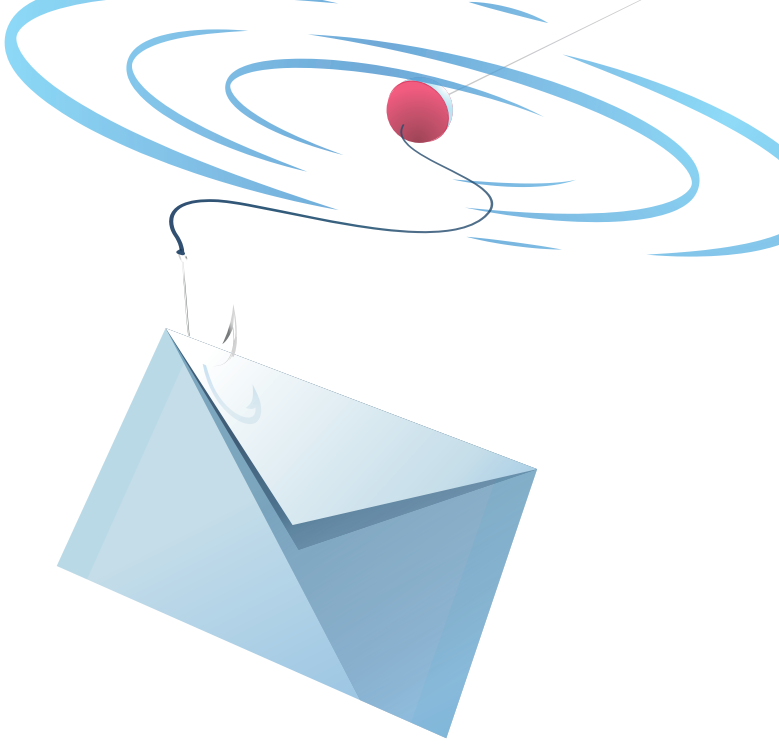
SOPHOS



Ne mordez pas à l'hameçon.

Le phishing est un business très lucratif. Restez sur vos gardes.

Les attaques de phishing connaissent depuis quelque temps un essor fulgurant, les attaquants affinant sans cesse leurs tactiques et se repassant les méthodes qui se sont révélées fructueuses. Ils ont en particulier tiré profit des malwares en tant que service (MaaS) disponibles sur le Dark Web pour augmenter l'efficacité et le volume de leurs attaques. Et les effets se font sentir : 41 % des informaticiens affirment recevoir au moins une attaque de phishing par jour.[1]

Dans ce livre blanc, nous examinerons l'évolution des attaques de phishing au cours des dernières années, ainsi que leur fonctionnement et leur apparence. Et comme les cybercriminels ciblent en priorité les employés, nous démontrerons toute l'importance de mettre en place une protection multicouche contre ces attaques, par le biais de technologies de sécurité avancées associées à la formation et à la sensibilisation des utilisateurs.

Bien plus que du spam

Traditionnellement, le phishing est associé aux fraudes touchant les services bancaires en ligne : les escrocs vous envoient un email vous demandant de vous connecter au site Web de votre banque via un lien qui vous amène en réalité vers un clone visuel de la page de connexion. De cette manière, vous envoyez vos identifiants directement dans les mains des criminels.

Mais le phishing ne se limite pas aux faux sites bancaires, aux liens vers des pilules miracles ou encore aux fausses notifications de livraisons. C'est un appât suspendu en permanence devant vous qui attend d'être avalé, révélant ainsi aux cyber criminels de précieuses informations.

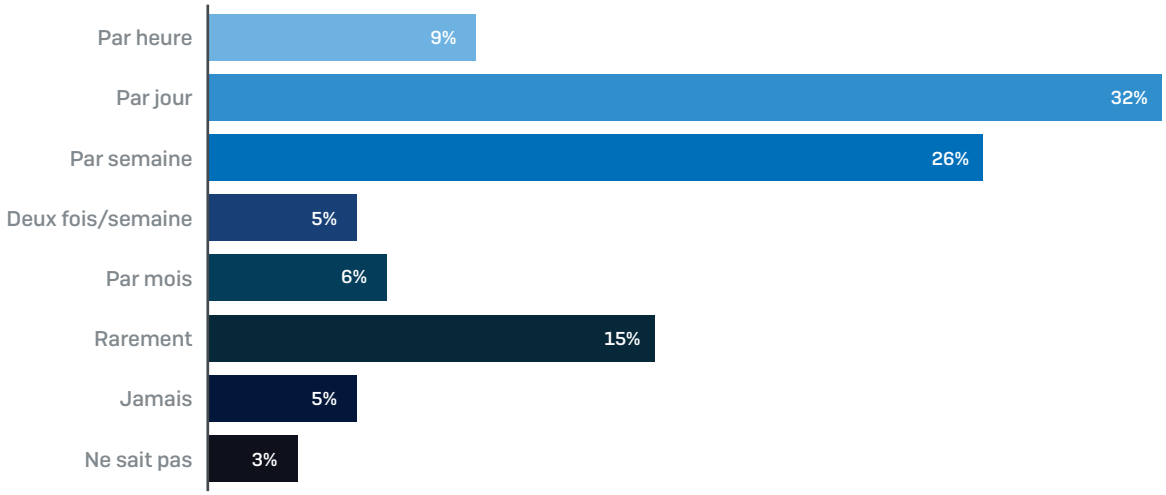
93%
des violations de données impliquent le phishing[2]

Le phishing est un business très lucratif

Ces dernières années, le volume des attaques de phishing a considérablement augmenté, alimenté par des services disponibles sur le Dark Web, comme les kits de phishing gratuits et le phishing-as-a-service. Il est aujourd'hui très simple, même pour des pirates novices, d'exploiter des malwares avancés qui ont été créés par des auteurs bien plus experts en la matière.

Et c'est pourquoi les attaques de phishing font désormais partie intégrante de notre quotidien. 41 % des professionnels de l'informatique ont signalé que leur société a fait l'objet d'au moins une attaque de phishing par jour, tandis que plus des 3/4 (77 %) en ont reçu au moins une fois par mois.[3]

Fréquence des attaques de phishing

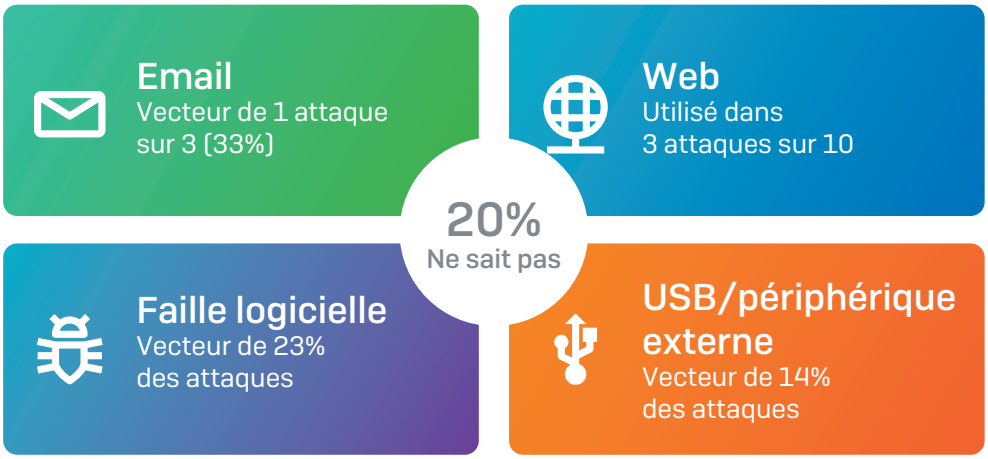


Le vecteur d'attaque le plus courant

Une récente enquête réalisée auprès de 3 100 entreprises dans le monde a révélé que l'email est le vecteur d'attaque le plus courant, utilisé dans 33 % des cyberattaques fructueuses. C'est également un vecteur extrêmement efficace : 53 % des entreprises touchées par une cyberattaque l'année dernière déclarent avoir reçu des emails de phishing.[4]

1/3
Les emails sont le vecteur de 1 cyberattaque sur 3

Les emails de phishing sont souvent la première étape d'une attaque complexe aux techniques variées. Par exemple, cliquer sur un lien dans un email de phishing vous connecte à un serveur C&C (Command & Control), qui va ensuite infecter l'entreprise à l'aide d'un logiciel malveillant.

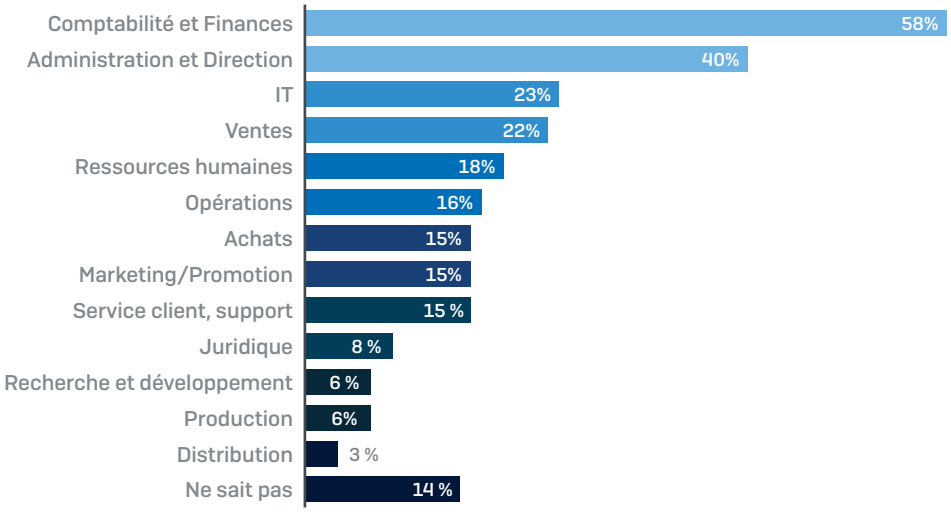


La principale motivation derrière une attaque de phishing est le gain financier. Le rapport « 2018 Data Breach Investigations Report » de Verizon a révélé que :

- **59 % des attaques sont motivées par le gain financier.** Par exemple pour collecter des identifiants afin de les revendre sur le Dark Web, infecter des systèmes avec un ransomware ou usurper l'identité d'un cadre d'une société pour convaincre les employés de transférer de l'argent ou des données sensibles.
- **41 % des attaques avaient pour but d'obtenir un accès non autorisé au système.** Par exemple pour obtenir l'accès au réseau d'une entreprise afin de voler des données ou d'obtenir le contrôle des systèmes.

L'appât du gain étant le principal moteur des attaques, il n'est pas surprenant que les cybercriminels ciblent souvent les employés à des postes clés qui ont accès aux informations financières de l'entreprise, afin de les inciter à effectuer des transferts d'argent vers des comptes bancaires en leur contrôle. Cependant, ils ciblent également les personnes en charge des processus d'exploitation de l'entreprise et des contrôles informatiques, pour lancer toutes sortes d'attaques, comme des ransomwares, et extorquer de l'argent.[5]

Les services les plus ciblés par les attaques de phishing



Il n'est pas surprenant que le phishing soit considéré comme le risque le plus significatif par les responsables informatiques, dont 50 % le placent parmi les trois plus grands risques. Puis en deuxième position apparait le facteur humain, c'est-à-dire le personnel de l'entreprise, les contractuels et les visiteurs. En effet, les cybercriminels exploitent de plus en plus les faiblesses et les comportements humains dans leurs attaques.

% les classant dans leur top 3

Améliorer l'efficacité et la productivité

Actuellement, 89 % des attaques de phishing sont le fruit du crime organisé. Le phishing est aujourd'hui géré comme une entreprise et les stratégies d'attaque ont évolué d'une manière qui nous parle à tous :

89%
des attaques de phishing sont orchestrées par le crime organisé

Comment faciliter mon travail et le rendre plus efficace, et comment me développer pour gagner plus d'argent ?

Cette évolution a débouché sur des méthodes de distribution des attaques plus efficaces, avec des services de phishing à la demande, des kits en libre-service et de nouvelles vagues de types d'attaques telles que le Business Email Compromise (BEC) qui visent des ressources de plus grande valeur à l'aide d'ingénierie sociale.

Kits de phishing gratuits

Avez-vous déjà rêvé que vos produits s'arrachent comme le dernier iPhone ? Pour nombre d'entre nous, si nous voyons une idée qui marche bien (venant d'un ami, collègue ou concurrent) nous sommes tentés de « l'emprunter » pour nous-mêmes, n'est-ce pas ? Et bien la communauté du phishing n'est pas différente. En fait, elle est encore mieux organisée.

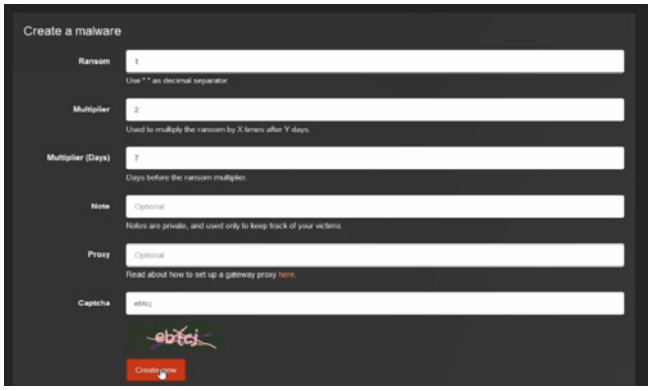
Un aspect intéressant de l'écosystème du phishing est qu'il existe un très grand nombre d'acteurs qui réalisent des attaques, mais seul un petit nombre de « phishers » sont capables de créer un kit de phishing à partir de zéro. On peut aujourd'hui aisément télécharger un kit de phishing sur les forums et les marketplaces du Dark Web. Les hackers ont ainsi tous les outils dont ils ont besoin pour créer des attaques de phishing fructueuses : emails, code de page Web, images, etc.

Les auteurs des kits cherchent à accroitre leurs profits en distribuant ces kits à des utilisateurs moins sophistiqués. Deux choix s'offrent à eux : offrir des kits gratuits contenant une porte dérobée ou « backdoor » par laquelle ils pourront utiliser les données volées par l'utilisateur ou bien directement vendre leurs kits pour réaliser un profit. Les kits les plus chers incluent désormais des fonctionnalités telles que des tableaux de bord pour suivre la campagne de phishing.

Attaques-as-a-service

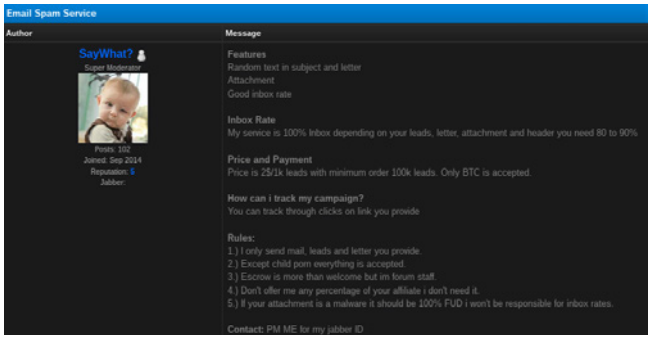
En fait, les attaquants n'ont même plus besoin de savoir comment créer un malware ou d'envoyer des emails. Des solutions as-a-service (à l'acte) et pay-as-you-go (à l'utilisation) sont proposées par la plupart des technologies de services en ligne, et le phishing ne déroge pas à la règle. Les pirates disposent ainsi de toujours plus de services.

- **Le ransomware-as-a-service** permet à un utilisateur de créer un compte en ligne, il ne lui reste plus qu'à renseigner un prix de départ de la rançon et un prix comprenant des pénalités de retard. Le fournisseur du service prélève un pourcentage sur chaque rançon payée. Il peut parfois offrir une réduction si l'utilisateur est capable de traduire le code du malware dans une autre langue ou si le volume d'attaques dépasse un certain seuil.



Le ransomware Satan : un service en ligne permettant aux escrocs de créer leur propre virus en quelques minutes et de commencer à infecter des systèmes Windows.

- **Le phishing-as-a-service** permet aux utilisateurs de payer pour des attaques qui seront réalisées pour eux, à l'aide de botnets internationaux afin d'éviter d'utiliser des domaines IP malveillants connus. Il est même proposé de ne facturer que les emails dûment délivrés, comme c'est le cas pour n'importe quel service légitime de campagne d'emailing.



Exemple de service de spam : tarifé par email envoyé vers une boîte mail active, avec suivi du taux de clics.

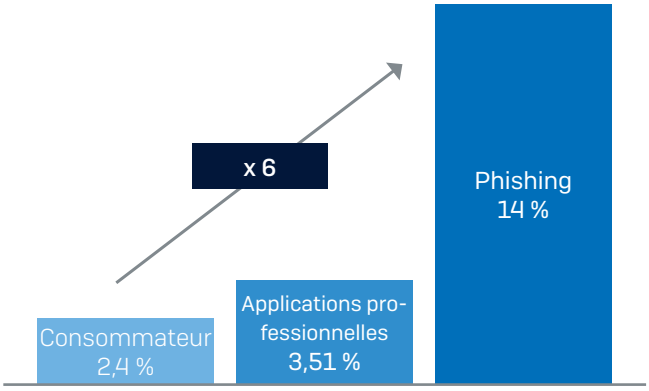
Ces services permettent aux attaquants même les moins avertis de se lancer dans le business du phishing, entraînant une explosion de ces types d'attaques.

Comme le marketing, mais 6 fois mieux

Plus inquiétant encore, ces services du Dark Web ont dégagé du temps aux attaquants qui peuvent désormais se concentrer sur l'amélioration de leurs campagnes et sur le peaufinage de leurs techniques.

Et leurs tactiques leur permettent d'obtenir des résultats qui feraient pâlir d'envie la plupart des équipes de vente et de marketing : les emails de phishing sont 6 fois plus susceptibles d'être cliqués que les emails de marketing ordinaires.[6]

Taux de clics des emails de phishing



Tout ce temps maintenant consacré à la recherche et au développement a fait grimper d'un cran les menaces de phishing. Les attaques BEC (Business Email Compromise), un sous-ensemble dangereux d'attaques de phishing qui permettent aux attaquants d'accroitre leurs profits en ciblant les personnes les plus importantes des entreprises, se multiplient.

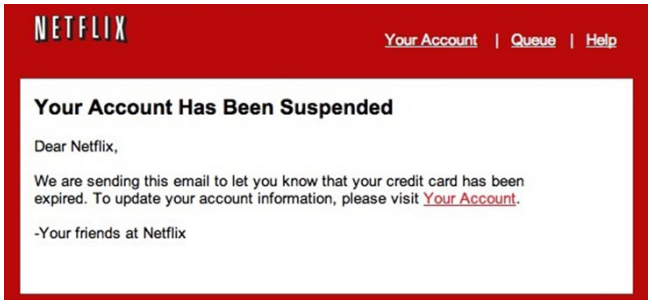
Le fonctionnement du phishing

Comme nous l'avons vu plus haut, le phishing recouvre bien plus que des emails contrefaits de banques en ligne ou de notification de livraison de colis. Leur objectif principal est de vous convaincre de fournir quelque chose de valeur. Et ce qui était au départ du simple « phishing » s'est transformé en trois familles d'attaques : les classiques, le phishing de masse + spear phishing et le Business Email Compromise, une sous-spécialité du spear phishing.

Phishing de masse

Ces attaques sont essentiellement opportunistes. Elles exploitent le nom de marque d'une société pour tenter d'attirer leurs clients vers des sites Web usurpés où ils seront piégés. Les attaquants récupèrent alors les informations de carte bancaire, les identifiants de connexion et d'autres informations personnelles qui seront ensuite revendues.

- Cible les actifs des personnes
- Généralement les clients des produits ou des services d'une marque
- Envoi de masse d'emails impersonnels
- Axé sur le vol de données personnelles, telles que les identifiants de connexion.

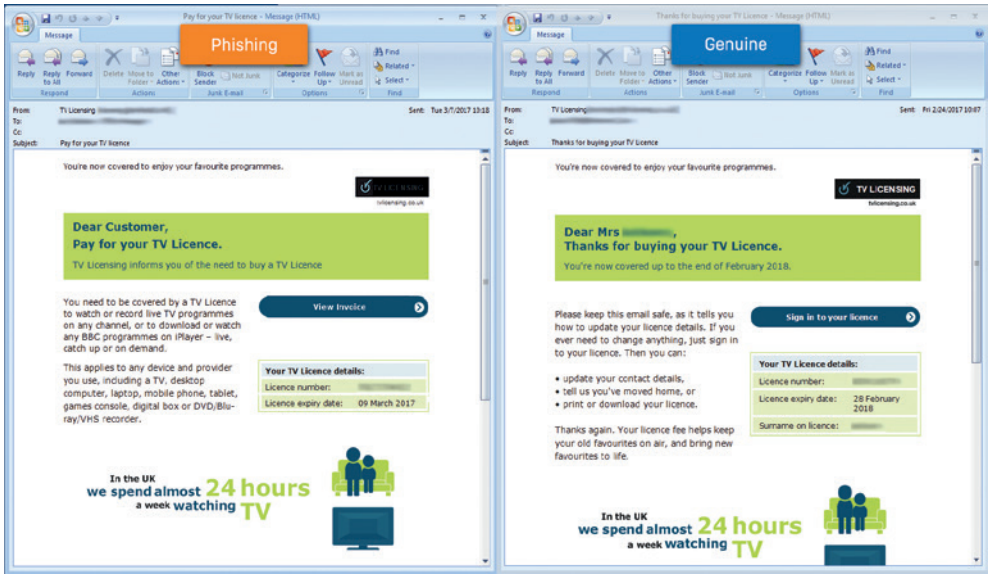


Un exemple typique de phishing de masse « Vérifier votre compte »

Spear phishing

L'autre type de menace est le spear phishing. Il s'agit d'emails usurpant l'identité d'un expéditeur spécifique ou d'une source fiable qui sont envoyés aux employés d'une entreprise pour tenter de les amener à faire certaines choses, comme envoyer de l'argent vers des comptes fallacieux.

- Cible les actifs d'une entreprise particulière
- Généralement un individu ou un groupe spécifique dans une entreprise
- Adresses email usurpant l'identité (« sosie ») pour augmenter leurs chances de réussite.
- Se fait passer pour une source fiable ou un cadre de l'entreprise



Les emails authentiques et les emails de phishing se ressemblent souvent, comme le montre cet exemple d'emails pour la redevance audiovisuelle au Royaume-Uni.

Les attaques de spear phishing sont de plus en plus fréquentes et les cybercriminels continuent d'affiner leurs techniques afin d'accroitre leur efficacité. Dans une enquête récente menée auprès de 330 professionnels de l'informatique, 55 % d'entre eux ont confirmé que l'identité de leur directeur avait été usurpée dans des attaques de spear phishing.[7]

Des sous-catégories de spear phishing plus ciblé utilisent l'ingénierie sociale pour obtenir des informations sur les personnes ciblées afin d'augmenter leurs chances de réussite. On les appelle la « fraude au Président », le whaling, et plus récemment le Business Email Compromise (BEC).

Business Email Compromise (BEC)

140k$
Pertes moyennes par fraude

Les attaques Business Email Compromise (BEC) sont ainsi nommées, car ici les comptes de messagerie des employés ont été compromis et non pas seulement parodiés. De cette manière, les attaques sont plus difficilement repérées par les utilisateurs.

- Cible les données professionnelles, les identifiants de connexion ou les fonds de l'entreprise
- Après avoir choisi une entreprise cible, les attaquants identifient des personnes à attaquer au sein de cette entreprise. Pour cela, ils vont chercher des informations sur des sites tels que Facebook ou LinkedIn afin d'élaborer des emails de phishing hautement ciblés et crédibles.
- L'attaquant isole ensuite une personne en lui faisant croire qu'un email provient d'un de ses supérieurs en lui mettant la pression pour agir le plus rapidement possible, par exemple en envoyant l'email en fin de journée ou de semaine.

Contrairement aux campagnes de phishing de masse ou de spear phishing, ces attaques ciblent généralement les fonds de l'entreprise. Et contrairement aux anciennes méthodes qui consistaient à joindre un PDF contenant les coordonnées du compte bancaire de destination, les attaques BEC n'envoient ce document que si la victime tombe dans le panneau. Le compte bancaire frauduleux est un atout important que l'attaquant doit protéger, car si la victime réalise immédiatement la supercherie elle pourrait transmettre l'information aux autorités.

Les attaques BEC sont plus difficiles à identifier, car les attaquants envoient leurs emails depuis des comptes de messagerie professionnelle compromis. Selon les derniers chiffres du FBI, un nombre impressionnant d'entreprises se font avoir régulièrement par ce genre d'attaques : rien qu'en 2016, les pertes atteignaient 3,1 milliards de dollars pour un ensemble de 22 000 entreprises.

L'évolution des techniques de phishing

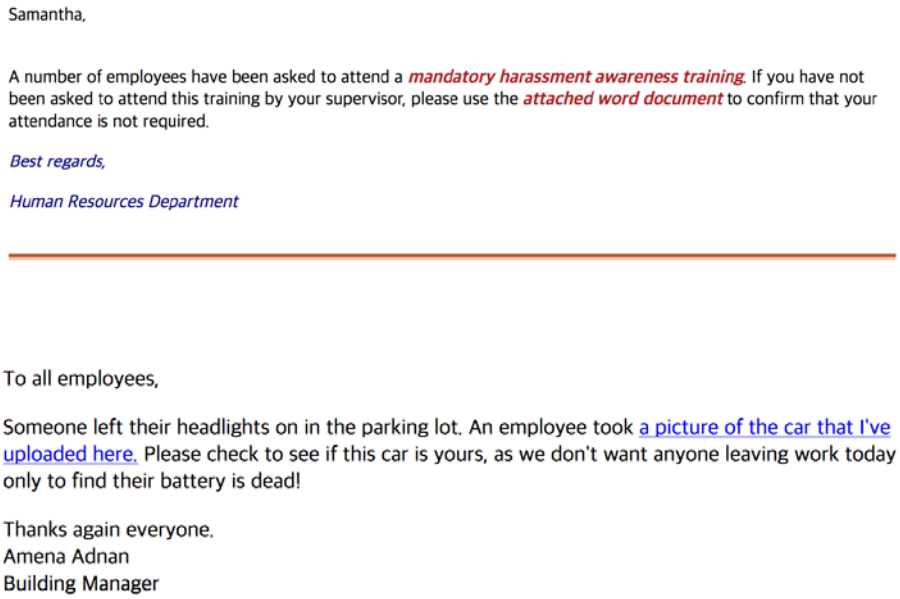
Les techniques de phishing continuent d'évoluer. Comme les personnes se méfient désormais des emails « trop beaux pour être vrais » offrant de superbes prix, les escrocs se tournent vers des emails simples et ordinaires qui ne seront pas suspectés immédiatement.

Le tableau ci-dessous montre les 10 principaux emails ayant piégé les employés lors d'une simulation d'emails de phishing envoyée par Sophos Phish Threat. Comme vous pouvez le voir, l'objet des emails est assez « normal », avec des sujets qui ne sont pas particulièrement suspects.

OBJET DE L'EMAIL	% D'EMAILS OUVERTS ET DE CLICS
[Jira] Une tâche vous a été assignée	39%
Réunion la semaine prochaine	29%
Formation de sensibilisation au harcèlement	26%
Phares laissés allumés	25%
Message eFax de la part de {Nom Client} — 2 page(s)	24%
Avis de passage pour {Prénom} {Nom}	22%
Facture de télépéage	21%
Présence d'un homme suspect autour des bureaux de {Nom Client}	20%
À LIRE - sondage annuel des employés	19%
Nouveau système de messagerie chez {Nom du client} -- à lire attentivement	18%

L'email le plus efficace fait référence à JIRA, un outil populaire de suivi de projets, suivi de près par une demande de réunion ou de formation interne au harcèlement, tous conçus pour nous faire « stresser » et oublier toute bonne pratique de vérification !

Et il ne s'agit ici que de quelques exemples d'emails de phishing qui montrent la simplicité, mais aussi l'efficacité d'emails ordinaires.



Samantha,

A number of employees have been asked to attend a *mandatory harassment awareness training*. If you have not been asked to attend this training by your supervisor, please use the *attached word document* to confirm that your attendance is not required.

Best regards,

Human Resources Department

To all employees,

Someone left their headlights on in the parking lot. An employee took a picture of the car that I've uploaded here. Please check to see if this car is yours, as we don't want anyone leaving work today only to find their battery is dead!

Thanks again everyone.
Amena Adnan
Building Manager

Identifiez les signes

Ces fausses factures qu'on vous envoie en vous disant que quelqu'un a acheté un billet d'avion avec votre carte de crédit et vous demande d'ouvrir la pièce jointe pour contester le paiement ? Du phishing de masse.

30%
des emails de phishing sont ouverts

De même que ces fausses notifications de coursier vous demandant de confirmer l'adresse de votre entreprise pour vous livrer un colis.

Le spear phishing, pour la majeure partie, est à peu près similaire, sauf que l'appât est plus spécifique. Ou, dans le cas des attaques BEC, le message ne contient pas de pièce jointe ni de lien malveillant, mais va plutôt vous demander de transférer de l'argent, rendant l'attaque plus crédible.

En résumé, si un email frauduleux commence par « Cher client », c'est du phishing. Mais s'il vous salue par votre nom, c'est du spear phishing. Et s'il provient de l'adresse email de votre patron, c'est une attaque BEC.

Bien sûr, de nombreuses attaques de spear phishing sont beaucoup plus pointues que ça - sans vouloir faire de mauvais jeu de mots. Les escrocs bien préparés connaitront votre fonction, votre numéro de ligne directe, la boulangerie où vous vous rendez parfois le midi, vos amis, le nom de votre patron, le nom de votre ancien patron, et même la marque de café que votre entreprise achète.

Et, comme vous pouvez probablement imaginer, quand il s'agit de spear phishing, rien n'attire le succès comme le succès lui-même. Plus les escrocs, cyber gangs ou hackers d'États en apprennent sur votre entreprise, plus leurs tentatives de phishing seront crédibles.

Ces informations peuvent être obtenues de plusieurs manières :

- Attaque antérieure fructueuse, telle qu'un malware ayant volé des données
- Documents privés de l'entreprise, tels que les annuaires téléphoniques ou les organigrammes, qui apparaissent dans les moteurs de recherche
- Les réseaux sociaux de votre entreprise et vos pages personnelles
- Ancien employé mécontent
- Données achetées à d'autres escrocs sur le Dark Web

Il existe encore bien d'autres moyens d'obtenir des informations censées rester « secrètes ». Si vous comprenez comment ces tactiques fonctionnent, vous diminuez de 30 % l'ouverture des emails de phishing chaque jour.

Utilisez ce moyen mnémotechnique pour aider vos utilisateurs à identifier les signes révélateurs d'un email de phishing :

P : Promesses qui semblent trop belles pour être vraies

H : Harcèle pour que vous répondiez

I : Insiste pour que vous agissiez maintenant

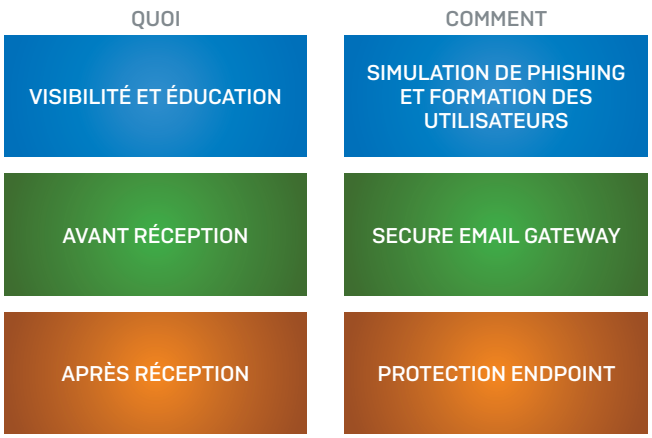
S : Sentiment d'urgence

H : Halte ! Supprimez l'email

En cas de doute, signalez-le à votre équipe informatique et supprimez l'email. Tout le monde s'en portera mieux dans votre entreprise.

La lutte contre le phishing

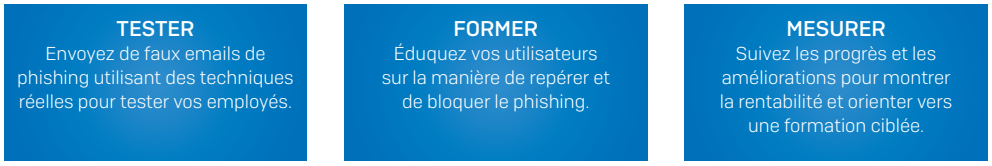
Les attaques de phishing sont extrêmement variées, et il n'existe malheureusement pas de solution miracle pour les stopper. Une défense multicouche contre les attaques de phishing associant des technologies avancées de sécurité et l'éducation des employés est la seule solution. Chez Sophos, nous recommandons à toutes les entreprises d'adopter une approche en trois axes :



1. Visibilité et éducation

Dans la lutte contre le phishing, vos utilisateurs sont le maillon faible. En effet, il suffit en moyenne de 16 minutes pour qu'une personne clique sur un email de phishing [Source : Verizon 2018 Data Breach Investigation Report].

- Vos utilisateurs sont en première ligne des attaques de phishing, c'est pourquoi il est vital que vous les sensibilisiez au problème et les formiez à reconnaitre, et à éviter, les emails de phishing. Un programme efficace de **simulation de phishing et de formation des utilisateurs** doit contenir trois étapes :



2. Avant réception

58 % des emails sont du spam et 77 % des emails de spam contiennent un fichier malveillant[6]. Il est donc vital d'installer une **passerelle de messagerie sécurisée** pour bloquer les emails de phishing avant même qu'ils n'atteignent votre boîte de réception. Les technologies clés à installer :

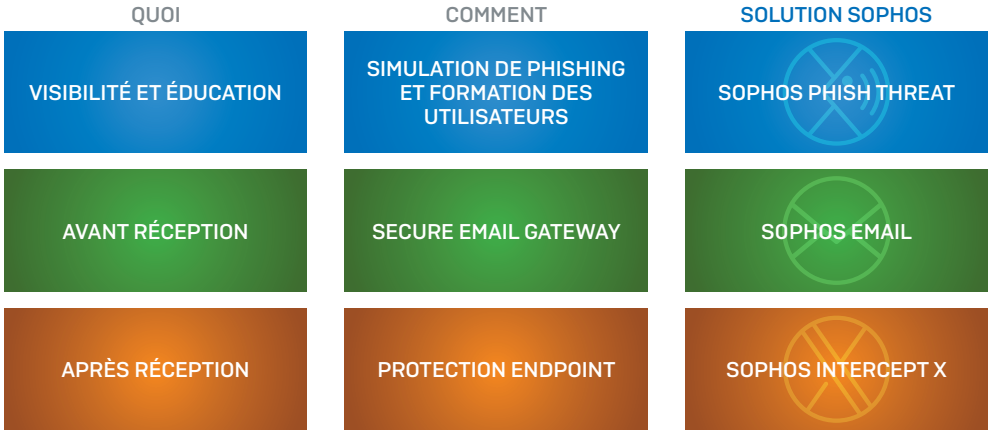
- **Anti-spam :** Des pièges à spam puissants installés dans le monde entier empêchent les emails d'atteindre vos utilisateurs.
- **Réputation de l'expéditeur :** Le filtrage des IP selon leur réputation bloque les emails indésirables au niveau de la passerelle.
- **Authentification de l'expéditeur :** Détectez l'usurpation d'identité de l'expéditeur, les anomalies d'en-tête et le contenu suspect du corps du message.
- **Sandboxing :** Exécutez les fichiers suspects en-dehors de votre réseau.
- **Blocage des URL malveillantes :** Filtrez les liens frauduleux, y compris les attaques furtives et à retardement.

3. Après réception

- La protection après réception est votre dernière ligne de défense. Elle protège votre entreprise si un utilisateur clique sur un lien malveillant ou ouvre une pièce jointe infectée. Installez une solution de **sécurité Endpoint** qui offre des techniques fondamentales et modernes, notamment :
- **Deep Learning :** Empêche les menaces inédites de s'exécuter au sein de votre infrastructure.
- **Anti-exploit :** Empêche les attaquants d'exploiter les failles des logiciels légitimes.
- **Anti-ransomware :** Bloque le chiffrement non autorisé des ressources de votre entreprise.

Sophos peut vous aider

Sophos est le seul éditeur à offrir une protection complète contre le phishing (visibilité et éducation, avant réception et après réception), le tout depuis une seule plateforme Web.



31%
de réduction du risque avec Sophos Phish Threat

Sophos Phish Threat teste et éduque vos utilisateurs à la sécurité à l'aide de simulations d'attaques automatisées, de formations de qualité et de rapports exploitables. Et cela fonctionne : En moyenne, les clients constatent que leurs employés sont 31 % moins susceptibles de se faire piéger au bout de seulement 4 emails Phish Threat.

Avec **Sophos Email**, faites de nouveau confiance à votre messagerie. La solution bloque les imposteurs et protège vos employés contre les attaques de phishing utilisant des adresses email frauduleuses usurpant le nom de contacts de confiance. Des techniques d'authentification SPF, DKIM, DMARC associées à des analyses de l'en-tête de l'email vous permettent d'identifier et d'autoriser les emails légitimes venant d'expéditeurs de confiance et de bloquer les imposteurs.

Sophos Intercept X associe un vaste ensemble de techniques fondamentales et modernes (Next-Gen) pour bloquer le plus large spectre d'attaques de ransomwares et de malwares. Sa technologie de Deep Learning issue des réseaux neuronaux se forme sur des centaines de millions de fichiers malveillants pour détecter de manière proactive les menaces inconnues

Exclusivité de Sophos, vous pouvez gérer toutes vos technologies de prévention du phishing depuis une seule console Web, qui s'appelle Sophos Central Vous n'avez plus besoin de maintenir des serveurs et vous pouvez y accéder à toute heure et en tous lieux, vous faisant gagner un temps précieux.

Vous pouvez démarrer avec un seul produit, puis en ajouter d'autres selon vos besoins.

Ne mordez pas à l'hameçon.

1, 3, 5, 7 Sources : Phishing Temperature Check, Freeform Dynamics in association with The Register and Sophos, 2017

2 Source : Verizon 2018 Data Breach Investigations Report

4 L'impossible défi de la cybersécurité, Sophos, juillet 2019

6 Source : Verizon 2016 DBIR & Experian Email Benchmark Report Q4 2016

7 Source : SophosLabs, 2017

Équipe commerciale France
Tél. : 01 34 34 80 00
Email : info@sophos.fr

2019-07-12 WP-FR (PC)

SOPHOS