Guide de bonne pratique contre le phishing (pour les entreprises)

GUIDE ANSIE

Sommaire

Introduction

L'hameçonnage (phishing) est une technique frauduleuse qui consiste à voler des données d'utilisateur comme des identifiants de connexion, des informations de carte bancaire, voire de l'argent, en utilisant des méthodes d'ingénierie sociale (social engineering). Le phishing représente le premier vecteur d'attaque chez les entreprises, pour s'en prémunir, rien ne vaut l'organisation d'une campagne de sensibilisation au phishing.

Ce type d'attaque est généralement lancé par messages électroniques, semblant provenir d'une source fiable, dont le but est de persuader l'utilisateur d'ouvrir une pièce jointe malveillante ou de cliquer sur une URL frauduleuse.

I. Comment fonctionne le phishing ?

Qu'elles soient menées par e-mail, sur les réseaux sociaux, par SMS ou tout autre vecteur, toutes les attaques de phishing obéissent aux mêmes principes de base.

L'attaquant envoie un argumentaire ciblé visant à persuader la victime de cliquer sur un lien, de télécharger une pièce jointe, d'envoyer les informations requises ou même d'effectuer un paiement.

L'omniprésence des réseaux sociaux offre aux hameçonneurs l'accès à un nombre croissant d'informations personnelles de leurs cibles. Armés de toutes ces données, ils peuvent adapter leurs attaques aux besoins, aux désirs et aux situations de leurs cibles, ce qui rend leurs propositions bien plus alléchantes. Dans ces cas de figure, les réseaux sociaux alimentent une ingénierie sociale plus puissante.

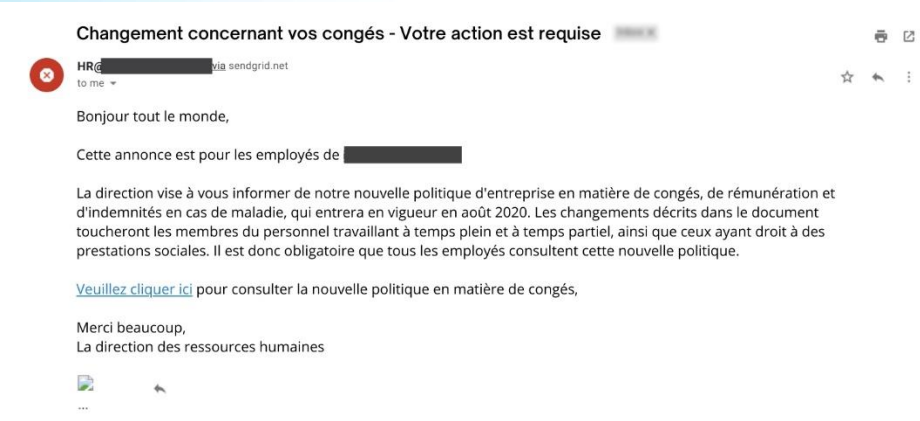
Le phishing profite du manque d'attention des utilisateurs et repose sur quatre principes :

- Usurper l'identité d'une organisation de confiance pour collecter les données personnelles des clients de cette organisation,
- Demander, sous un faux prétexte, de fournir des informations personnelles,
- Rediriger la victime vers un site Internet pirate mais identique au site Internet officiel de l'organisation usurpée pour que la victime saisisse les informations demandées,
- Exploiter les données collectées pour usurper une identité dans le but d'obtenir des avantages et services (argent, biens, papiers d'identité et documents administratifs).

II. Les types de phishing

1. Le spear phishing

Le spear phishing cible un groupe ou un type spécifique de personnes, par exemple l'administrateur système d'une entreprise. L'email ci-dessous est un exemple d'email de spear phishing. Notez l'attention portée au secteur dans lequel travaille le destinataire, le lien de téléchargement sur lequel l'assaillant demande à la victime de cliquer, et la réponse immédiate exigée.



Changement concernant vos congés - Votre action est requise

HR@[redacted] via sendgrid.net
to me

Bonjour tout le monde,

Cette annonce est pour les employés de [redacted]

La direction vise à vous informer de notre nouvelle politique d'entreprise en matière de congés, de rémunération et d'indemnités en cas de maladie, qui entrera en vigueur en août 2020. Les changements décrits dans le document toucheront les membres du personnel travaillant à temps plein et à temps partiel, ainsi que ceux ayant droit à des prestations sociales. Il est donc obligatoire que tous les employés consultent cette nouvelle politique.

Veuillez cliquer ici pour consulter la nouvelle politique en matière de congés,

Merci beaucoup,
La direction des ressources humaines

2. Le whaling

Le whaling est un type de phishing encore plus ciblé qui s'attaque généralement aux PDG, directeurs financiers ou autres directeurs de l'industrie ou d'une entreprise en particulier. Un email de whaling peut stipuler que l'entreprise du destinataire est poursuivie en justice et qu'il doit cliquer sur le lien afin d'obtenir plus d'informations.

Le lien vous conduit à une page où il vous est demandé de saisir des données essentielles sur l'entreprise, telles que le numéro d'identification fiscale et le numéro de compte bancaire.

3. Le smishing/vishing

Le smishing est une attaque qui utilise la messagerie texte ou SMS pour mener l'attaque. Une technique de smishing courante consiste à envoyer un message à un téléphone portable via un SMS contenant un lien cliquable ou un numéro de téléphone à rappeler.

Un exemple fréquent d'attaque de smishing est un SMS qui semble provenir de votre banque. Il vous indique que votre compte a été compromis et que vous devez réagir immédiatement. L'assaillant vous demande de vérifier votre numéro de compte bancaire, votre numéro de sécurité sociale, etc. Une fois que l'attaquant reçoit les informations, il peut contrôler votre compte bancaire.

Le but du vishing est le même que les autres types d'attaques de phishing. Cette attaque a lieu via un appel vocal. D'où le « v » à la place du « ph » dans son nom.

Une attaque de vishing fréquente consiste à recevoir un appel d'une personne qui prétend être un représentant de Microsoft. Cette personne vous indique qu'elle a détecté un virus sur votre ordinateur. On vous demande ensuite de fournir les informations de votre carte de crédit, pour permettre à l'assaillant d'installer une version mise à jour d'un antivirus sur votre ordinateur. L'assaillant dispose maintenant des informations relatives à votre carte de crédit et vous avez probablement installé un malware sur votre ordinateur.

III. Prevention contre tout type de phishing

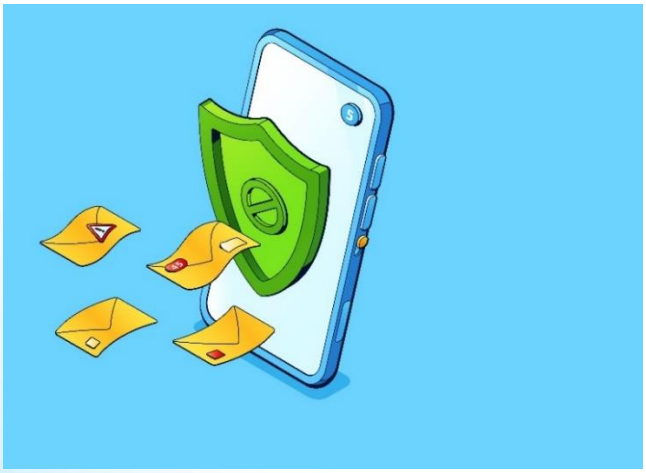
1. Marquer les courriels externes

Les employés doivent comprendre le risque que représentent les courriels externes. Bien qu'ils puissent être légitimes et provenir d'entités telles que des clients, des adresses électroniques personnelles d'employés, des vendeurs, des fournisseurs et des clients potentiels, la majorité des courriels de phishing proviennent d'adresses externes. Sur des plateformes telles que Microsoft Exchange ou Office365, il est possible de modifier la ligne d'objet ou le corps du texte d'une adresse électronique entrant dans l'organisation pour avertir le destinataire qu'il ne s'agit pas d'une communication interne et qu'elle peut être potentiellement malveillante. Ce simple avertissement peut faire réfléchir les employés avant d'interagir avec un courriel externe, par exemple en ouvrant une pièce jointe ou en cliquant sur un lien hypertexte.

2. Filtre anti-spam

Un filtre anti-spam est sans doute la défense la plus élémentaire qu'une entreprise puisse déployer pour réduire le nombre de spams et d'e-mails non sollicités qui atteignent les boîtes aux lettres des employés. Bien que certains courriels de phishing puissent toujours contourner cette défense, en réduisant le nombre de courriels qui ne sont pas liés à l'entreprise, les employés auront moins de pourriels

dans leurs boîtes aux lettres et signaleront moins de courriels à l'équipe de sécurité, qui pourra ainsi se concentrer sur les véritables courriels de phishing.



3. Le filtrage des pièces jointes

Ce n'est pas une bonne idée de bloquer purement et simplement les pièces jointes - les employés auront des difficultés à envoyer des documents légitimes en interne et en externe. La meilleure façon d'aborder cette situation est d'examiner quels types de fichiers sont souvent utilisés à des fins malveillantes, quels types de fichiers l'organisation traite régulièrement, et si leur blocage aurait un impact négatif sur l'entreprise. Les types de fichiers les plus évidents qui sont utilisés à des fins malveillantes sont les suivants :

.exe (exécutable)

.vbs (Visual Basic Script)

.js (JavaScript)

.iso (image de disque optique)

.bat (Fichier Batch Windows)

.ps/.ps1 (Scripts PowerShell)

.htm/.html (pages Web / langage de balisage hypertexte)

En général, les entreprises utilisent et envoient par courrier électronique les formats de fichiers suivants, qui peuvent également être utilisés à des fins malveillantes :

.zip (Archive)

.doc/.docx/.docm (fichier de document, souvent pour Microsoft Word)

.pdf (Portable Document Format)

.xls/.xlsx/.xlsm (fichier de feuille de calcul, souvent pour Microsoft Excel)

4. Technologie de sécurité du courrier électronique

Les technologies que nous allons couvrir sont SPF, DKIM et DMARC.

4.1. Enregistrements anti-falsification

Les enregistrements de domaine (DNS) peuvent être utilisés à des fins très diverses, par exemple pour permettre à un serveur de messagerie d'utiliser un domaine personnalisé, pour héberger un site web et pour permettre également de configurer des enregistrements anti-spoofing. Étant donné que de nombreuses cyber-attaques proviennent de courriels d'hameçonnage et d'usurpation d'identité, ces enregistrements de domaine aident à protéger les noms de domaine personnalisés contre l'exploitation par un attaquant. Les trois types d'enregistrements suivants : SPF, DKIM et DMARC ; peuvent être utilisés ensemble pour aider à renforcer la sécurité du service de messagerie d'une organisation.

4.2. Enregistrements SPF

Un enregistrement SPF (Sender Policy Framework) est un type d'enregistrement DNS (TXT) qui peut contribuer à empêcher la falsification d'une adresse électronique. Cet enregistrement est établi pour identifier les noms d'hôtes ou les adresses IP qui sont autorisés à envoyer des e-mails pour votre domaine personnalisé. Lorsqu'un enregistrement SPF est spécifié sur votre domaine, cela permet d'empêcher un acteur malveillant d'usurper votre domaine. L'enregistrement SPF TXT contient trois parties : la déclaration du type d'enregistrement, les adresses IP et les domaines externes qui peuvent envoyer des messages au nom de votre domaine, et une règle d'application.

4.3. Enregistrements DKIM

DKIM (Domain Keys Identified Mail) est une méthode d'authentification du courrier électronique qui vérifie de manière cryptographique si un courrier électronique a été envoyé par ses serveurs de confiance et n'a pas été altéré pendant la transmission. Le fonctionnement de DKIM est le suivant : lorsque le serveur de messagerie envoie un courriel, un hachage crypté du contenu du courriel est généré à l'aide d'une clé privée, puis il ajoute ce hachage à l'en-tête du courriel en tant que signature DKIM. Le serveur récepteur sera en mesure de vérifier si le contenu du courriel n'a pas été altéré en recherchant la clé publique correspondante dans les enregistrements DNS du domaine. Une fois que le serveur de messagerie récepteur a décrypté l'e-mail avec la clé publique, il calcule un nouveau hachage et vérifie si le hachage original et le hachage nouvellement généré correspondent pour garantir l'intégrité du message électronique.

4.4. Enregistrements DMARC

Domain-based Message Authentication, Reporting & Conformance (DMARC) est un protocole d'authentification, de politique et de rapport pour les courriels. DMARC est construit en grande partie à partir de concepts tirés de SPF et DKIM, mais il ajoute plusieurs améliorations à ces protocoles. Ce type d'enregistrement

permet au propriétaire du domaine de préciser ce qui doit se passer si les courriels échouent aux vérifications SPF et DKIM. Il existe trois options de base que le serveur de messagerie peut prendre : aucune, quarantaine et rejet.

5. Sensibilisation à la sécurité

Il est essentiel que les organisations prennent l'hameçonnage au sérieux et qu'elles organisent régulièrement des séances de sensibilisation des utilisateurs afin que chacun puisse détecter et signaler un courriel suspect lorsqu'il en voit un. Il existe deux façons principales de sensibiliser les utilisateurs à l'importance du phishing et à la manière de l'identifier rapidement.

5.1. Formation de sensibilisation

De préférence au cours du processus d'intégration (lorsqu'un nouvel employé rejoint une entreprise), les utilisateurs doivent suivre une formation en personne ou en ligne qui leur apprend à repérer les e-mails de phishing et les mesures à prendre (généralement les signaler à l'équipe de sécurité). Cette formation doit couvrir les éléments d'identification d'un e-mail de phishing, tels que :

- Venant d'une adresse d'envoi inconnue.
- Fautes de grammaire et d'orthographe.

5.2. Attaques de phishing simulées

Il est fréquent que les organisations soucieuses de sécurité lancent des attaques de phishing simulées contre leurs propres employés afin de déterminer l'efficacité de leur formation actuelle à la sécurité. Il existe un certain nombre de services de sécurité qui proposent des attaques de phishing en tant que service, et vous permettent de personnaliser l'e-mail qui sera envoyé aux boîtes aux lettres du domaine de l'organisation. Si l'utilisateur clique sur un lien "malveillant", il sera redirigé vers un site Web sûr (généralement détenu par l'entreprise qui mène l'attaque simulée) et sera informé qu'il vient de tomber dans un courriel de phishing. Les équipes de sécurité peuvent également surveiller le nombre de personnes qui leur signalent l'email de phishing, identifiant ainsi les employés qui

ont compris la formation et sont capables d'identifier les emails suspects. Ces événements doivent être organisés tous les quelques mois pour tester les employés et identifier ceux qui tombent systématiquement dans le piège des e-mails de phishing afin qu'ils puissent recevoir une formation supplémentaire.

IV. Comment réagir ?

La réponse immédiate correspond aux mesures que l'analyste enquêteur doit prendre une fois qu'il a identifié un courriel de phishing, de la détection à la conclusion de son rapport d'enquête. Ces étapes permettront de trier l'attaque et de prendre des mesures pour traiter le risque généré par les courriels malveillants qui ont été distribués avec succès dans les boîtes aux lettres des employés. Ces étapes sont les suivantes :

A. Récupérer une copie originale de l'e-mail de phishing.

B. Rassembler les artefacts de l'email de phishing

C. Informer les destinataires qui ont reçu le courriel

D. Examiner les artefacts malveillants pour recueillir des indicateurs de compromission qui peuvent être bloqués pour protéger l'organisation.

E. Prendre des mesures défensives

F. Remplir le rapport d'enquête, en documentant toutes les étapes ci-dessus.

1. Récupérer l'original de l'e-mail suspect

Une version originale de l'e-mail peut être obtenue en extrayant l'e-mail directement de la solution de messagerie, comme les serveurs Microsoft Exchange, ou en demandant à un employé de transférer l'e-mail vers une boîte aux lettres sécurisée.

2. Rassembler les artefacts du courriel original

Une fois que nous avons collecté et analysé les artefacts des e-mails, nous sommes en mesure de prendre des mesures défensives afin de bloquer les e-mails entrants et sortants qui présentent ces artefacts. Pour récapituler, les artefacts d'email qui sont importants pour nous incluent :

- Expéditeur de l'e-mail (mailbox@domain)
- Domaine de l'expéditeur (@domaine)
- IP du serveur d'envoi
- Ligne d'objet

3. Informer les destinataires du courriel

Une partie cruciale de la réponse immédiate à une attaque de phishing consiste à informer toutes les personnes qui ont reçu l'e-mail. Cela permet de réduire le risque qu'elles ouvrent l'e-mail et interagissent avec lui.

4. Analyse et investigation des artefacts

Nous avons déjà vu comment enquêter sur les artefacts basés sur les courriels, le Web et les fichiers pour recueillir plus d'informations et déterminer leur degré de malveillance. Les outils à utiliser comprennent le sandboxing de niveau entreprise, URL2PNG, VirusTotal, IPVoid, WannaBrowser, une machine virtuelle, etc.

5. Prenez des mesures défensives

Les mesures défensives sont les actions prises par l'équipe de sécurité pour réduire le risque généré par l'attaque de phishing. Il peut s'agir de bloquer les artefacts du courrier électronique, du Web et des fichiers. Si un courriel malveillant contient une URL qui conduit l'utilisateur à un collecteur d'informations d'identification, le blocage de cette URL sur un proxy Web empêcherait les employés de se connecter à la page Web, ce qui réduirait complètement le risque qu'ils saisissent leurs informations d'identification.

6. Remplir le rapport d'enquête

Votre rapport d'enquête comprendra des notes sur toutes les étapes que vous avez suivies pendant le processus de réponse immédiate. Il s'agit d'une piste d'audit qui montre que le courriel a été identifié, examiné et que des mesures défensives ont été prises pour protéger l'organisation contre cette attaque.

Conclusion

Dans l'ensemble, le phishing est réel et dangereux. Tout le monde doit y faire attention car cela arrive à tout le monde ; et se faire arnaquer peut coûter cher. Nous vous proposons en effet de tester les réflexes de vos salariés à travers un test de phishing. Nous pouvons même aller plus loin, en vous proposant une formation continue qui favoriser l'ancrage mémoriel et les bons réflexes de chacun sur le long terme.