WHITE PAPER

vade

Attaques de Phishing

Des menaces sophistiquées
qui passent entre les mailles du filet

Table des matières

Introduction

Les emails de phishing maladroits appartiennent au passé. Aujourd'hui, les hackers font preuve d'une ingéniosité redoutable et sont passés maîtres dans l'art de dissimuler leurs attaques aux yeux des utilisateurs et des filtres de messagerie. Ils sélectionnent désormais leurs victimes avec soin et effectuent de nombreuses recherches avant de lancer leurs attaques. Même après avoir suivi une formation de sensibilisation à la sécurité, les utilisateurs, toujours plus sollicités, finiront par baisser leur garde et faire courir un risque à votre entreprise.

Après avoir affiné leurs techniques et opté pour des attaques de plus en plus ciblées, les hackers ont commencé à délaisser les grandes entreprises au profit des PME. Les attaques ciblant les grandes entreprises sont certes extrêmement rentables lorsqu'elles aboutissent, mais elles sont complexes à mettre en œuvre en raison de l'importance du budget et des ressources humaines alloués à l'informatique. En revanche, le danger est réel, toujours plus présent et toujours plus difficile à détecter pour les PME.

Les hackers se font passer pour les marques dans lesquelles vous avez le plus confiance

Par le passé, les hackers choisissaient leurs victimes au hasard, ou ne les choisissaient pas du tout, et envoyaient des emails de phishing à des centaines, voire des milliers de destinataires. Pour améliorer leur taux de réussite, ils enquêtent désormais sur leurs cibles et déterminent les marques avec lesquelles elles sont liées, par exemple des banques, des fournisseurs de logiciels et d'applications, des magasins en ligne, etc.

Les marques les plus usurpées en 2019 vont des services dans le cloud aux banques, en passant par les plateformes de streaming. Leur point commun ? Une image inspirant la confiance, reconnaissable immédiatement, et de nombreuses victimes potentielles.

No. 1

D'après les PME, le phishing et l'ingénierie sociale constituent la principale stratégie utilisée lors des cyberattaques – **Keeper & Ponemon, 2019 Global State of Cybersecurity in SMB**

66%

des PME ont subi une cyberattaque en 2018 – **Ibid.**

Nombre d'URL de phishing uniques détectées par Vade
T1–T4 2019

Microsoft	PayPal	NETFLIX	facebook	BANK OF AMERICA
64,331	61,226	43,185	42,338	19,800

Techniques de phishing

Les hackers ont recours à diverses techniques pour imiter l'apparence d'un email d'une marque connue. Ils s'appuient notamment sur les logos, images et boutons d'appel à l'action originaux de la marque en question. Si la qualité apparente de l'email de phishing contribue à son authenticité perçue, ce sont ses aspects techniques qui convainquent les utilisateurs de sa légitimité.

Usurpation d'adresses email

L'usurpation du domaine exact est une technique permettant à un hacker de reproduire l'adresse email d'une marque. Également appelée « usurpation de domaine », cette technique est moins couramment utilisée que les autres, car la plupart des filtres de messagerie la détectent facilement grâce aux protocoles DMARC (Domain Message Authentication Reporting) et DKIM (DomainKeys Identified Email).

Avec **l'usurpation du nom affiché**, un hacker peut afficher le nom et l'adresse email de la marque en lieu et place du nom de l'expéditeur de l'email. Cette stratégie est la plus couramment utilisée et très efficace, car de nombreux utilisateurs ne regardent que le nom de l'expéditeur, et pas son adresse email. Elle est particulièrement redoutable sur les appareils mobiles, car l'adresse email y est souvent masquée. L'utilisateur doit en effet appuyer sur le champ « De » pour l'afficher.

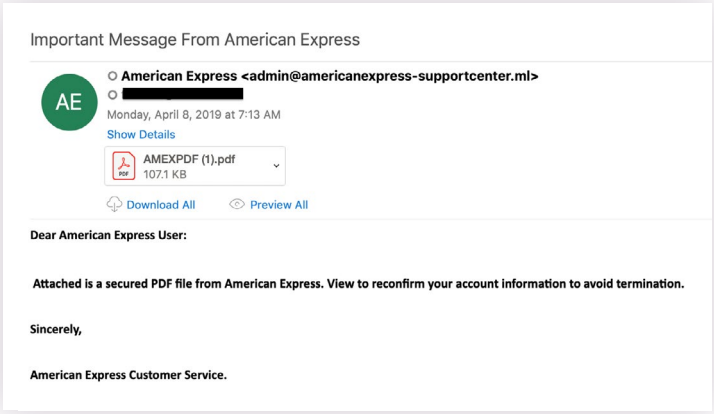
Avec **l'utilisation de domaines voisins**, un hacker crée une adresse email suffisamment proche de l'originale pour tromper les utilisateurs. Il peut par exemple ajouter des extensions comme co, company, ca et ml à la fin de l'adresse pour faire croire qu'elle utilise un domaine de la marque.

Une autre méthode d'usurpation consiste à inclure des le**ttres en cyrillique (russe)** dans l'adresse email. Il devient alors difficile pour un filtre de faire la différence entre des caractères similaires, comme la lettre latine 'a' et la lettre cyrillique 'а".

> americanexpress.com > americanexpress.com
> microsoft.com > microsoft.com

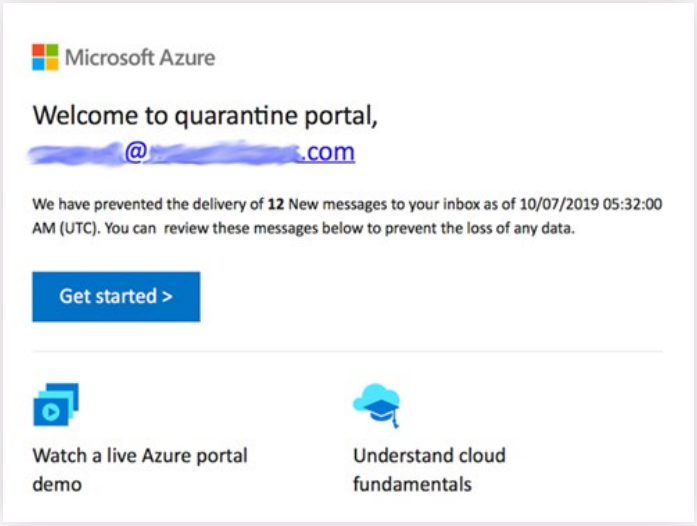
Pourquoi les emails usurpant des marques parviennent-ils à tromper les filtres ?

Les filtres classiques recherchent des expéditeurs disposant d'une mauvaise réputation, par exemple les adresses IP connues pour envoyer des volumes importants de spams et les domaines connus pour héberger des pages Web de phishing. Si les adresses IP et domaines sont uniques, non connus du filtre et jouissent d'une bonne réputation, la tentative d'usurpation peut passer inaperçue.could bypass a filter.



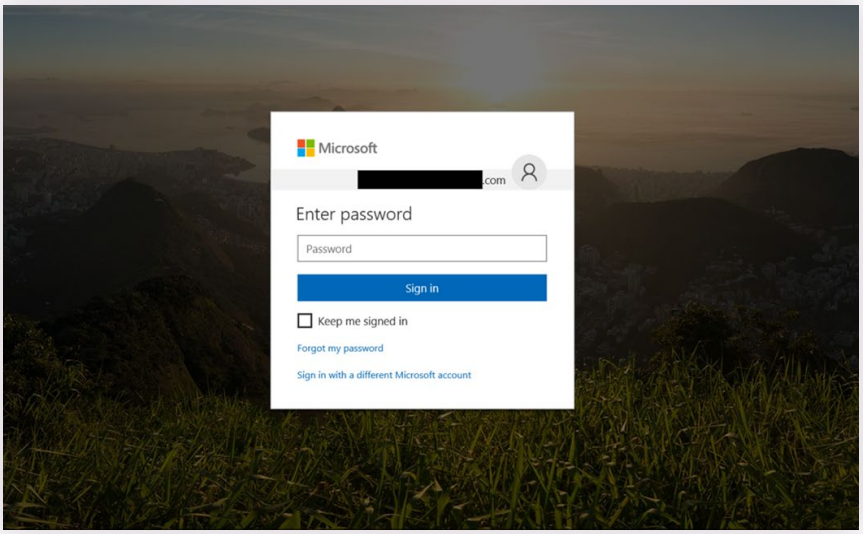
Utilisation d'images et de logos de marques

Dans les attaques les plus simples, les hackers peuvent inclure une image dans l'email de phishing, généralement un logo de mauvaise qualité, que les utilisateurs remarquent facilement.



En revanche, dans **les attaques plus évoluées**, ils multiplient les images. L'email paraît ainsi plus authentique et l'utilisateur est plus susceptible de le juger légitime. Bien souvent, le logo de la marque est légèrement altéré. Ces modifications suffisent à tromper les filtres qui reconnaissent les images à l'aide de leur signature (hachage cryptographique), mais ne sont pas visibles à l'œil nu.

Les pages de phishing les plus travaillées utilisent également des images de haute qualité pour renforcer leur authenticité perçue. Bien souvent, un utilisateur lambda est incapable de faire la différence entre une page de phishing de qualité et la véritable page de la marque.

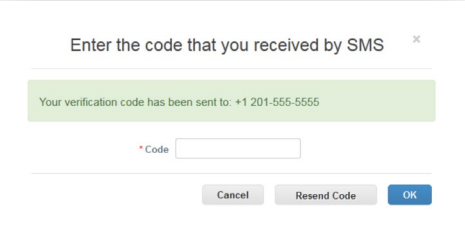


Visuellement, l'image ci-dessus semble identique à celle de la page officielle de connexion à Microsoft 365. Le hacker a copié le code CSS de la véritable page Microsoft 365 et l'a inséré dans sa page. Le résultat obtenu est suffisamment proche de l'original pour tromper l'utilisateur. .

Exploiting authentication tools

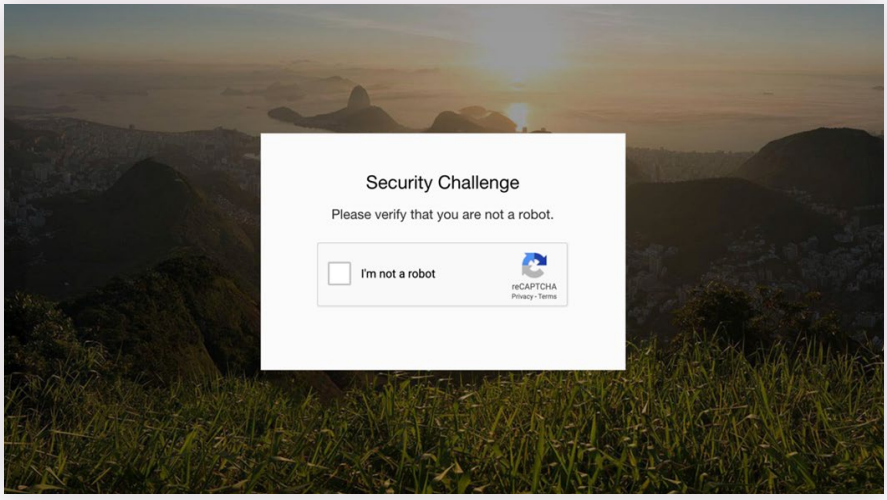
L'authentification à deux facteurs (2FA) constitue l'une des meilleures protections contre le vol d'identifiants et est désormais bien connue. Les utilisateurs y sont habitués et sont donc en confiance lorsqu'ils sont invités à saisir leurs identifiants dans le cadre de cette procédure.

Pour exploiter ce mécanisme, les hackers incluent dans leurs pages de fausses fenêtres contextuelles d'authentification 2FA. Ainsi détourné, ce protocole permet de voler les identifiants plutôt que de les protéger. Lorsqu'un utilisateur saisit ses identifiants de connexion sur une page de phishing, ceux-ci sont immédiatement dérobés par le hacker. Il essaie alors de s'identifier à l'aide de ces informations, ce qui entraîne l'envoi d'un code sur le téléphone de l'utilisateur. La fausse fenêtre contextuelle s'affiche alors sur la page de phishing, et l'utilisateur y saisit le code pour confirmer son identité. Le hacker récupère ainsi le code d'authentification nécessaire pour accéder au compte de sa victime.



Conçus pour protéger les sites Web des bots, les tests **CAPTCHA et ReCPATCHA** constituent une autre forme d'authentification. Encore une fois, les utilisateurs les connaissent bien et pensent être en sécurité lorsqu'ils y sont confrontés.

De récentes attaques de phishing détectées par Vade utilisent de faux tests CAPTCHA et ReCAPTCHA conçus pour pousser les internautes à penser que la page Web qu'ils visitent est sûre. Que l'utilisateur réussisse ou non le test CaPTCHA importe peu, car le test n'est présent que pour ajouter une touche d'authenticité à la page.



Kevin Mitnick, un expert en sécurité, a présenté une autre forme d'exploitation du mécanisme d'authentification à deux facteurs. Il a en effet montré qu'un hacker pouvait copier un cookie de session à l'aide d'un outil de développement inclus dans le navigateur Internet lorsque la victime saisit ses identifiants pourtant protégés avec l'authentification 2FA. Il peut alors coller ce cookie dans un navigateur et accéder au compte de la victime.

Comment savoir si une méthode d'authentification est légitime?

Vérifiez si les URL sont longues et complexes, avec des codes régionaux ne correspondant pas au pays d'origine du site Web authentique. Vérifiez également si la fenêtre contextuelle est associée à un formulaire fonctionnel ou non. Bien souvent, lorsque vous saisissez des identifiants dans un formulaire non fonctionnel, la validation n'aboutit nulle part.

Obfuscation et multiplication des URL

Si un email contient une URL de phishing connue, il sera bloqué par les filtres. Cette protection pose un problème aux hackers, qui vl'ont résolu grâce à la technique dite de l'obfuscation d'URL.

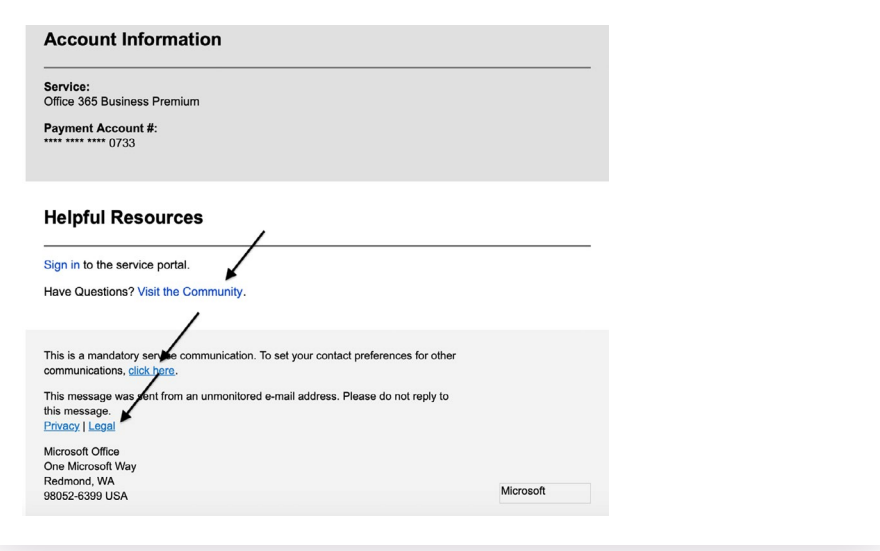
Un hacker peut insérer une URL d'une marque connue et de confiance dans un email et lui adjoindre une **redirection**, une méthode tout à fait légitime pour rediriger des pages obsolètes vers des pages à jour, vers l'URL d'une page de phishing.

Les outils de **raccourcissement d'URL**, qui raccourcissent les URL et en créent des alias, sont également utilisés à cette fin. Un lien de phishing connu dont la structure de l'URL est normale diffère totalement de sa version raccourcie.

> URL d'origine : https://www.vadesecure.com
> URL raccourcie : https://bit.ly/2P9wh7n

Le masquage d'une URL dans un **QR Code** permet de tromper les listes noires d'URL et les algorithmes en mesure de détecter les images et les objets, mais incapables d'extraire les URL masquées. L'URL de phishing associée au QR Code redirige généralement l'utilisateur vers un site Web de Bitcoin qui l'invite à payer une rançon.

La **multiplication des URL** est une méthode consistant à inclure de nombreuses URL légitimes dans un email, en plus de l'URL de phishing à proprement parler. Bien souvent, l'URL malveillante est la dernière de l'email. Le hacker espère ainsi que le filtre de messagerie validera l'email après avoir identifié plusieurs URL légitimes de marques de confiance.



Comment puis-je repérer une URL de phishing ?

Passez le curseur sur l'ensemble des URL de l'email pour voir où elles mènent. Les marques bien établies ont généralement recours à des structures d'URL courtes et claires. Si vous cliquez sur l'URL, assurez-vous que l'URL de la page sur laquelle vous arrivez est bien celle que vous attendiez. En cas de doute, saisissez l'adresse du site Web de la marque directement dans votre navigateur.

Comment Vade bloque les attaques ciblées

La technologie anti-phishing de Vade utilise l'intelligence artificielle pour bloquer les menaces les plus sophistiquées.

Analyse des caractéristiques – Des modèles d'apprentissage automatique supervisé explorent le contenu des emails, y compris les métadonnées, le code HTML et les pièces jointes à la recherche d'URL, de domaines et de signatures de phishing connus.

Définition aléatoire des jetons – Pour protéger l'utilisateur des pages dormantes et des liens dynamiques, les jetons des URL sont remplacés de manière aléatoire pendant que le moteur d'IA analyse l'URL à la recherche de contenus malveillants. Au cours de ce processus, les jetons ne déclenchent ainsi pas le suivi de l'utilisateur ou une action quelconque sur l'URL.

Détection des images et des objets – Des modèles d'apprentissage profond avec Computer Vision analysent les images de l'email, y compris les logos des 30 marques les plus ciblées par le phishing, pour repérer les modifications qu'un hacker aurait pu apporter pour tromper les technologies basées sur les signatures. Les modèles de Computer Vision sont également entraînés pour reconnaître les QR Code, fréquemment utilisés dans les emails de sextorsion pour cacher des URL au sein d'une image. Ces modèles extraient les URL et les analysent pour déterminer si elles sont malveillantes ou non.

Analyse de l'affichage sur appareils mobiles – Pour protéger les utilisateurs des attaques de phishing conçues spécifiquement pour les appareils mobiles, des algorithmes explorent les pages Web avec 30 combinaisons appareil/navigateur afin d'identifier les menaces visibles uniquement sur certains appareils.

Exploration régionale des pages Web – Les pages Web sont analysées depuis quatre zones géographiques (Amérique du Nord, Amérique du Sud, Europe et Asie) pour identifier les pages de phishing affichées uniquement lorsque l'internaute est basé dans une région spécifique.

J'ai signalé cet email de phishing la semaine dernière. Pourquoi est-ce que je le reçois encore ?

La plupart des filtres analysent la réputation (adresse IP, domaine) et la signature (code), mais ne voient pas les emails comme les êtres humains. Même si visuellement, l'email peut paraître parfaitement identique, les hackers apportent de subtiles modifications à sa signature pour convaincre les filtres qu'il est unique et lui permettre ainsi de ne pas être repéré lors de l'analyse.

Protection contre le phishing continue et adaptative

La meilleure défense contre le phishing associe formation des utilisateurs et technologie anti-phishing. Mieux un utilisateur est formé, plus il est susceptible de signaler les emails suspects. Cette formation doit intervenir lors de sessions formelles, mais aussi au moment du clic pour fournir du contexte et lier l'incident avec le contenu de la formation.

Les attaques de phishing évoluent en permanence et de nouvelles menaces sont détectées chaque jour. Les modèles d'apprentissage automatique de Vade sont entraînés en permanence à l'aide de nouvelles données sur les menaces issues des signalements des utilisateurs de nos clients, des URL de phishing signalées sur IsItPhishing.AI, et de l'analyse continue des plus de 1 milliard de boîtes de messagerie protégées par Vade. À mesure que de nouvelles menaces sont détectées et analysées, les modèles sont révisés et mis à jour afin de les identifier et de les bloquer.

En savoir plus

vadesecure.com/en/solutions/anti-phishing

À propos de Vade

Notre mission?. Protéger les emails du monde entier des menaces les plus sophistiquées. Que ce soit pour assurer la protection des particuliers via les plus grands FAI ou les entreprises via nos partenaires MSP, nos solutions de sécurité de l'email basées sur l'IA sont conçues pour détecter l'indétectable.

- 1 milliard de boîtes mails protégées
- 100 milliards d'emails analysés / jour
- 1,400+ partenaires dans le monde
- Renouvellement annuel de 95%
- 15 brevets internationaux actifs

En savoir plus
www.vadesecure.com

@vadesecure