SÉCURITÉ DES SYSTÈMES D'INFORMATION AU SEIN DE L'UNIVERSITE

-

L'HAMEÇONNAGE

(« PHISHING » EN ANGLAIS)

R. ARON

RESPONSABLE DE LA SECURITÉ DES SYSTÈMES D'INFORMATION (RSSI)

Aix*Marseille université

INTRODUCTION

Ce document a pour objectifs de présenter « l'Hameçonnage » (« Phishing » en anglais) :

- Qu'est-ce que l'hameçonnage ?

- Quels sont les différents types d'hameçonnage ?

- Comment repérer qu'un courriel est une tentative d'hameçonnage ?

- Quels sont les buts recherchés par les pirates (Hackers) ?

- Quelles sont les conséquences potentielles pour l'utilisateur ?

- Quelles sont les conséquences potentielles pour l'établissement ?

- Comment réagir face à un courriel d'hameçonnage ?

Qu'est-ce que l'Hameçonnage (Phishing en anglais) ?

L'hameçonnage est l'action de leurrer des personnes afin d'obtenir d'elles des informations qui permettront ensuite à des « pirates » (« hackers » en anglais) de les utiliser à diverses fins illégales.

Le mot « phishing » provient de la contraction de deux mots anglais :

- « phreaking », désignant le piratage de cartes téléphoniques aux Etats-Unis dans les années 1970,
- « fishing », désignant l'action de pêcher.

Ce qui a conduit l'Office québécois de la langue française à proposer le terme « hameçonnage » pour désigner cette action, en 2004.

Quels sont les différents types d'hameçonnage ?

L'hameçonnage utilise différents canaux :

- L'envoi de courriels (à des destinataires ciblés ou non),
- Le contact téléphonique,
- Parfois (rarement) l'échange de documents sous forme papier.

Comment repérer qu'un courriel est une tentative d'hameçonnage ?

L'hameçonnage utilise différents canaux :

- L'adresse de l'émetteur n'est pas, en général, en « univ-amu.fr »
- Le lien internet sur lequel il invite à cliquer, n'est pas en « univ-amu.fr »
- Le message demande des informations de type :
    - Identifiant, mot de passe,
    - Numéro de carte bancaire, cryptogramme etc.

Quels sont les buts recherchés par les pirates (Hackers) ?

Phase 1 : La récupération d'identifiants permettant de se connecter sur des ressources web :

- Espaces personnels ou professionnels,
  - Comptes bancaires,
  - Réseaux sociaux,
  - Stockage en ligne…
- Espaces professionnels,
  - Environnement Numérique de Travail,
  - Bases de données professionnelles de l'établissement,
  - Réseaux sociaux…

Quels sont les buts recherchés par les pirates (Hackers) ?

Phase 2 : L'exploitation de ces ressources web :

- Utilisation directe
  - Coordonnées bancaires (ex. achat sur internet ou confection de cartes doublons)
  - Compte d'utilisateurs de divers espaces internet
- Vente de listes sur le « darknet »
  - Coordonnées bancaires,
  - Compte d'utilisateurs/administrateurs d'ordinateurs personnels ou de serveurs (ex. vente de grappes réseaux de PC « Zombies » : pour réaliser des attaques en déni de service contre des sites web ciblés),
  - Compte d'utilisateurs de divers espaces internet (ex. récupération d'informations pour revente : liste de coordonnées de personnels, de clients etc.)

Quelles sont les conséquences potentielles pour l'utilisateur ?

Du point de vue personnel :

- **Problèmes bancaires : débits indus à récupérer, agios, blocage de compte…**

- **Problèmes sociaux :**
  - Faux courriels envoyés avec l'identité de l'utilisateur piraté (ex. à des personnes présentes dans le carnet d'adresses)
  - Usurpation d'identité sur les réseaux sociaux avec diffusion de messages et de fichiers multimédias indésirables), avec parfois suspension voire fermeture du compte utilisateur par le réseau social en question, suite à la diffusion d'informations « ne correspondant pas à sa charte d'utilisation ».
  - Informations personnelles révélées à des personnes ciblées ou bien à tout internet.

- **Problèmes administratifs :**
  - Usurpation d'identité : prouver qui l'on est et qui a fait quoi à notre place.
  - Résoudre les problèmes causés par l'usurpateur.

Quelles sont les conséquences potentielles pour l'utilisateur ?

Du point de vue professionnel :

- **Problèmes bancaires (artisants, entreprises) : débits indus à récupérer, agios, blocage de compte…**

- **Problèmes sociaux vis-à-vis des clients / utilisateurs :**
  - Faux courriels envoyés avec l'identité de l'utilisateur/entreprise piraté(e) (ex. à des personnes présentes dans le carnet d'adresses ou les bases de données du système d'information,
  - Usurpation d'identité sur les réseaux sociaux avec diffusion de messages et de fichiers multimédias indésirables), avec parfois suspension voire fermeture du compte utilisateur par le réseau social en question, suite à la diffusion d'informations « ne correspondant pas à sa charte d'utilisation ».

- **Problèmes vis-à-vis de l'employeur :**
  - Ex. dénigrement de l'employeur ou de collègues de travail sur un réseau social par un « pirate » ayant usurpé l'identité d'un utilisateur (perte d'emploi possible).

- **Déficit d'image commerciale et de sérieux vis-à-vis des clients / utilisateurs :**
  - Faux courriels envoyés avec l'identité de l'utilisateur/entreprise piraté(e) (ex. à des personnes présentes dans le carnet d'adresses ou les bases de données du système d'information,
  - Fausses informations diffusées sur des sites web ou par courriels en nombres.

Quelles sont les conséquences potentielles pour l'établissement ?

- **Problèmes de Sécurité des Systèmes d'Information (SSI) :**
  - Perte de : Disponibilité, Intégrité, Confidentialité, Traçabilité concernant les informations contenues dans les bases de l'établissement : l'établissement pourrait, dans le pire des cas, devoir fermer ses portes car il serait bloqué dans son fonctionnement (scolarité ne pouvant plus gérer les étudiants, service RH bloqué car ses données ne seraient plus fiables etc.).
- **Problèmes juridiques :**
  - Responsabilités devant l'Etat (gestion et confidentialité notamment), responsabilités vis-à-vis des usagers, responsabilités vis-à-vis des personnels (divulgation d'informations concernant les personnels, non-paiement des salaires etc.)
- **Perte d'image :**
  - Au niveau :
    - Scientifique,
    - Attractivité vis-à-vis des étudiants et des personnels,
    - Politique (perception de l'établissement par l'Etat)
- **Perte financière :**
  - Issue des problèmes évoqués ci-dessus.

Comment réagir face à un courriel d'hameçonnage ?

La conduite à tenir est simple :

- Ne jamais y répondre,
- Ne pas cliquer sur les images (affichées ou non affichées sous forme de cadres).

En effet, cela pourrait permettre aux pirates d'identifier votre ordinateur, l'exposant d'autant plus aux attaques informatiques par la suite.

Pour rappel :

Aucun service de l'université ne vous demandera d'information personnelle (notamment nom de connexion ou login, mot de passe), par courriel.

Comment réagir face à un courriel d'hameçonnage ?

<u>En cas de besoin d'information</u> :

Un service de l'université vous contacterait directement

afin que vous vous présentiez physiquement dans ses locaux

ou bien que vous lui transmettiez des documents par courrier interne.

<u>Lorsqu'un agent a répondu, par erreur, à ce type de sollicitation</u> :

Il est nécessaire qu'il modifie immédiatement son mot de passe

en utilisant l'application "Sesame" accessible depuis l'ENT.

La DOSI de campus de son site de rattachement peut lui apporter de l'aide

si nécessaire.