Phishing dans l'enseignement primaire et secondaire

une introduction

Bonjour ! Voici le deuxième e-book de notre série sur la cybersécurité dans les établissements d'enseignement primaire et secondaire. Dans cette série, nous faisons un tour d'horizon des menaces de cybersécurité les plus courantes qui pèsent sur les établissements scolaires. **Notre premier épisode était consacré aux logiciels malveillants.**

Cette fois, nous parlons du **phishing**, ou hameçonnage. Et malheureusement, vous pouvez ranger votre canne à pêche.

jamf

DANS CET E-BOOK, NOUS ABORDONS :

Qu’est-ce que le phishing ?

Le terme de phishing est assez ancien, du moins à l’échelle de l’histoire d’Internet. Il est antérieur à l’invention du Wi-Fi et à des sites comme Google et Wikipédia. Comme la pêche à la ligne, le phishing utilise un appât pour attirer des personnes peu méfiantes dans un piège.

Le phishing est utilisé pour recueillir des informations bancaires, des identifiants de connexion ou des données personnelles identifiables (PII) – une date de naissance ou un numéro de sécurité sociale, par exemple. C’est la méthode d’attaque initiale la plus courante : elle représente 16 % des attaques de données, selon le rapport **Coût d’une violation de données 2023 d’IBM**. Son coût est considérable : il s’élève en moyenne à 4,76 millions de dollars pour l’organisation touchée.

Le phishing utilise quelques tactiques communes pour augmenter la probabilité que leur victime morde à l’hameçon :

L’urgence : les pirates exigent souvent une attention immédiate. Ils font planer la menace de la suppression d’un compte, de pénalités en cas de retard de paiement, de danger pour un proche ou d’autres conséquences négatives. Ils peuvent aussi faire appel à l’empathie de leur cible en prétendant être en détresse et demander de l’aide.

Les sosies : l’URL d’un site web peut ressembler étroitement à une URL authentique, à quelques caractères spéciaux près. Les pirates peuvent créer des sites web ou des e-mails très ressemblants pour imiter le site d’une banque ou un e-mail de réinitialisation de mot de passe, par exemple.

L’usurpation d’identité : les pirates peuvent se faire passer pour une personne que vous connaissez en utilisant son adresse e-mail, son numéro de téléphone ou même sa voix, ce qui augmente la probabilité que vous cédiez à la tentative de phishing.

S’ils utilisent ces méthodes d’ingénierie sociale, c’est pour une raison simple : elles nécessitent rarement de grandes compétences techniques. Après tout, il est beaucoup plus facile de manipuler quelqu’un pour qu’il vous donne ses identifiants que d’essayer toutes les combinaisons de mots de passe jusqu’à trouver la bonne.

Ingénierie sociale

L’ingénierie sociale est une technique de manipulation psychologique qui exploite les erreurs ou les faiblesses humaines pour obtenir des informations privées, des accès ou des contenus de valeur. On parle parfois de « piratage humain ».

Types courants d'attaques de phishing

Les attaques de phishing se présentent sous plusieurs formes. Examinons-en quelques-unes

PHISHING PAR E-MAIL

Le pirate envoie un e-mail à un grand nombre de personnes. Cet e-mail peut contenir une pièce jointe qui installe des logiciels malveillants ou un lien qui redirige vers un site web conçu pour dérober des identifiants de connexion.

PHISHING CIBLÉ

Le pirate vise cette fois des personnes spécifiques ou des petits groupes, le plus souvent par e-mail. Le message envoyé renferme un contenu familier pour la victime. Des élèves et des enseignants recevront par exemple un e-mail qui semble provenir d'un logiciel scolaire, mais dont les liens redirigent vers un site web malveillant.

WHALING

Ces attaques visent des personnalités importantes – le PDG d'une entreprise, par exemple. Le pirate peut se faire passer pour un partenaire commercial et demander de l'argent par virement bancaire. Il peut également se faire passer pour un recteur d'académie afin d'obtenir des informations auprès d'un directeur d'établissement.

ATTAQUE AU POINT D'EAU

L'attaque au point d'eau s'apparente au phishing ciblé, car ces deux techniques visent une cible spécifique. Mais dans l'attaque au point d'eau, l'adversaire ne commence pas par contacter ses victimes. Il va plutôt pirater un site web fréquenté par ses cibles et le modifier pour voler leurs données ou exécuter des logiciels malveillants.

USURPATION DE DNS

Lorsque vous saisissez l'adresse d'un site web dans votre navigateur, le logiciel du système de noms de domaine (DNS) traduit cette adresse en une série de chiffres. L'usurpation de DNS manipule le logiciel DNS en modifiant ces chiffres. De ce fait, lorsque vous tapez l'adresse correcte dans votre navigateur, le DNS compromis vous redirige vers le site du pirate dans l'espoir que vous y saisissiez vos identifiants.

SMISHING

Combinaison des termes « SMS » et « phishing », le smishing désigne l'hameçonnage par message texte. Il peut être difficile à repérer, car les liens inclus dans les SMS sont souvent raccourcis ou difficiles à prévisualiser.

Pensez également que les victimes utilisent souvent leur mobile lorsqu'elles sont pressées ou en déplacement : elles sont donc moins susceptibles de prendre le temps de vérifier le lien.

VISHING

Le vishing, contraction de « voix » et de « phishing », désigne une forme d'hameçonnage qui utilise la voix d'une personne. Il peut s'agir d'un inconnu au téléphone qui va faire appel à la gentillesse de ses cibles. Avec les progrès de l'intelligence artificielle (IA), un pirate peut même prendre la voix d'un proche qui vous demande instamment de lui envoyer de l'argent.

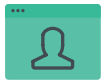
L’impact du phishing sur les établissements primaires et secondaires

Le K12 Security Information eXchange (K12 SIX) fournit aux écoles de précieux conseils en matière de cybersécurité. Dans sa carte des incidents, le K12 SIX répertorie les incidents de cybersécurité enregistrés par les établissements scolaires primaires et secondaires américains entre 2016 et 2022. Voici quelques exemples d’attaques de phishing dans le secteur de l’éducation :

Des enseignants ont reçu des e-mails contenant un lien de phishing qui a permis aux pirates de **détourner leurs virements bancaires** et de dérober plus de 50 000 $ de salaire.

Les pirates se sont fait passer pour des administrateurs et ont envoyé des e-mails au de la paie et des RH **pour demander les informations W-2 des employés**. Des victimes ont été recensées dans plusieurs écoles.

Un pirate s’est fait passer pour un prestataire du district et a convaincu le personnel de ce district de **transférer 2,9 millions de dollars sur son compte**. Fort heureusement, la somme a été récupérée.



Un élève a lancé une attaque de phishing ciblé : il a créé un compte e-mail semblant appartenir à un membre haut placé de l’administration afin de demander des identifiants de connexion à plusieurs enseignants. Il a ensuite utilisé ensuite ces informations pour améliorer ses notes et faire baisser celles des autres étudiants.

Un enseignant a répondu à l’e-mail d’**un pirate qui s’est fait passer pour son collègue** et lui a demandé 500 dollars en cartes-cadeaux.

Ces attaques ont un point commun : un e-mail qui semble provenir d’une source fiable. Les e-mails proviennent d’adresses quasiment identiques à celles qu’elles imitent, voire parfois d’un véritable compte professionnel qui aura été compromis.

Si ces attaques visent principalement le corps enseignant et le personnel, les données des étudiants sont également touchées. Le phishing est une première étape courante dans les attaques de ransomware, qui entraînent des violations de données capables de hanter les étudiants pendant de longues années. Les pirates peuvent en effet utiliser les informations d’un étudiant pour contracter des prêts ou ouvrir des comptes de carte de crédit, pour ne citer que deux exemples. Ces étudiants, souvent jeunes, ignorent qu’ils devront vérifier leur rapport de solvabilité pendant de nombreuses années après l’attaque.

PRÉVENTION DU PHISHING

Le phishing peut être difficile à prévenir. Quelles que soient les défenses mises en place par les écoles, il suffit qu'une seule personne communique ses identifiants à un pirate.

Mais tout espoir n'est pas perdu !

Les écoles peuvent lutter contre la menace omniprésente du phishing.

Sensibilisation des utilisateurs

Le phishing reposant souvent sur l'ingénierie sociale, des utilisateurs capables d'identifier ces tentatives de manipulation forment la première ligne de défense. En effet, si les utilisateurs ne cliquent jamais sur des liens trompeurs, ne téléchargent pas de pièces jointes malveillantes et n'obéissent pas aux demandes des attaquants, les attaques de phishing échouent les unes après les autres.

Conseil :

Faites entrer la sensibilisation au phishing dans la salle de classe !

Voici quelques thèmes à aborder :

Qu'est-ce que le phishing ?

Le phishing est une forme d'escroquerie dans laquelle les pirates usurpent une identité dans le but de recueillir des informations privées. Ils peuvent se faire passer pour un ami, un membre de la famille, un collègue ou une personne d'autorité. Ils peuvent aussi se faire passer pour votre banque, une entreprise chez qui vous avez un compte (Google, Apple ou Microsoft, par exemple) ou une institution susceptible de détenir vos informations. Le phishing se fait généralement par e-mail, mais les pirates peuvent aussi utiliser les SMS, les réseaux sociaux, le téléphone, voire une conversation en personne. Les pirates n'ont pas toujours besoin de vous contacter directement : **ils peuvent publier un contenu trompeur sur un réseau social** en usurpant le compte de l'un de vos amis.

Que faire si vous soupçonnez une tentative de phishing ?

Si vous recevez un e-mail suspect, la première chose à faire est de **ne pas cliquer sur quoi que ce soit** – ni sur les liens, ni sur les pièces jointes. S'il semble provenir de l'école, signalez-le à votre service informatique. Certaines écoles proposent un bouton qui vous permet de le faire en un clic.

À quoi ressemble le phishing ?

Une attaque par phishing peut utiliser l'e-mail, les messages directs, le SMS, le téléphone, un site web ou une rencontre en personne. Il n'y a pas deux attaques identiques, mais certains signes méritent votre vigilance :

- Vous recevez un message ou un appel d'une personne que vous connaissez à une heure étrange du jour ou de la nuit.
- Le message induit un sentiment d'urgence, en demandant un paiement rapide ou en évoquant une situation critique.
- L'adresse e-mail ou l'URL du site web ressemblent **beaucoup** à des adresses que vous connaissez, mais présentent des erreurs discrètes. Elles comportent des caractères spéciaux, ou bien certains caractères ont été remplacés (« 0 » à la place de « o », par exemple). Sachez que certaines attaques de phishing utilisent une adresse e-mail parfaitement légitime : les pirates sont simplement parvenus à prendre le contrôle du compte de messagerie.
- Le message est trop beau pour être vrai : par exemple, il vous suffit de donner quelques informations pour recevoir une carte-cadeau de 100 $!
- La demande est inattendue : par exemple, un « ami » vous écrit pour vous demander votre adresse, votre date de naissance ou d'autres informations personnelles.

Filtrage de contenu

Malheureusement, la sensibilisation des utilisateurs a ses limites. Personne n'est infaillible, et il suffit d'une seule tentative réussie pour créer une faille. C'est là que le filtrage du contenu peut s'avérer utile.

Pour dire les choses simplement, le filtrage de contenu bloque l'accès aux sites web malveillants. Par exemple, si un utilisateur commet une erreur et clique sur un lien de phishing dans un e-mail, le filtre de contenu le reconnaît et bloque l'ouverture du lien.

Le filtrage peut s'effectuer de plusieurs manières. L'une des solutions consiste à établir une liste d'autorisations et de blocages : les administrateurs informatiques autorisent ou bloquent explicitement une sélection de sites web. C'est assez efficace, mais l'approche la plus sûre consiste à créer une petite liste d'autorisations, ce qui revient à bloquer des pans considérables d'Internet. Cette méthode empêche les élèves d'explorer librement cet Internet auquel ils auront accès lorsqu'ils auront quitté l'école.

Le filtrage de contenu est une bien meilleure méthode. Il utilise l'intelligence artificielle (IA) et le machine learning (ML). Au lieu de réduire l'internet à une poignée de sites web, l'IA et le ML peuvent déterminer intelligemment si un site est sûr sans qu'un administrateur informatique n'ait à l'autoriser ou à le bloquer explicitement. Cela permet d'autoriser l'accès à une plus grande partie du Web tout en bloquant les sites web menaçants, y compris ceux qui n'ont pas encore été découverts. Cette approche donne aux élèves la liberté d'explorer Internet à l'abri de garde-fous. **Elle leur offre également la possibilité d'apprendre à devenir des citoyens numériques prudents longtemps après la fin de l'école.**

Authentification unique (SSO)

L'authentification unique (SSO) permet aux utilisateurs de se connecter sans avoir à mémoriser un mot de passe pour chacun de leurs comptes. Elle peut même être configurée de manière à ce qu'ils puissent se connecter à l'aide de leur empreinte digitale. Il vous suffit de vous souvenir de votre mot de passe SSO : votre fournisseur SSO vous connectera à tous vos autres comptes.

C'est un bon moyen de prévenir le phishing. La SSO ne fonctionne que pour les sites web et les comptes qui ont été enregistrés. Si vous cliquez sur un lien de phishing, votre fournisseur SSO ne reconnaîtra pas le site web et ne transférera aucune de vos informations aux pirates. La SSO peut demander une empreinte digitale à titre de facteur d'authentification supplémentaire. Cela complique encore la tâche des pirates qui veulent se connecter à votre compte.

Gestion des appareils

La gestion des appareils est un élément essentiel de la sécurité d'un établissement scolaire. En inscrivant tous les appareils qui accèdent aux ressources de l'école dans une solution de gestion des appareils mobiles (MDM), les administrateurs informatiques bénéficient d'une grande visibilité sur leur niveau de sécurité.

Pour qu'un appareil puisse bénéficier d'une fonction telle que le filtrage de contenu, il doit d'abord s'inscrire dans la solution MDM. C'est elle qui donne aux administrateurs le pouvoir de configurer les appareils, d'appliquer certains réglages ou d'activer le filtrage de contenu.

L'authentification multifacteur

L'authentification multifacteur (AMF) est un excellent moyen de réduire les chances de réussite du phishing. L'AMF exige au moins deux méthodes d'authentification parmi les catégories suivantes :

- **Une information que vous connaissez,** comme un mot de passe, un code PIN ou une question de sécurité
- **Une caractéristique de ce que vous êtes,** comme votre empreinte digitale ou votre visage
- **Un objet que vous possédez,** comme un autre appareil ou une clé de sécurité

Par exemple, vous saisissez votre mot de passe (une information que vous connaissez) et vous recevez un message texte contenant un code à six chiffres sur un appareil de confiance (un objet que vous possédez).

Voici un scénario dans lequel l'AMF serait utile :

1. Vous recevez un e-mail vous invitant à accéder à un document Google partagé. (Vous ne vous rendez pas compte qu'il s'agit d'un e-mail de phishing !)

2. Vous cliquez sur le lien, qui vous amène sur un site ressemblant à la page de connexion de Google.

3. Vous saisissez vos informations, mais vous n'êtes jamais redirigé vers un document.

4. Les pirates ont dérobé vos informations ! Plus tard, ils essaient de se connecter à votre compte.

5 Vous recevez une notification de l'AMF qui vous demande d'approuver la demande de connexion.

6. Comme la demande provient d'une localisation inconnue ou intervient à un moment où vous n'essayez pas de vous connecter, vous la refusez.

Les pirates ne parviennent pas à accéder à votre compte.

Ce **type de phishing** n'a rien d'hypothétique : il a même été utilisé à maintes reprises. Dans un contexte scolaire où la collaboration est fréquente, il est facile de tomber dans le piège, car ce type d'e-mail est courant et personne ne sera surpris de le recevoir.

MISE EN ŒUVRE : JAMF SCHOOL ET JAMF SAFE INTERNET

Nous avons évoqué plusieurs moyens de prévenir le phishing. Parlons maintenant de leur mise en œuvre.

Jamf School

En ce qui concerne la gestion des appareils, **Jamf School** est une solution MDM spécialement conçue pour les établissements scolaires. Elle réunit un large éventail de fonctions :

- Inventaire des appareils, pour que les administrateurs sachent quels appareils sont connectés aux ressources de l'école.
- Visibilité totale sur l'état des appareils, afin de résoudre rapidement le moindre problème
- Possibilité de définir des restrictions et d'appliquer des réglages sur un appareil, notamment pour exiger la création d'un code secret
- Compatibilité avec la SSO (avec un fournisseur d'identité supplémentaire)
- Un moyen simple pour les enseignants de demander des applications au service informatique
- Et bien d'autres encore !

Les capacités de gestion de Jamf School créent une base solide pour sécuriser les appareils. La SSO et la configuration des appareils peuvent atténuer l'impact d'une tentative de phishing.

Jamf Safe Internet

Jamf Safe Internet apporte une couche de sécurité supplémentaire et est compatible avec les appareils Apple, Chromebook et Windows. Entièrement personnalisable, Jamf Safe Internet permet de définir et modifier facilement des règles qui vont s'appliquer à différents groupes d'appareils en fonction de leur situation géographique, de leur type ou d'autres attributs. Cet outil fonctionne avec tous les types d'appareils : poste informatique mobile, appareil scolaire individuel et appareils personnels utilisés à l'école.

Pour se défendre contre des menaces comme le phishing, Jamf Safe Internet propose :

- **Un filtrage de contenu puissant** enrichi par IA et ML, qui bloque l'accès aux sites web de phishing avant même qu'ils ne soient identifiés comme malveillants.
- **Le blocage des DNS et des noms de domaine** pour se défendre contre l'usurpation de DNS
- **Le filtrage de contenu sur l'appareil** (iPad) pour un filtrage effectif partout
- **La protection sur le réseau** qui bloque les sites web malveillants avant qu'ils ne puissent nuire aux appareils.
- **L'application de Google SafeSearch** et Google Safe Browsing pour empêcher les sites malveillants ou inappropriés d'apparaître dans les recherches.

Sécurité **sans surveillance :** les élèves sont libres de naviguer sur Internet et de développer leur citoyenneté numérique sans exposer leur vie privée.