Association Loisirs et culture

Phishing : toutes les astuces pour éviter de tomber dans le panneau

Jean Marie Herbaux

Table des matières

Le phishing, ou hameçonnage en français, est l'un des plus grands fléaux d'Internet. Des individus envoient des e-mails en tentant de se faire passer pour quelqu'un d'autre pour vous amener à cliquer sur un lien. Ils parviennent à voler vos identifiants en vous faisant croire que vous vous connectez sur un site de confiance, mais ce n'est qu'une copie. Dès l'instant où vous entrez votre mot de passe, ils ont accès à votre compte.
Cette menace n'est pas nouvelle, mais elle prend de l'ampleur. Depuis 2020, le nombre de personnes en télétravail ou effectuant des transactions sur Internet a largement augmenté, ce qui multiplie les opportunités pour les pirates informatiques.
Des attaques plus sophistiquées reposent pour beaucoup sur l'ingénierie sociale, où les pirates tentent de duper leurs victimes.
Dons tous les cos, la meilleure parade est d'abord la formation pour repérer ce genre d'arnaque.
Dons cette note de lecture, nous vous expliquons le fonctionnement de ces attaques et les différents types, ainsi que les bons réflexes à adopter.

1. Qu'est-ce que le phishing ?

Le hameçonnage (phishing en anglais) désigne un type d'attaque où un pirate part à la pêche aux informations. Le vocabulaire utilisé dans le domaine est généralement celui de la pêche, car les pirates essaient de leurrer leurs victimes avec un appât. Le terme phishing est un jeu de mots comme phishing en anglais, qui signifie pêche .

1) L'attaque est composée de deux catégories.

a. La première est un message

le plus souvent un e-mail, envoyé aux victimes. Il contient généralement une alerte au sujet d'un problème avec le compte qui demande de cliquer sur un lien pour passer en revue ou rectifier la situation. Ou bien il s'agit d' annoncer que vous avez gagné quelque chose.

b. La seconde catégorie

La seconde catégorie est une simple page web qui demande à l'utilisateur de se connecter. Toutefois, il s'agit d'une copie d'un site légitime, par exemple une fausse page d'identification pour Facebook. L'utilisateur entre son mot de passe qui est immédiatement communiqué au pirate ayant lancé l'attaque.

c. Le plus courant

Le cas plus courant de phishing est l'e-mail de masse. Les pirates peuvent par exemple créer une fausse page d'identification pour PayPal, puis envoyer un faux message mentionnant des transactions inhabituelles à une base de données contenant des milliers voire des millions d'adresses e-mail. Tous n'utiliseront pas PayPal, et une majorité ne cliquera pus sur le lien, soit parce qu'ils ont identifié la supercherie. soit parce qu'ils passent par un favori de leur navigateur. Cependant. en envoyant un très grand nombre d'adresses, cette attaque est très rentable, Il leur suffit d'un très faible pourcentage de personnes qui tombent dans panneau pour accéder de nombreux comptes.

2) le spear phishing ou harponnage

Pour continuer dans le thème marin, le spear phishing ou harponnage est une variante de cette attaque. Plutôt que de lancer un vaste filet pour tenter de duper le plus de monde possible, les pirates ciblent des personnes en particulier. Il peut s'agir d'un groupe comme une entreprise ou les employés d'un hôpital ou d'une administration ou alors d'une personne très spécifique. Dans ce cas. l'attaque sera un peu plus recherchée. L'auteur prendra le temps de consulter les informations

accessibles en ligne sur ses victimes potentielles. Il pourra par exemple consulter les données publiques de l'entreprise, mais également se rendre sur les profils des employés sur les réseaux sociaux. Pour les attaques ciblées sur une seule personne, il pourra découvrir ses centres d'intérêt et lui envoyer une offre promo alléchante. par exemple.

3) Le whaling qui cible spécifiquement les entreprises

Le whaling ou chasse à la baleine est une attaque qui cible spécifiquement les entreprises. Il vise un dirigeant ou un cadre supérieur. Ici, l'auteur crée un message destiné à duper la victime en reprenant tout le jargon professionnel et en utilisent des références à des éléments qui ne sont généralement disponibles qu'en interne mais qui peuvent être trouvé sur Internet. Ainsi, le pirate peut se faire passer pour un fournisseur ou un partenaire. Dans quelques cas, il réussit à se raite passer pour le PDG. Bien souvent l'envoi d'un e-mail très ciblé est suivi d'un coup de fil pour confirmer. La victime est alors plus encline à croire, ayant eu un contact direct avec la personne. L'auteur de l'attaque peut se contenter d'un lien pour obtenir des identifiants mais dans cette situation spécifique il vise le plus souvent à obtenir un transfert d'argent S'il n'a pas pu avoir assez de détails sur sa victime pour créer une attaque crédible il peut d'abord viser une autre personne dans le but d'obtenir plus d'informations sur sa véritable cible. Ce genre d'attaque n'est plus nécessairement rapide, dans certains cas, l'auteur peut créer une personnalité en ligne, sur les réseaux sociaux par exemple, et établir progressivement un rapport avec sa victime pendant des semaines. ou des mois.

4) Le smishing s'appuie sur les smartphones

Le smishing, contraction de SMS et phishing s'appuie sur les smartphones. Bon nombre d'utilisateurs pensent qu'il est moins risqué de cliquer sur un lien sur son mobile. il aurait pas de Virus. Ce raisonnement est on ne peut plus faux, c'est pour cela que les pirates n'hésitent pas à envoyer tin lien par SMS. Qui n'a pas déjà reçu un SMS d'un transporteur de colis avec un lien pour accéder au suivi ou pour reprogrammer la livraison ? Difficile de distinguer le vrai du faux. puisque très souvent l'expéditeur n'est pas identifiable et le contenu du message n'est que du texte sans mise en forme. L'auteur n'a aucun besoin d'essayer de dupliquer une identité visuelle. Ce gui rend cette technique beaucoup plus simple,

5) Le vishing hameçonnage par téléphone

Le vishinq (voice phishinq}, ou hameçonnage par téléphone est une autre technique qui utilise le téléphone plutôt qu'un e-mail ou un SMS. Cette attaque est très efficace, mais demande plus de temps puisqu'il faut interagir avec chaque victime. Les pirates peuvent modifier l'identification de l'appelant pour se faire passer pour un numéro officiel et légitime, ou pour que le téléphone affiche simplement Microsoft, par exemple. Ils peuvent alors se présenter comme le support technique qui aurait automatiquement repéré un problème sur ordinateur, ou même pour le service client d'une entreprise que vous connaissez bien. Ils peuvent même obtenir des informations très spécifiques, si par exemple vous avez publié des photos de vos achats sur les réseaux sociaux. Ils vont alors vous poser des questions pour vérifier votre identité, comme si c'était vous qui veniez de les appeler et non l'inverse. Ils peuvent à ce moment-là vous demander votre mot de passe pour accéder à votre compte ou alors vous demander de cliquer sur un lien pour vous identifier ou encore installer un logiciel qui surveillera votre ordinateur et collectera mots de passe et numéro de carte bancaire.

6) Attaque par le fichier HOSTS

Les précédentes méthodes de phishing sont toutes techniquement très simples, et consistent à convaincre la victime de cliquer sur lien pour s'identifier ou pour donner volontairement des informations. Une autre variante est un peu plus complexe, mais très difficile à repérer même pour les utilisateurs avertis. la première phase de l 'attaque consiste à vous faire installer un malware, un petit programme qui va effectuer quelques modifications dans un fichier clé de votre ordinateur. Ici, ils utilisent la technique habituelle le plus souvent, qui consiste à le mettre en pièce jointe, tenter de le faire passer pour une facture ou tout autre fichier que vous pourriez ouvrir sans vous méfier. Une fois lancé, le programme modifie le fichier HOSTS.

Lorsque vous saisissez une adresse d'un site ou que vous cliquez sur un lien, exemple Google.fr, votre ordinateur contacte un serveur DNS pour lui demander l'adresse IP du site afin de pouvoir se connecter. Toutefois, avant de contacter Le serveur DNS il consulte d'abord le fichier HOSTS de Windows. Celui-ci peut contenir des associations de noms de domaine et d'adresses IP permanentes. Il permet aussi par exemple de bloquer l'accès à certains sites en leur mettant une adresse IP fausse. (Une technique qui peut être utilisée pour bloquer la publicité). Toutefois, ici, notre malware ajoute le nom de domaine d'un site spécifique, par exemple Facebook ou PayPal et l'associe à l'adresse IP d'une fausse page de connexion. Ainsi, en tentant de vous rendre sur le site, peu importe si vous saisissez l'adresse ou si vous utilisez les favoris du navigateur, vous obtiendrez la fausse page, tout en affichant la bonne adresse.

2. Comment se protéger ?

1) Méfiez-vous de tout message.

La première protection passe par l'humain Il faut toujours être méfiant de tout message reçu. Si un email ou un SMS vous demande de cliquer pour accéder à votre compte, ne le faites pas à moins d'être absolument certain que le message est légitime. *Passez toujours par les favoris du navigateur. ou en utilisant l'adresse du site directement.*
S'il S'agit d'un problème avec votre compte, vous devriez pouvoir y accéder une fois identifié, sans avoir à cliquer sur le lien.
N'ouvrez jamais les pièces jointes, à moins de savoir exactement ce que c'est. Les messages sont. souvent accompagnés d'un malware qui se fait passer pour une facture, un dossier compressé ou tout autre fichier a priori inoffensif.
Ne vous fiez pas à l'adresse de l'expéditeur, qui est très simple à falsifier.
Aucun agent de Microsoft ne vous appellera pour un problème sur votre ordinateur. Ces appels sont toujours une arnaque. De la même manière, ne donnez jamais d'informations personnelles à un conseiller qui vous appelle, même s'il semble être en lien avec un de vos centres d'intérêt ou un achat effectué récemment.

2) Attention à l'orthographe

Les auteurs des e-mails de phishing ne s'appliquent pas toujours à créer un message crédible. Dans certains cas, le courriel est quasiment impossible à distinguer d'un vrai, très souvent la qualité laisse à désirer. L'orthographe et la grammaire sont souvent médiocres. Les auteurs ne maitrisent pas la langue française et ont notamment recours aux traducteurs automatiques.

3) Attention aux fausses adresses web

Pensez également que les liens des e-mails ne sont pas toujours ceux qui sont affichés. Tout comme il est possible de transformer les mots « *cliquez ici* » en lien qui renvoie vers n'importe quelle adresse. Il est également possible de mettre le texte d'une adresse, ainsi qu'un lien qui renvoie vers un site compétemment différent quand on clique dessus. *Pour savoir où renvoie un lien, il suffit de passer sa souris dessus et de regarder dans la barre d'état de la fenêtre en bas à gauche*.

4) Changez régulièrement vos mots de posse

Ce conseil n'est pas spécifique au phishing. Il arrive régulièrement que des bases de données contenant un grand nombre d'informations personnelles, parfois avec les mots de passe, fuitent sur Internet. De plus, si avez êtes victime de phishing et si vous avez saisi vos identifiants sur un faux site, et vous ne vous êtes peut être pas rendu compte. *Changer régulièrement vos mots de passe permet de bloquer tout intrus qui aurait pu avoir accès à vos comptes*.

5) Utilisez un gestionnaire de mots de passe

Les gestionnaires de mots de passe constituent l'une des rares solutions qui augmentent votre sécurité tout en vous simplifiant la vie. Notre préféré est LastPass. Il en existe d'autres mais évitez celui intégré à votre navigateur qui est bien moins sûr. À chaque fois que vous vous inscrivez sur un site, ou que vous vous identifiez pour la première fois, il vous propose de mémoriser votre identifiant et votre mot de passe. Ainsi, à chaque nouvelle connexion sur le site. le gestionnaire remplit automatiquement les champs.
L'avantage est que ce programme ne sera pas trompé par un faux site visuellement identique. Si l'adresse ne correspond pas, il n'affiche pas le mot de passe. Si vous cliquez sur un lien dans un message de phishing vous ne pourrez pas vous identifier automatiquement. Ceci bloque effectivement toute tentative de phishing, à l'exception de la modification du fichier HOSTS.
De plus, un gestionnaire de mots de passe permet de générer des mots de passe compliqués, et vous n'aurez pas à les mémoriser puisque Le logiciel s'en charge.

6) Utilisez un bon antivirus

Un Logiciel antivirus ne peut pas vous protéger contre les attaques de type phishing classiques. Il peut à la limite bloquer l'accès à certaines adresses web qui sont connues pour être de faux sites. mais les pirates en changent constamment. La plupart du temps. les sites utilisés dans les attaques ne sont en ligne que quelques jours. Les antivirus ne peuvent donc pas suivre. En revanche. l'antivirus peut vous protéger des infections d'un malware qui tenterait de modifier le fichier HOSTS. Windows Defender intégré à Windows 10 surveille en plus le fichier HOSTS et signale toute modification suspecte. Combinez-le à un gestionnaire de mots de passe et votre ordinateur devrait être bien protégé contre les faux sites

7) • Attention à ce que vous publiez sur les réseaux sociaux

Sur Internet, il faut considérer que toute information est publique et sera impossible à supprimer. Peu importe si votre profil n'est visible que par vos amis. Cela ne signifie pas que les informations contenues resteront confidentielles. Des bases de données de grands sites fuitent régulièrement et vous ne savez pas qui peut avoir accès vos informations. Pour les attaques ciblées, les auteurs utiliseront toutes les informations qu'ils peuvent trouver sur vous pour être crédibles et vous convaincre de cliquer sur leur lien, ou de leur donner d'autres informations. Vous avez sans doute déjà reçu un message suspect d'au moins un de vos contacts dont le compte a été piraté. L'intrus a pu accéder à toutes les informations du profil piraté, ainsi qu'à l'ensemble des publications et autres données de votre profil et des profils de ses autres contacts qui sont visibles des amis. Ainsi. aucune information ne peut être considérée comme privée dès lors qu'elle a été mise en ligne.