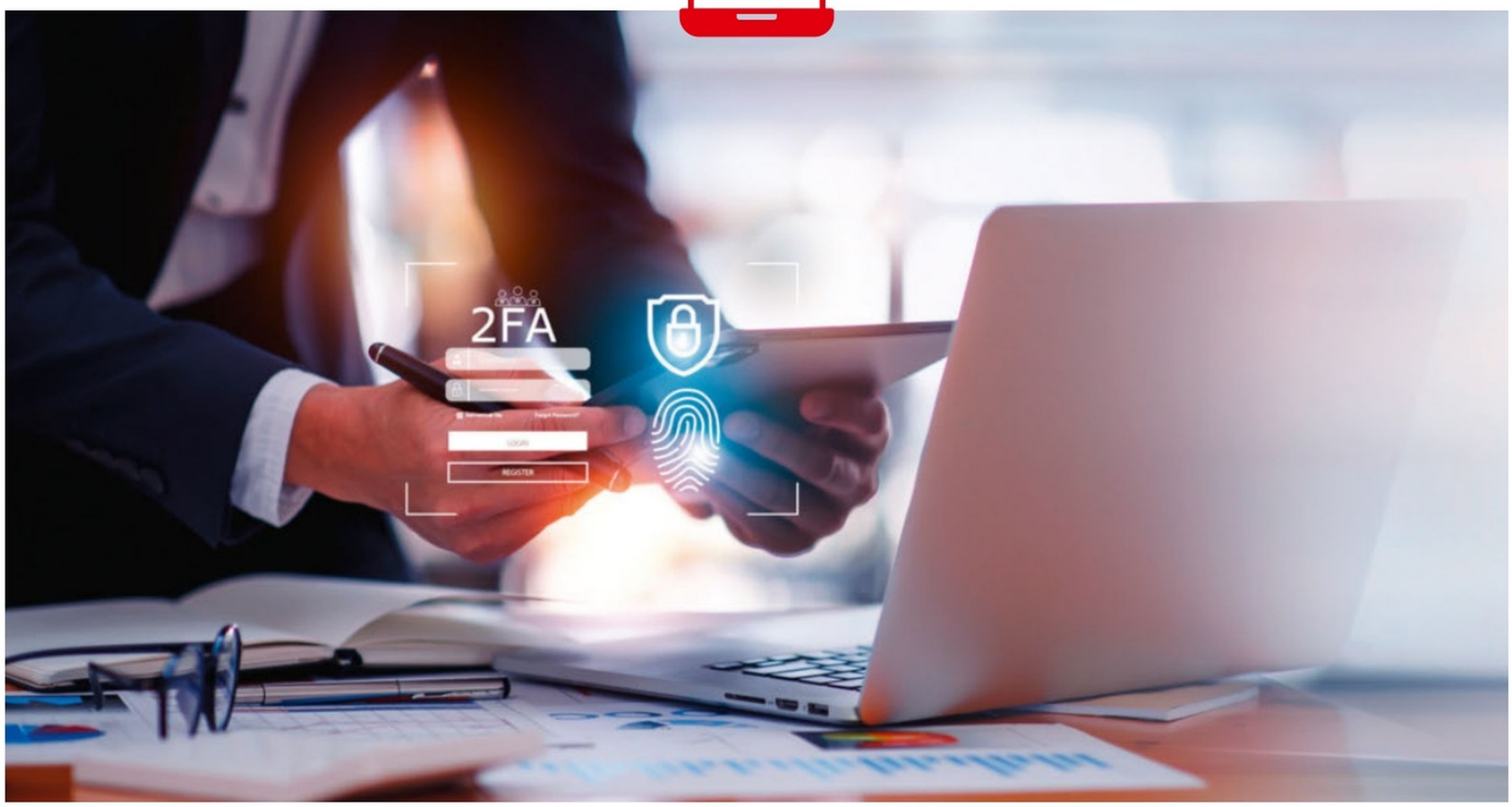


© adobestock.com

organismes portent toujours leur nom comme nom de domaine (après le @). Si l'adresse ne porte pas le nom de l'entité ou qu'elle présente des fautes d'orthographe, il s'agit certainement d'un message frauduleux qu'il ne faut absolument pas ouvrir.
Ce sera aussi très certainement le cas si l'adresse ne se termine pas par un .com, un .fr, voire un .eu si vous êtes en France, par exemple. Certains hameçonnages par messagerie électronique se présentent sous une forme plus ou moins grossière dans leur mise en page avec des images et des logos qui ne sont pas nets ou déformés, car récupérés via des captures d'écran réalisées par les cybercriminels qui ne sont pas reconnus pour leurs qualités de graphistes. En cas de doute, comparez les éléments visuels du potentiel e-mail phishing avec l'un des messages officiels que vous auriez reçus récemment de la part de l'organisme mentionné dans le message. D'autres types de messages doivent également vous alerter dont l'objet serait de vous informer que vous venez de gagner à la loterie, que les impôts vous doivent de l'argent ou qu'il ne vous reste plus que quelques jours pour envoyer certaines informations pour pouvoir récupérer votre gain à un jeu concours (auquel vous n'avez pas participé). En effet, les objets trop alléchants ou, au contraire, trop alarmistes sont suspects. Ils cherchent à inciter la victime à ouvrir le message et à tomber dans le panneau qui libérerait le code malveillant ou enverrait directement certaines informations au cybercriminel.
Faites bien attention aux messages qui ne contiennent aucune personnalisation. En effet, normalement, lorsqu'on cherche à vous écrire, c'est à vous et non à d'autres personnes. D'une façon générale, retenez qu'aucune entité, qu'elle soit gouvernementale ou professionnelle, n'est en droit de vous demander votre code de carte bancaire ou vos codes d'accès personnels par messagerie. Soyez également particulièrement vigilant sur la qualité du texte du message. En effet, les tentatives d'hameçonnage par messagerie électronique comportent la plupart du temps des fautes d'orthographe et/ou de grammaire. Des formules très spéciales ou une syntaxe inhabituelle doivent également vous alerter, car il peut s'agir d'une traduction plus ou moins heureuse d'un message rédigé à la base dans une autre langue et traduit automatiquement par des logiciels.

Comment se protéger, les bons réflexes à avoir

Si vous suivez nos conseils sur les signaux qui ne trompent pas, vous devriez être relativement à l'abri des hameçonnages, mais le risque zéro n'existant pas, il faut également prendre en compte plusieurs réflexes.
Le premier et le plus important de tous est le fait qu'il ne faut jamais communiquer d'informations sensibles par messagerie électronique ou par téléphone. En effet, aucune administration ou société privée sérieuse ne vous demandera vos données bancaires, vos identifiants ou vos mots de passe par l'un de ces canaux.
Si vous repérez un lien cliquable (dans une autre couleur que le texte principal et souligné), approchez le curseur de votre souris, mais sans cliquer avec le bouton de celle-ci. Cette astuce permet de voir le lien réel qui doit s'afficher en bas de la fenêtre de votre messagerie électronique : si l'adresse ne commence pas par le nom de l'organisme ou de la société mentionné dans le message, ne cliquez surtout pas dessus. Systématiquement, lorsque vous souhaitez vous rendre sur le site de cette



© adobestock.com

© adobestock.com

administration ou de l'entreprise, tapez son nom dans un moteur de recherche ou utilisez le raccourci que vous avez précédemment créé.

Si vous pensez avoir remarqué un signal d'alerte, en cas de doute, essayez d'entrer directement en contact avec l'entité qui semble vouloir correspondre avec vous. Cela vous permettra de vérifier qu'elle cherche bien à vous joindre. D'une façon générale, lors de l'inscription à un service ou de la souscription à un abonnement, utilisez des mots de passe complexes et différents pour chacun des sites et applications fréquentés. Cela peut vous éviter de vous faire voler vos identifiants et limite les possibilités de compromission de vos comptes. Utilisez un logiciel de gestionnaire de mots de passe comme Dashlane, LastPass, Keeper, NordPass, 1Password, voire celui des navigateurs Internet ou de Google.

Certains sites permettent de consulter les activités que vous y avez pratiquées. Regardez dans l'historique si vous ne constatez pas d'accès inhabituels que vous n'auriez pas pu faire. Si des accès illégitimes ont été réalisés, changez immédiatement votre mot de passe correspondant. Certains services permettent d'activer la fonction de double authentification. Si tel est le cas, nous vous conseillons vivement d'y souscrire.

Les ransomwares, des phishing à part

Avant 2018, on peut dire que les attaques par ransomwares ciblaient principalement les particuliers, mais depuis, les organisations aux moyens plus importants se trouvent également être de plus en plus attaquées. Dans son rapport de 2020, le service cybermalveillance.gouv.fr expliquait que les attaques par rançongiciels avaient pris une ampleur considérable en 2020, devenant la principale menace à laquelle les professionnels ont été confrontés cette année-là aussi bien dans le secteur privé que dans le public. A contrario, ce type d'attaque a peu touché les particuliers en 2020 avec moins de 1 % des recherches d'assistance. En 2021, cette tendance s'est encore plus renforcée. Une attaque par ransomware ou rançongiciel consiste à mettre l'ordinateur hors d'état de fonctionner de manière irréversible ou d'empêcher l'accès à certains fichiers enregistrés dans la machine. Le cybercriminel adresse alors un message à sa victime pour lui proposer de débloquer les données ou l'appareil attaqué contre le paiement d'une rançon. Il peut aussi arriver que la personne malveillante menace de rendre publiques les données dérobées. La plupart du temps, elle demande l'utilisation de cryptomonnaie (Bitcoin, Ethereum, etc.) pour le paiement afin qu'elle puisse garantir son anonymat et compliquer la tâche des autorités à la retrouver. Malheureusement, le versement de la rançon demandée ne garantit en rien la récupération des données ou la non-publication des photos ou

LES ENTITÉS SUSCEPTIBLES DE VOIR LEUR IDENTITÉ USURPÉE

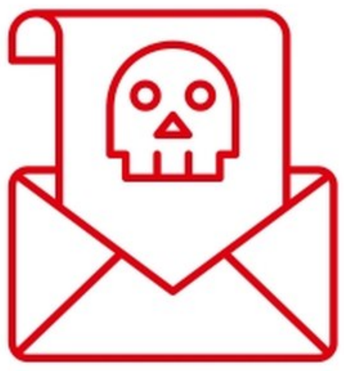
L'hameçonnage a pour principe de base l'usurpation d'identité et les cybercriminels n'hésitent pas à utiliser celle d'organismes connus dans leurs messages frauduleux dont voici les principaux : le **Trésor public** (les impôts), la **Caisse d'assistance familiale** (caf), la **Sécurité sociale** (ameli), les **banques**, les opérateurs **télécoms**, les fournisseurs d'**énergie**, les **réseaux sociaux**, les sites d'**e-commerce**, les sociétés de **livraison** ou encore les systèmes de **paiement en ligne**.

vidéos sensibles. Pire, cela peut même encourager les cybercriminels à demander plus vu qu'un premier paiement a été réalisé. Le paiement des rançons est toujours vivement déconseillé.

Comment réagir et quoi faire en cas d'attaque ?

Si vous avez reçu un spam ou si le message apparaît comme une tentative de phishing, voire d'attaque par ransomware, ne répondez surtout pas et n'ouvrez pas les pièces jointes, les images ou les liens intégrés.

- Signalez-le sur la plateforme **www.signal-spam.fr**. Cela permettra à la **CNIL** (Commission Nationale de l'Informatique et des Libertés) de déclencher une enquête pour tenter de sanctionner les spammeurs et auteurs de ces attaques.
- Plus généralement, vous pouvez également utiliser la plateforme **PHAROS** (Plateforme d'Harmonisation d'Analyse, de Recoupement et d'Orientation des Signalements) accessible à l'adresse **https://www.internet-signalement.gouv.fr/PharosS1/**. Une enquête pénale peut être ouverte, sous l'autorité du procureur de la République. PHAROS reçoit chaque année plusieurs dizaines de milliers de signalements.
- Le site **https://phishing-initiative.fr/** permet également de vérifier ou de signaler un site.
- Sinon, vous pouvez aussi utiliser le numéro de téléphone du service I**nfo Escroqueries** au 0 805 805 817 (appel gratuit).
- Au-delà des signalements, pensez également à changer vos mots de passe afin de limiter la portée de l'attaque si celle-ci a pu aboutir.
- Le site **cybermalveillance.gouv.fr** est aussi un dispositif national d'assistance aux victimes d'actes de malveillance numérique, mais regroupe également de nombreuses informations et permet de se sensibiliser aux risques numériques proposant aussi un observatoire de la menace en France. ■



CAS D'ÉTUDE : KASPERSKY TESTE LES EMPLOYÉS DE PLUSIEURS SOCIÉTÉS

Afin de sensibiliser les administrateurs des réseaux d'entreprise, mais également les utilisateurs, la société Kaspersky a analysé les données d'un simulateur de phishing. L'étude montre clairement que les employés ont tendance à ne pas remarquer les pièges dans les e-mails puisque près d'un salarié sur 5 a cliqué sur le lien figurant dans les modèles de messages électroniques imitant des attaques de type phishing. L'outil permet ainsi d'aider les entreprises à vérifier que leurs employés peuvent distinguer un e-mail de phishing d'un message authentique pour ne pas faire courir de risque aux données des sociétés. Un modèle est ainsi créé par l'administrateur qui l'envoie aux collaborateurs sans les avertir et suit les résultats.

Selon de récentes campagnes de simulation de phishing, les 5 types d'emails de phishing les plus efficaces sont :

- Objet : Erreur de tentative d'envoi – malheureusement, notre coursier n'a pas pu livrer votre article. Expéditeur : Service de livraison de colis. >>> **Taux de conversion de clics : 18,5 %**
- Objet : Emails non transmis pour cause de serveurs mails surchargés. Expéditeur : L'équipe support de Google. >>> **Taux de conversion de clics : 18 %**
- Enquête en ligne auprès des employés : ce que vous aimeriez améliorer au sein de l'entreprise. Expéditeur : département RH. >>> **Taux de conversion de clics : 18 %**
- Objet : Rappel : nouveau dress-code interne. Expéditeur : ressources humaines. >>> **Taux de conversions de clics : 17,5 %**

- Objet : Attention à tous les salariés : nouveau plan d'évacuation du bâtiment. Expéditeur : département sécurité. >>> **Taux de conversion de clics : 16 %**

Parmi les autres emails ayant engendré un fort taux de clics, on retrouve : des confirmations envoyées de la part de services de réservation (11 %), une notification à propos d'une commande (11 %) et une annonce de jeu concours IKEA (10 %). En revanche, les courriels qui menacent le destinataire ou offrent des avantages immédiats semblent avoir moins de « succès ». Un modèle ayant pour objet « J'ai piraté votre ordinateur et je connais votre historique de recherche » a obtenu 2 % de clics, tandis que les offres pour obtenir Netflix gratuitement et pour obtenir 1 000 dollars en cliquant sur un lien n'ont trompé que 1 % des employés. *Source : Kaspersky Security Awareness Plateform*