SAE11 – Le phishing

RANDRIANASOLO Andy-Maël,
LOURAIBI Anas,
VIRMAUX Bastien

Sommaire

1. Qu’est ce que le phishing

Le phishing ou hameçonnage en français est l’une des arnaques les plus anciennes et les plus connues d’internet. L’objectif principal est d’amener des utilisateurs à révéler des informations confidentielles comme des coordonnées bancaires, des informations de connexion… dans le seul but de gagner de l’argent en les exploitant.

Le phishing peut s’adresser autant aux particuliers comme aux entreprises le point commun entre ces deux types et l’argent et les données personnelles qui peuvent être une vraie mine d’or pour les malfaiteurs.

Le phishing se décline en plusieurs types, ici nous vous citerons seulement les

déclinaisons les plus répandues dans le monde telles que :

- **Le phishing par mail** : Elle a pour but d'envoyer un mail frauduleux bien structuré qui est envoyé pour usurper l'identité d'une organisation légitime.
- **Spear phishing** : Elle a pour but de cibler une victime précise en collectant au paravent des informations publiques sur celle-ci afin qu'elle tombe plus facilement dans l'arnaque et donc de pouvoir créer une relation de confiance pour ensuite lui dérober des informations privées.**(Utilisé contre les entreprises ⇒ FOVI)**
- **Phishing par site web**: Elle a pour but d'usurper un site web afin que des personnes naïves rentrent leurs informations confidentielles sur celui-ci. Il est souvent en lien avec le phishing par mail.

Souvent, ces 3 types d'arnaques sont rassemblés ensemble.

---

2. Les procédés du phishing

Après avoir compris le but du phishing et les déclinaisons qui existent de cette arnaque, on peut se demander comment les arnaqueurs procèdent pour mettre en place ce genre de mode opératoire.

Procédons par étape :

1️⃣ **Rechercher des informations**
Pour convaincre une victime de cliquer sur un lien, il cherche d'abord des informations publiques sur celle-ci.
Dans le cas d'une entreprise, il peut arriver qu'un malfaiteur observe pendant plusieurs mois ce qui se passe sur les emails des entreprises pour ensuite mettre en place l'arnaque.

2️⃣ **Préparer sa fraude**
Il crée un site internet qui usurpe un service tel que Netflix, Amazon,… il fait attention d'héberger son site internet chez des hébergeurs qui ne regarde pas le contenu et crée un mail avec les informations retrouvées dans **l'étape 1**.

3️⃣ **Envoyer sa fraude**
Avec la recherche d'informations faites au préalable, le malfaiteur est en capacité d'envoyer la fraude via l'adresse e-mail, mais aussi via les messages
⚠️ Nous verrons, que cette partie est automatisée à l'aide de d'autres actions malveillantes

4️⃣ **Inciter la victime à agir**
Pour que la victime fasse l'action, le malfaiteur doit rendre le mail le plus crédible possible en intégrant la peur, la frustration, l'urgence.

5️⃣ **Le point de non retour**
Une fois que la victime a entré ces informations confidentielles, le malfaiteur peut décider de les utiliser, mais le plus souvent il regroupe les informations de plusieurs victimes dans plusieurs fichiers et les vende sur internet à d'autres cybercriminels qui utiliseront ces informations pour faire des choses illégales.

En seulement **4 étapes**, une personne malveillante peut récupérer vos informations et les utiliser à votre insu.

Dans le monde moderne, ce genre de pratique est automatisé à l'aide des nombreuses fuites de données des grosses entreprises, mais aussi via des tests en force pour vérifier que la personne a bien un email ou un numéro de téléphone enregistré dans l'entreprise pour paraître plus crédible.

> **Exemple :** Pour éviter d'envoyer des e-mails à des personnes n'ayant pas de compte Amazon, les malfaiteurs testent dans la page d'inscription des milliers d'emails à l'aide de programmes automatisés, si Amazon répondait correctement à la requête alors l'adresse mail était ajoutée à une liste d'emails enregistrés.

---

3. Exemples et chiffres clés du phishing

Aujourd'hui, dans le monde il existe beaucoup de services (banques, réseaux sociaux, etc…) qui se font usurper leurs apparences visuelles pour tromper l'utilisateur et récupérer leurs informations personnelles.

En effet, il y a quelques exemples de phishing connus et utilisés fréquemment :

- **Banque**
  - Il est très fréquent d'y trouver des attaques par hameçonnage visant les sites bancaires, car ce sont ces services qui stockent l'argent de toute une population.

PeyPal

Accès fraduleux

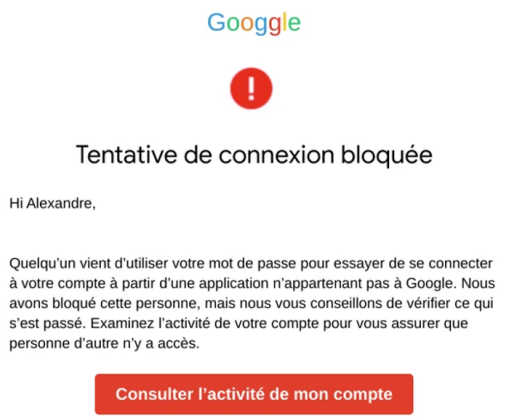
Bonjour,

Nous avons interdit l'accès à votre compte pour la raison suivante.
Votre dernière tentative de connexion a échoué depuis l'adresse IP suivante :
9 rue des cerisiers, 75100, Paris, Île-de-France
Pour être sur que vos informations restent protégées contre les menaces, cliquez sur le bouton "Vérifier mon compte"

Chez PayPal, votre sécurité est notre priorité absolue.

Vérifier mon compte

- **Réseaux sociaux**
  - Avec la montée d'utilisateurs de réseaux sociaux, les pirates ont trouvé une nouvelle source de données à exploiter en effet beaucoup de profils contiennent des informations privées à exploiter pour gagner de l'argent voire même reprendre le contrôle d'un compte afin de faire circuler d'autres arnaques avec l'image d'une personne lambda.



- **Entreprise**
  - Depuis 2010, un nouveau type d'hameçonnage s'est créé dans le monde de l'entreprise. Il s'agit d'un **FOVI (Faux Ordres de Virements)**. Le but est de se faire passer pour un dirigeant d'entreprise ou un prestataire qui demande un virement bancaire par mail, pouvant s'élever à des millions d'euros fondés sur le principe qu'une grosse entreprise fait énormément de virements bancaires, mais vérifie plus vers qui. (le FOVI est bien du phishing, il trompe l'entreprise en se faisant passer pour une autre)

> La personne ayant mis en lumière cet arnaque s'appelle **Hushpuppi** (Ramon Abbas).

Maintenant que nous avons quelques exemples de phishing, voyons quelques chiffres concrets :

Nombre d’américains qui ouvrent des e-emails de phishing.(35-44ans)

38,80 %

(Src : Verizon)

Nombre d’américains qui ouvrent ensuite les liens ou les pièces jointes.

39,12%

(Src : Verizon)

En **2020**, Nombre d’utilisations des noms de marques pour capturer des informations sensibles par les sites de phishing.

55 %

(Src : F5 Labs Phishing and Fraud Report)

En **2021**, représentation de la violation de données causée par le phishing.

22 %

(Src : IC3 Report du FBI)

En **2021**, **74%** des entreprises au États-Unis et **73%** au Royaume-Uni ont déclaré avoir été victimes du phishing.

(Src : GraphUs)

Nombre d’emails concernés par le phishing dans le monde

3 milliards

(Src : Valimail)

4. Comment s’en protéger et réagir ?

Pour se protéger du phishing, il n’existe pas de logiciel miracle qui permet de bloquer à 100 % le phishing toutefois voici une liste des signes qui doivent vous alerter :

- **Email d’un service ou d’une société dont vous n’êtes pas client**
- **Nom d’expéditeur inhabituel**
- **Adresse d’expédition fantaisiste**
- **Objet d’email trop alléchant ou alarmiste**
- **Une apparence suspecte**
- **Absence de personnalisation**
- **Demande inhabituelle**
- **Demande d’informations confidentielles**
- **Message aguicheur ou inquiétant**
- **Fautes de français/langue surprenantes**
- **Incitation à cliquer sur un lien ou une pièce-jointe**

Comme vu précédemment dans les exemples, il existe plein de raisons plus farfelues les unes des autres pour essayer de récupérer des informations personnelles… voici quelques demandes qui doivent vous alerter :

- **Mise à jour ou de confirmation de données personnelles**
  - Maintenant, les grandes entreprises vous demandent directement sur leurs sites officielles, JAMAIS PAR MAIL ou MESSAGE
- **Défaut de paiement ou problème de facturation**
  - Jamais une entreprise hormis certaines comme les services VOD ne vous informera d’un défaut de paiement par mail, le plus souvent ces informations sont distribuées par voie postale.
- **Demande d’informations inattendue**
  - Une entreprise ne demandera jamais par mail de rentrer vos informations de connexion dans le cadre d’un remboursement, livraison…
- **Demande d’informations contre l’envoi d’un cadeau**
- **Appel à l’aide**

    - Un cybercriminel se fait passer pour une personne qui se trouve dans une situation compliquée et vous demande de l'argent (très fréquent sur les Réseaux Sociaux)

Si vous émettez toujours un doute avec les conseils énumérés juste au-dessus le site cybermalveillance.gouv.fr donne des conseils supplémentaires pour vérifier l'intégrité d'un mail :

- **Avant de cliquer, survoler le lien**
    - (sans cliquer) Ce qui affichera alors l'adresse vers laquelle il pointe réellement afin d'en vérifier la vraisemblance ou aller directement sur le site de l'organisme en question par un lien favori que vous aurez vous-même créé.
- **Vérifier l'adresse du site que s'affiche dans votre navigateur**
    - Si cela ne correspond pas exactement au site concerné, c'est très certainement un site frauduleux. Parfois, un seul caractère peut changer dans l'adresse du site pour vous tromper. Au moindre doute, ne fournissez aucune information et fermez immédiatement la page correspondante.
- **En cas de doute, contactez si possible directement l'organisme concerné**
    - Connectez-vous en saisissant l'adresse officielle dans la barre d'adresse de votre navigateur.

Toutefois, il existe quelques outils sur internet pour bloquer les e-mails de phishing comme :

- **Altospam**
- **Bitdefender**
- **MailWasher**

Leurs fonctionnements varient en fonction de chacun toutefois le **mode de blocage le plus répandu et le système de liste noire, liste banche**. Il a pour principe de bloquer certains expéditeurs par leur adresse e-mail ou adresse IP, mais les malfaiteurs changent régulièrement d'e-mail qui rend la tâche de ces outils beaucoup plus complexe.

Pour protéger vos comptes, activer aussi, si possible la double authentification, pour avoir une notification de connexion.

Après avoir vu qu'est-ce que le phishing ? Les procédés du phishing, les exemples et chiffres du phishing on peut se demander si les gouvernements et entreprises y font quelque chose.

Dans le cas de la France, plusieurs lois interdisent les actions effectuées par le phishing telles que :

- **Article 313-1 du Code pénal**, escroquerie
- **Article 226-18 du Code pénal**, Collecte de données à caractère personnel par un moyen frauduleux, déloyal ou illicite
- **Article 323-1 du Code pénal**, Accès frauduleux à un système de traitement automatisé de données
- **Article 226-4-1 du Code pénal**, Usurpation d'identité
- **Article L163-3 et L163-4 du Code monétaire et financier**, Contrefaçon et usage frauduleux de moyen de paiement
- **Article L.713-2 et L.713-3 du Code de la propriété intellectuelle**, Contrefaçon des marques

Malheureusement, dans seulement de très rares cas la justice condamne un malfaiteur, car ils sont souvent basés dans d'autres pays comme l'Afrique plus précisément en Côte d'Ivoire. **Toutefois, il existe un site internet développé par l'État français qui permet de signaler si vous êtes victime de phishing : signal-spam.fr**.

Dans le cas des entreprises, **Google** met tout en œuvre afin de bloquer les mails et sites de phishing, ils ont mis en place un outil pour que les utilisateurs puissent signaler les sites web : **safebrowsing.google.com,** mais les sites web usurpés qui aident à la pratique toutefois les malfaiteurs utilisent énormément de techniques pour éviter que leur site web soit analysé par les robots du moteur de recherche.

5. Bibliographie

1. Qu’est-ce que le phishing ?
    a. www.avast.com (https://www.avast.com/fr-fr/c-phishing#:~:text=Le phishing (ou hameçonnage) est,la part de leurs victimes)
2. Les procédés du phishing
    a. www.avast.com (https://www.avast.com/fr-fr/c-phishing#:~:text=Le phishing (ou hameçonnage) est,la part de leurs victimes)
3. Exemples et chiffres clés du phishing
    a. **Wikipédia**
    b. **blog-usecure.io**
    c. **Image : Internet**
4. Comment s’en protéger et réagir ?
    a. **www.economie.gouv.fr** (https://www.economie.gouv.fr/particuliers/phishing-hameconnage-filoutage)
    b. **www.signal-spam.fr** (https://www.signal-spam.fr/)
    c. **safebrowsing.google.com** (https://safebrowsing.google.com/safebrowsing/report_phish/?hl=fr)
    d. **www.it-connect.fr (**https://www.it-connect.fr/protection-anti-phishing-google-chrome-va-proteger-tous-les-utilisateurs-en-temps-reel/)
    e. **www.cybermalveillance.gouv.fr** (https://www.cybermalveillance.gouv.fr/tous-nos-contenus/fiches-reflexes/hameconnage-phishing)
    f. **www.cyberpreventys.com** (https://www.cyberpreventys.com/conseils-informatique-cybersecurite/comment-fonctionne-logiciel-antispam/#:~:text=L'antispam est un logiciel,des données de l'entreprise)

🧑‍🎓 **RANDRIANASOLO Andy-Maël,**
LOURAIBI Anas,
VIRMAUX Bastien

SAE11 – Le phishing