CARBONITE® an opentext™ company | WEBROOT® an opentext™ company

Types d'attaques de phishing que vous devez connaître pour rester en sécurité

INTRODUCTION

Comme les pinsons de Darwin, le hameçonnage (phishing) est passé d'une technique unique à un ensemble de tactiques diversifiées et hautement spécialisées, chacune étant adaptée à des types spécifiques de cibles et de technologies. Décrit pour la première fois en 1987, le hameçonnage se fait désormais par message SMS, téléphone, via la publicité et, bien sûr, par e-mail.

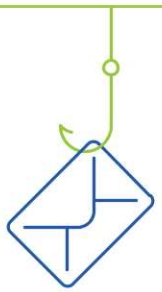
En résumé, toutes ces tactiques servent un même but: obtenir des informations confidentielles auprès d'une cible sans méfiance afin d'en tirer quelque chose de valeur. Mais le fait de connaître l'ensemble extrêmement diversifié des tactiques de hameçonnage d'aujourd'hui peut aider les gens ordinaires, qu'ils s'agissent d'internautes privés ou d'entreprises, à être mieux préparés à l'inévitable situation où ils seront la cible de ces attaques.

Voici 11 tactiques de hameçonnage courantes que vous devez connaître...

1 HAMEÇONNAGE STANDARD

Ratisser large

À la base, le hameçonnage standard consiste à tenter de dérober des informations confidentielles en prétendant être une personne ou une organisation autorisée.
Il ne s'agit pas d'une attaque ciblée et elle peut être diffusée *en masse*.



La plupart des sources attribuent la première description d'une attaque par hameçonnage à un article paru dans l'International HP Users Group, Interex en 1987.

Savez-vous comment déterminer si un e-mail est légitime ?

Voici cinq façons de repérer un e-mail de hameçonnage.

Un exemple de hameçonnage standard

Cette tactique a été, par le passé, davantage axée sur la quantité que sur la qualité. Le public était large et les e-mails étaient truffés d'erreurs évidentes. À mesure que le hameçonnage s'est développé, il est devenu plus sophistiqué et plus difficile à repérer. Pouvez-vous repérer les signaux d'alerte dans l'e-mail de hameçonnage ?

The White House Instruction for Coronavirus Inbox ×

info@whcoronavirustaskforce.com Jun 8, 2020, 1:09 PM (10 days ago)
to me

STATEMENTS & RELEASES. The White House. April 2, 2020

Read the White House instruction for America about quarantine which will be prolonged till August 2020.

Protect yourself and your family from the pandemic by following official White House guidelines for slowing the spread of the virus.

Steps to Stay Safe During the Pandemic

Best,

White House Coronavirus Task Force

2

HAMEÇONNAGE DE LOGICIELS MALVEILLANTS

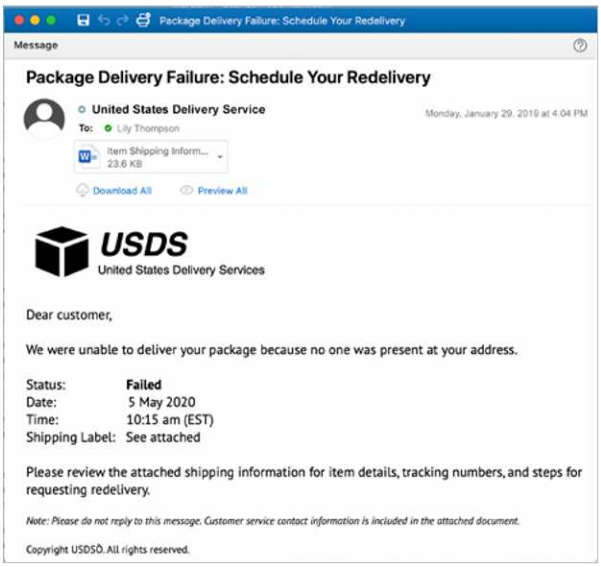
Méfiez-vous des macros

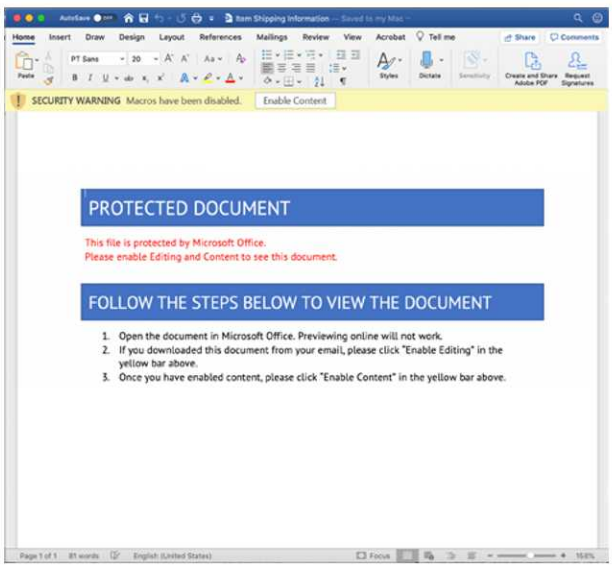
En utilisant les mêmes techniques, ce type de hameçonnage introduit des bugs indésirables après avoir convaincu un utilisateur de cliquer sur un lien ou de télécharger une pièce jointe qui installera des logiciels malveillants sur un appareil. Il s'agit actuellement de la forme d'attaque de hameçonnage la plus courante.

Vous avez reçu un e-mail non sollicité d'un expéditeur inconnu ? Méfiez-vous quant au contenu à télécharger qu'il contient. Nombre d'entre eux sont des pièces jointes malveillantes appelées « macros ».

Comment détecter le hameçonnage par logiciel malveillant

Le hameçonnage par logiciel malveillant se caractérise par la présence d'un document vierge en pièce jointe, vous invitant à activer des macros pour afficher son contenu, comme dans l'exemple courant « d'échec de livraison » ci-dessous. **Il s'agit là d'un signal d'alerte majeur.**



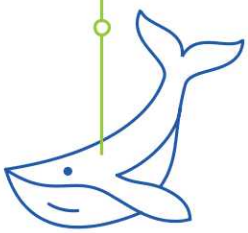


Hameçonnage standard
Logiciels malveillants Phishing
Spear Phishing
Smishing
Moteur de recherche Phishing
Vishing
Pharming
Clone Phishing
Phishing de l'homme du milieu (HDM)
BEC
Malvertising
Protégez-vous

3 SPEAR PHISHING

Attraper le plus gros poisson

Alors que la plupart des attaques de hameçonnage ratissent large dans l'espoir d'inciter le plus grand nombre d'utilisateurs possible à mordre à l'hameçon, le spear phishing implique des recherches approfondies sur une cible prédéfinie à forte valeur ajoutée, comme un PDG, un fondateur ou une personnalité publique, en s'appuyant souvent sur des informations accessibles au public pour élaborer une ruse convaincante.



Lorsque la cible est de très grande importance, le spear phishing est parfois appelé « chasse à la baleine ».

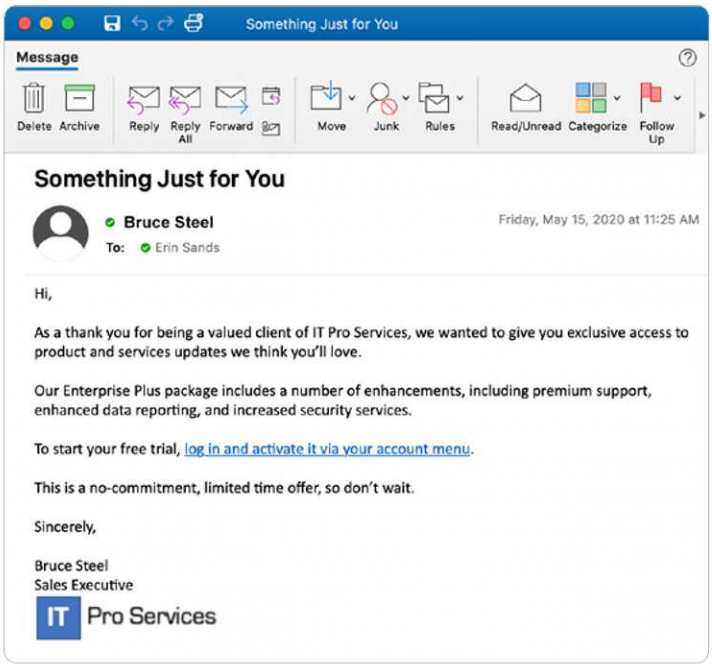
Une arnaque de 24 millions de dollars US

La permutation de carte SIM est un type de spear phishing où les attaquants dupent l'opérateur téléphonique d'une cible, en se faisant passer pour cette dernière et en affirmant qu'elle souhaite remplacersa carte SIM par l'une des leurs. Un tel cas a abouti à une perte de 24 millions de dollars en crypto-monnaie.

Vous souhaitez partager et recevoir des conseils sur les escroqueries actuelles avec d'autres personnes soucieuses de la cybersécurité ?
Rejoignez la communauté Webroot.

Un exemple de Spear Phishing

Vous trouverez ci-dessous une reconstitution d'une véritable tentative de spear phishing ciblant un client fournisseur de services gérés.



Hameçonnage standard
Logiciels malveillants Phishing
Spear Phishing
Smishing
Moteur de recherche Phishing
Vishing
Pharming
Clone Phishing
Phishing de l'homme du milieu (HDM)
BEC
Malvertising
Protégez-vous

4

SMS + PHISHING = SMISHING

Ne cliquez pas

Le phishing activé par SMS utilise les messages texte pour diffuser des liens malveillants, souvent sous la forme de codes courts, afin de piéger les utilisateurs de smartphones dans leurs escroqueries.

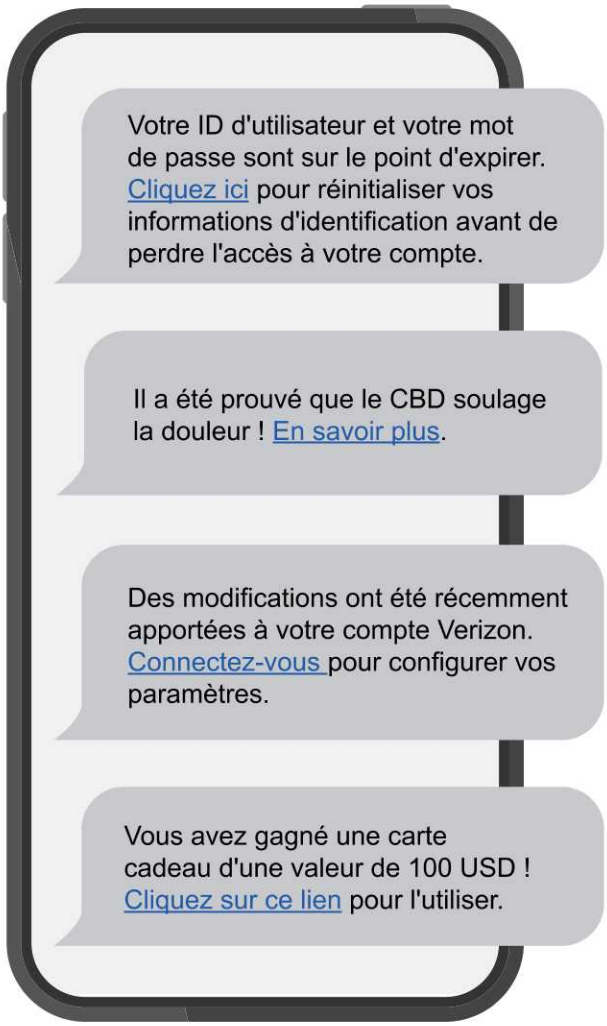
LE SAVIEZ-VOUS ?

Les taux d'ouverture des messages SMS tournent autour de 98 %. Comparez cela au taux d'environ 20 % pour les e-mails, et vous comprendrez tout de suite pourquoi les cybercriminels aiment le smishing.

Apprenez tout ce que vous devez savoir sur le smishing et comment éviter ces pièges dans ce billet de blog.

Repérer une attaque de smishing

Rester à l'affût. Les attaques de smishing commencent souvent avec quelque chose comme :



Hameçonnage standard
Logiciels malveillants Phishing
Spear Phishing
Smishing
Moteur de recherche Phishing
Vishing
Pharming
Clone Phishing
Phishing de l'homme du milieu (HDM)
BEC
Malvertising
Protégez-vous

5 PHISHING DANS LES MOTEURS DE RECHERCHE

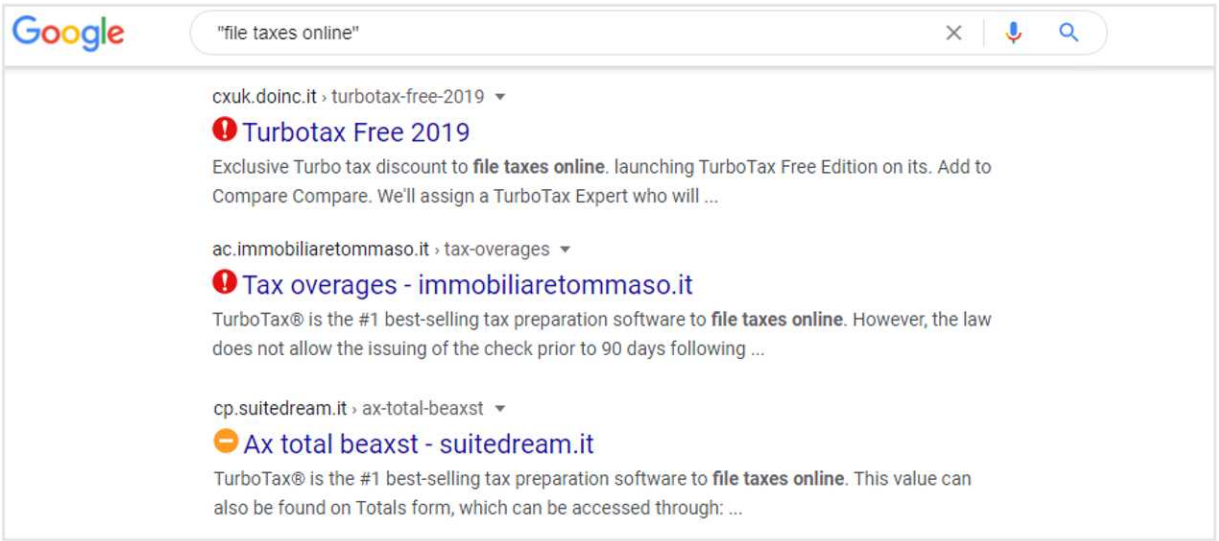
Faites attention à ce que vous choisissez

Dans ce type d'attaque, les cybercriminels attendent que vous veniez à eux. Le phishing via les moteurs de recherche injecte des sites frauduleux, souvent sous la forme d'annonces payantes, dans les résultats des termes de recherche populaires.

Les sites de hameçonnage des moteurs de recherche promettent souvent des offres incroyables, des opportunités d'avancement de carrière ou des taux d'intérêt bas pour les prêts. N'oubliez pas que si cela semble trop beau pour être vrai, c'est probablement le cas.

Détecter une escroquerie par hameçonnage dans les moteurs de recherche

Souvent, la seule différence entre le site de l'arnaque et l'adresse du site que vous recherchez réellement est un .com au lieu d'un .org. Examinez attentivement l'URL, le méta titre et la méta description avant de cliquer. Pour une couche de sécurité supplémentaire, utilisez un outil tel que l'extension Webroot Filtering pour signaler les menaces potentielles, comme dans l'image ci-dessous.



6

VISHING

Vous rendre vulnérable

Le vishing implique un acteur frauduleux qui appelle une victime en prétendant appartenir à une organisation réputée et tente de lui soutirer des informations personnelles, telles que des coordonnées bancaires ou les numéros d'une carte bancaire.

Le plus souvent, « l'appelant » semble de toute évidence être un robot, mais à mesure que la technologie progresse, cette tactique est devenue de plus en plus difficile à identifier.

Dring, dring... Bonjour, je fais partie du support technique de Windows. Je vous appelle parce que votre ordinateur a été infecté par un virus.

Vous êtes la victime d'une attaque par Vishing ? Voici ce qu'il faut faire.

Chaque fois que la période de déclaration des impôts arrive, le vishing fait partie de la liste du Trésor public qui répertorie les escroqueries tentant de piéger des contribuables. L'IRS demande à ce que celles-ci soient signalées à l'adresse phishing@irs.gov.

Comment éviter les escroqueries par Vishing

1. Soyez méfiant lorsque vous répondez à des appels provenant de numéros inconnus.
2. Si l'appelant demande des informations personnelles, ne les fournissez pas par téléphone.
3. Utilisez une application d'identification de l'appelant, mais ne lui faites pas entièrement confiance.
4. Recherchez le numéro de téléphone de l'appelant en ligne pour voir s'il s'agit d'une arnaque connue.
5. Si l'appel concerne un produit ou un service que vous utilisez, accédez au site Web du fournisseur ou appelez directement le fournisseur pour confirmer le problème.

7 PHARMING

Empoisonnement à la source

Également connu sous le nom d'empoisonnement du cache DNS, le pharming est une forme de phishing techniquement sophistiquée impliquant le système de noms de domaine (DNS) d'Internet. Le pharming redirige le trafic Web légitime vers une page usurpée à l'insu de l'utilisateur, souvent pour dérober des informations précieuses.

Le DNS agit comme un répertoire de l'Internet, et prend une longue chaîne de chiffres, à savoir l'adresse IP, pour la convertir en une URL que nous connaissons tous, comme amazon.com. Lorsque les cybercriminels interfèrent avec cette communication, on parle d'empoisonnement du cache DNS.

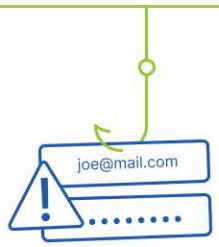
Opération Sea Turtle

Compte tenu du niveau de sophistication technique qu'il nécessite, l'empoisonnement du cache DNS est souvent effectué par des pirates informatiques soutenus par l'État. Dans l'un des exemples les plus célèbres, un groupe connu sous le nom de code « Sea Turtle » a utilisé cette technique pour espionner les agences de renseignement gouvernementales à travers le Moyen-Orient et l'Afrique du Nord. L'attaque a été annoncée par le groupe de renseignement privé Cisco Talos en 2019.

8

PHISHING PAR CLONAGE

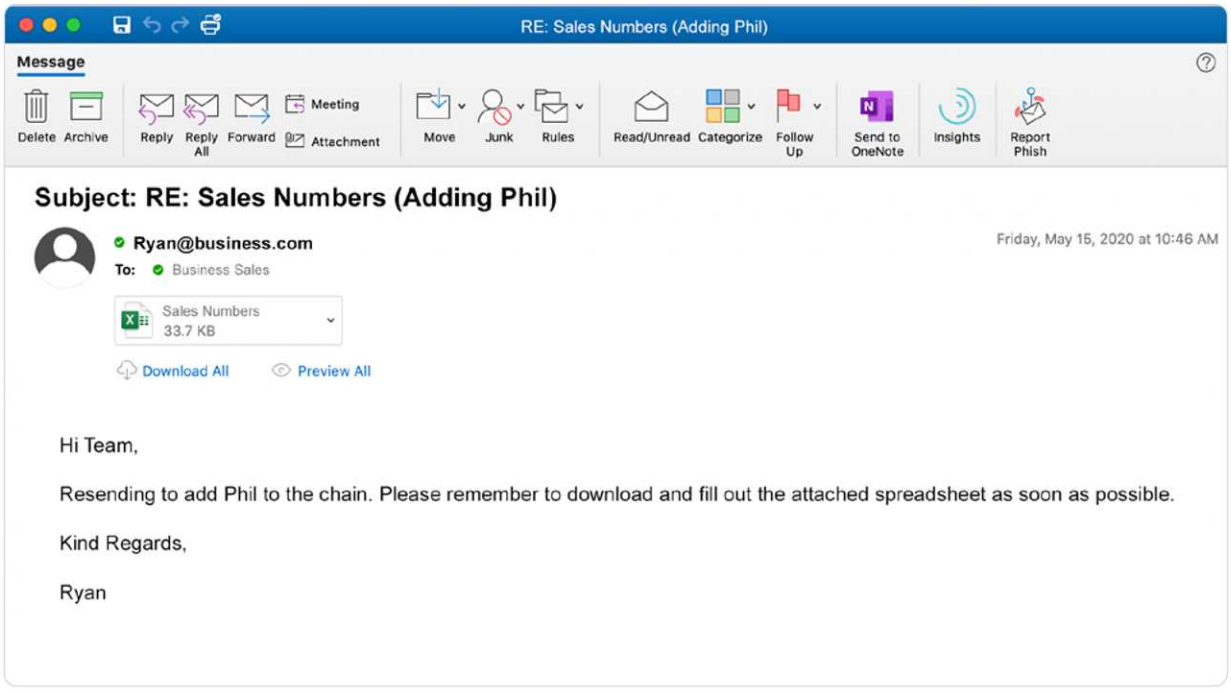
Dans ce type d'attaque, un acteur malveillant apporte des modifications à un e-mail existant, pour créer un e-mail presque identique (cloné) mais dont le lien, la pièce jointe ou un autre élément légitime est remplacé par un élément malveillant. Ces attaques ne peuvent pas démarrer sans qu'un attaquant n'ait d'abord compromis un compte de messagerie. Une bonne protection consiste donc à utiliser des mots de passe robustes et uniques en plus d'une authentification à deux facteurs.



Outlook, Gmail et d'autres fournisseurs de messagerie vous permettent de vérifier les emplacements à partir desquels les personnes ont accédé à votre compte. Si vous constatez que votre e-mail a été compromis, procédez comme suit.

À quoi ressemble le phishing par clonage

Vous trouverez ci-dessous un exemple qui démontre combien il est difficile de détecter un phishing par clonage. En exploitant la confiance sociale, le pirate augmente les chances de propager l'infection.

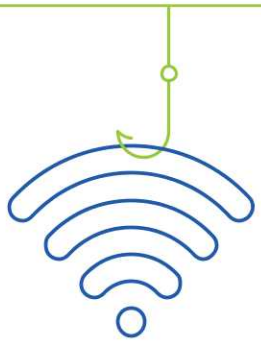


9

HOMME DU MILIEU (MAN-IN-THE-MIDDLE)

Une attaque par hameçonnage via le Wi-Fi public

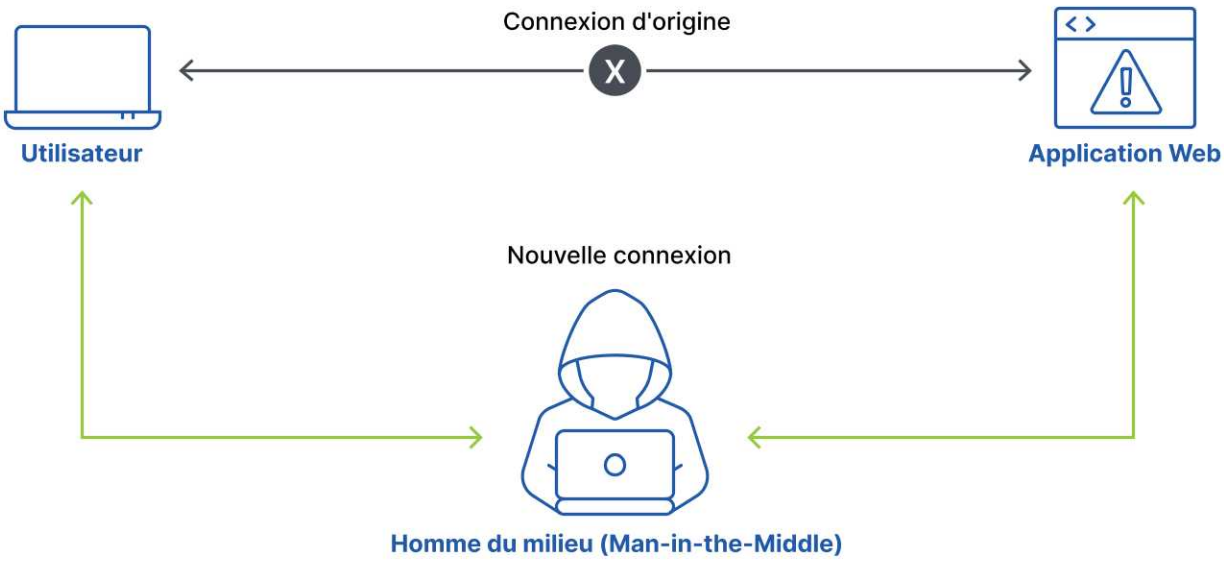
Une attaque « man in the middle » implique une écoute indiscrète qui surveille la correspondance entre deux parties qui ne se doutent de rien. Lorsqu'un tel stratagème est employé pour dérober des informations d'identification ou d'autres informations sensibles, cela devient une attaque de phishing « man-in-the-middle ». Ces attaques sont souvent menées à bien en créant des réseaux WiFi publics factices dans des cafés, des centres commerciaux et d'autres lieux publics. Une fois rejoint, l'homme du milieu peut hameçonner des informations ou diffuser des logiciels malveillants sur les appareils.



Sur la plupart des ordinateurs personnels, en particulier ceux exécutés sur les systèmes d'exploitation Windows, le partage de fichiers local est activé par défaut. Pour éviter que des logiciels malveillants ne soient envoyés sur votre appareil, désactivez ce paramètre lorsque vous vous connectez à des réseaux inconnus.

Fonctionnement du phishing MIM

Une victime qui tente de se connecter à son compte bancaire, par exemple, envoie sans le savoir ses informations d'identification à l'attaquant. L'attaquant connecte ensuite la victime au compte pour éviter tout soupçon.



10

COMPROMISSION D'E-MAIL (BEC) :

Ne réglez pas le paiement

Aujourd'hui, l'une des menaces les plus coûteuses pour les entreprises est la compromission des e-mails professionnels. Il s'agit d'un faux e-mail prétendant provenir d'une personne au sein ou associée à l'entreprise d'une cible et qui généralement fait état d'une demande urgente de paiement ou d'achat.

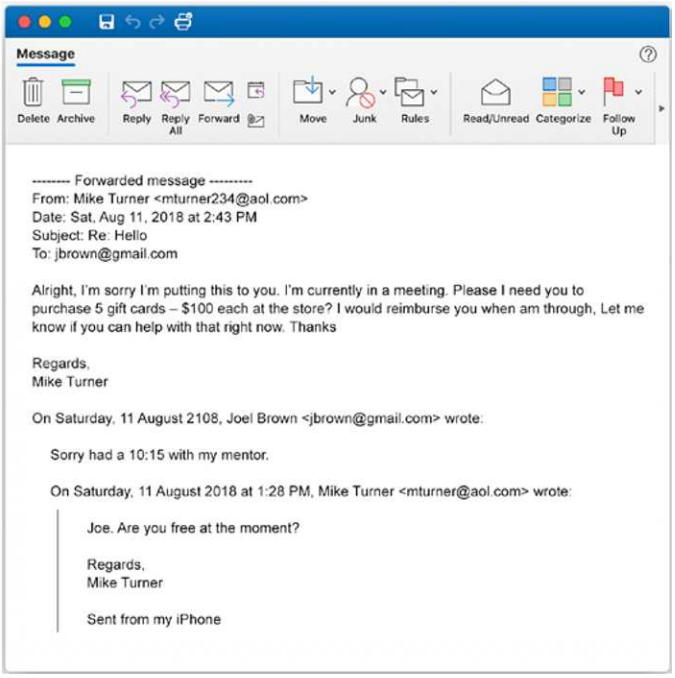
Le cas classique Schéma BEC

L'un des modèles les plus répandus pour compromettre les e-mails professionnels consiste à envoyer une demande « urgente » qui proviendrait d'un supérieur, vous demandant d'acheter des cartes cadeaux. Ces attaques s'appuient souvent sur des informations accessibles au public comme un accord commercial récemment conclu, et demandent à ce que des cartes-cadeaux d'un grand détaillant soient livrées de toute urgence à une adresse contrôlée par l'acteur malveillant.

Cela vous semble familier ?

« Pour remercier le client X, j'ai besoin que vous envoyiez 3 000 USD de cartes-cadeaux Target au responsable des achats le plus vite possible ! »

Sur les 3,5 milliards de dollars que les entreprises ont perdu selon les estimations du FBI à cause de la cybercriminalité en 2019, près de la moitié (1,7 milliard de dollars) a été imputée à la compromission d'e-mails.



11 MALVERTISING

Cette annonce n'est pas ce que vous pensez

Ce type de hameçonnage tire parti des exploits des logiciels de publicité ou d'animation pour usurper des informations appartenant aux utilisateurs ciblés. La publicité malveillante est généralement intégrée dans des publicités qui semblent par ailleurs normales, et elle est placée sur des sites Web légitimes comme Yahoo.com, mais avec du code malveillant implanté à l'intérieur.

Le kit d'exploit RIG, l'un des outils de malvertising les plus efficaces pour accéder à Internet, tire parti des quelques secondes nécessaires pour qu'une annonce soit redirigée vers son emplacement prévu afin d'injecter un logiciel malveillant dans un navigateur en lui ordonnant de commencer à chiffrer des fichiers qui peuvent ensuite être conservés en vue d'une rançon.

Une mauvaise surprise

Le kit d'exploit Angler (illustré ci-dessous) a livré CryptXXX, un rançongiciel auparavant omniprésent, qui générait 3 millions de dollars USD par mois pour ses créateurs.

Hameçonnage standard
Logiciels malveillants Phishing
Spear Phishing
Smishing
Moteur de recherche Phishing
Vishing
Pharming
Clone Phishing
Phishing de l'homme du milieu (HDM)
BEC
Malvertising
Protégez-vous

COMMENT VOUS PROTÉGER CONTRE LES ATTAQUES DE HAMEÇONNAGE

Afin de vous protéger contre les attaques de hameçonnage, vous devez commencer par savoir ce qui existe. En effet, selon les recherches réalisées par Webroot, une formation continue de sensibilisation à la sécurité peut aider à réduire les infractions de près de 70%.

Voici quelques conseils à garder à l'esprit pour éviter le hameçonnage :

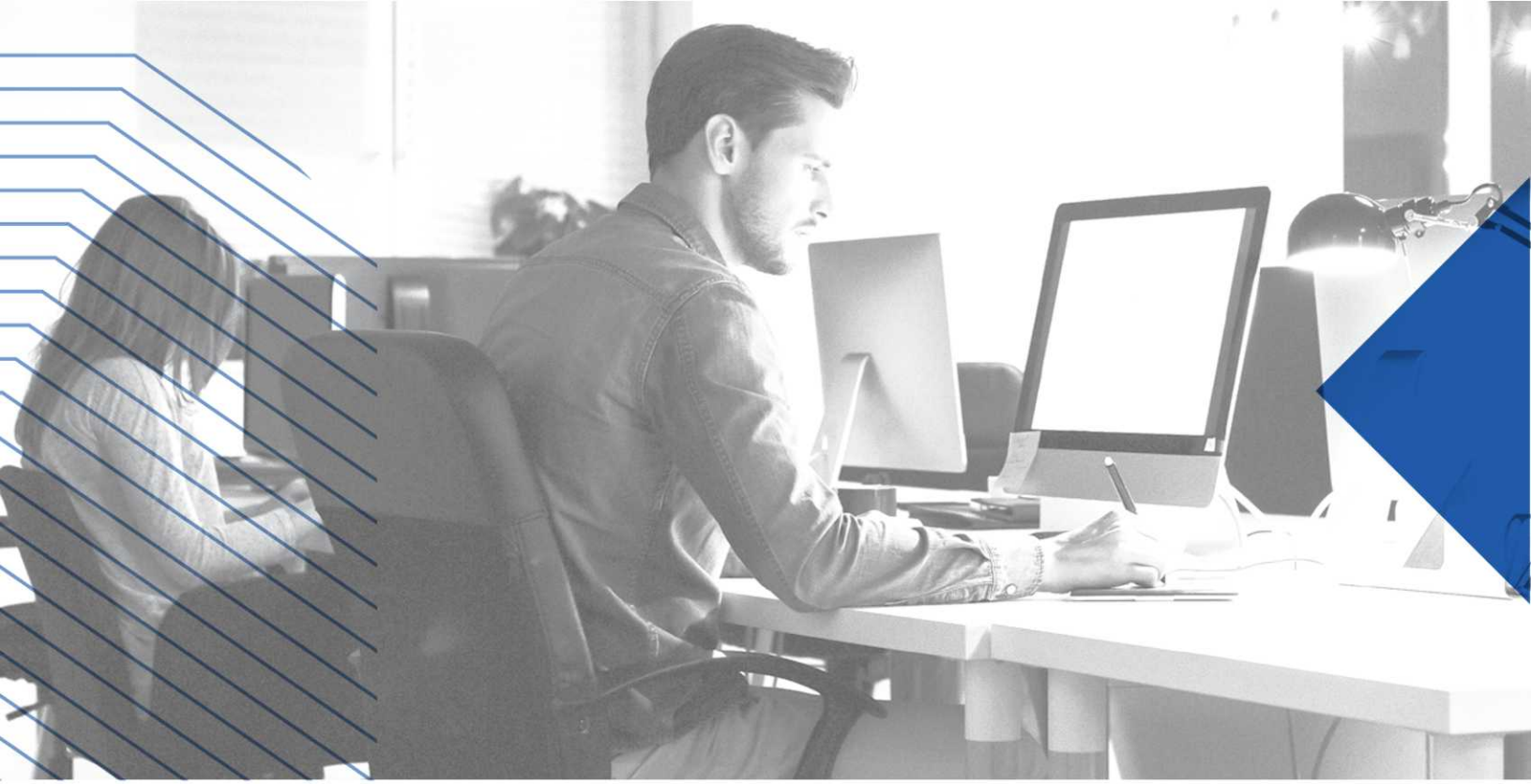
1. Ne cliquez jamais sur des liens d'expéditeurs inconnus ou si des détails de la communication ont éveillé vos soupçons.
2. Dans la mesure du possible, survolez un lien pour vous assurer que la destination correspond à ce à quoi vous vous attendez. Notez que cela ne fonctionnera pas sur un appareil mobile ou si des codes courts sont utilisés ; soyez donc très prudent sur les appareils mobiles.
3. Si vous pensez qu'un e-mail est une tentative de hameçonnage, vérifiez à nouveau le nom de l'expéditeur, la salutation et l'adresse physique en pied de page et la présence d'un bouton de désabonnement. En cas de doute, supprimez-la.
4. Si vous n'êtes pas sûr qu'une communication soit légitime, essayez de contacter la marque ou le service via un autre canal (son site Web ou en appelant une ligne de service client, par exemple).
5. Évitez de saisir des informations personnellement identifiables, sauf si vous êtes certain de l'identité de la partie avec laquelle vous communiquez.

Combler toutes vos failles de sécurité

Bien qu'une grande vigilance aidera à maintenir la plupart des attaquants à distance, personne ne peut être sûr à 100 % par lui-même. Après tout, le hameçonnage existe encore aujourd'hui car il fonctionne bel et bien. C'est pourquoi il est important de combiner une formation de sensibilisation à la sécurité avec une protection des terminaux professionnels de qualité, grâce à l'intelligence artificielle améliorée, les mises à jour basées sur le cloud et l'anti-hameçonnage en temps réel, la protection DNS et la sauvegarde fiable des données.

En mettant en œuvre une, deux ou les cinq solutions ci-dessus, vous pouvez être sûr que votre entreprise sera plus résiliente face à cette menace croissante.

- Hameçonnage standard
- Logiciels malveillants Phishing
- Spear Phishing
- Smishing
- Moteur de recherche Phishing
- Vishing
- Pharming
- Clone Phishing
- Phishing de l'homme du milieu (HDM)
- BEC
- Malvertising
- Protégez-vous



Protégez votre entreprise. Protégez votre activité.

DEVENEZ CYBER-RÉSILIENT.

Webroot et Carbonite offrent ensemble la meilleure solution de sécurité des terminaux et une sauvegarde et restauration de niveau entreprise dans une suite complète conçue pour les entreprises comme la vôtre. Commencez avec notre protection primée des terminaux.

COMMENCER

CARBONITE® an opentext company | WEBROOT® an opentext company