PLOUZENNEC Eliaz

Compte rendu : LE PHISHING

29/11/23

Contenu

Introduction :

Le phishing est présent partout, c'est une des arnaques les plus rependus sur internet, maintenant on va étudier le phishing pour pouvoir en connaitre plus, ainsi le reconnaitre et s'en défendre. On va étudier ses formes, ses risques, comment en faire pour l'étudier, et ce que dit la loi.

Définition :

Le Phishing est une technique utilisé par les escrocs en ligne, la technique consiste à envoyer des mails frauduleux pour pouvoir usurper l'identité de la personne et obtenir des renseignements personnels, ainsi l'arnaqueur peut lui soutirer de l'argent.

Les différentes techniques ou types de phishing :

Il y plusieurs techniques ou types de phising, les plus connus sont :

- Abus de confiance
- Fausse loterie
- Mise à jour d'informations
- Appel à donation
- Usurpation d'identité

Toutes ces techniques se basent sur la vulnérabilité du destinataire, ils abusent de la naïveté des personnes pour qu'ils cliquent.

Ainsi il existe aussi différents types de phishing :

- **Le smishing.**

  Message par sms, offre ou liens frauduleux

- **Le vishing.**

  Par message mais avec usurpation d'identité
- **Le Clone phishing.**

  Clonage d'un e-mail d'une entreprise, mais avec des liens frauduleux intégrés
- **Le whaling.**

  Attaque sur les haut placés tels que des PDG, pour des infos.

  Et d'autres :
  - Le Pharming.
  - Le Pop-up phishing.
  - Le Spear phishing.
  - L'evil twin phishing.
  - L'Angler phishing
  - Le HTTPS phishing

Les risques du PHISHING :

Il y a de nombreux risques de phishing, selon le type, cela peut avoir des impacts différents.

Pour le smishing ou le vishing par exemple, ce ne sont que des attaques personnels, ils peuvent soutirer qu'individuellement, peuvent soutirer de l'argent ou usurper l'identité cependant pour le whaling cela peut aller très loin, jusqu'à la perte de donnés de l'entreprise ou le préjudice à la reputation.

Si ces attaquent arrivent à quelqu'un alors elle sera cible priopitaire pour les autres phishing, ainsi ça multiplient son risque juridique. Quant aux entreprises ça donne un risque aux clients et aux fournisseurs.

Exemple de déroulé de phishing :

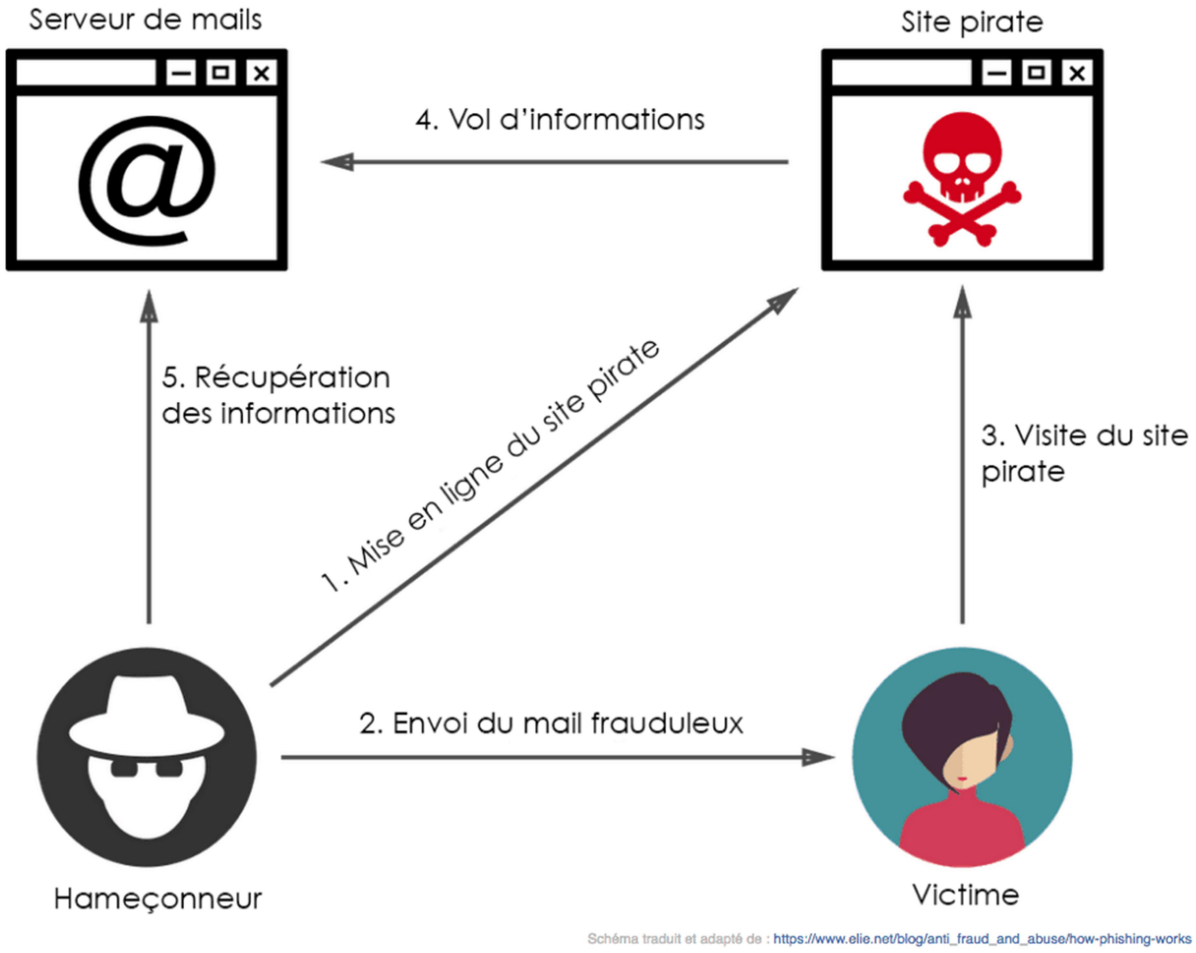
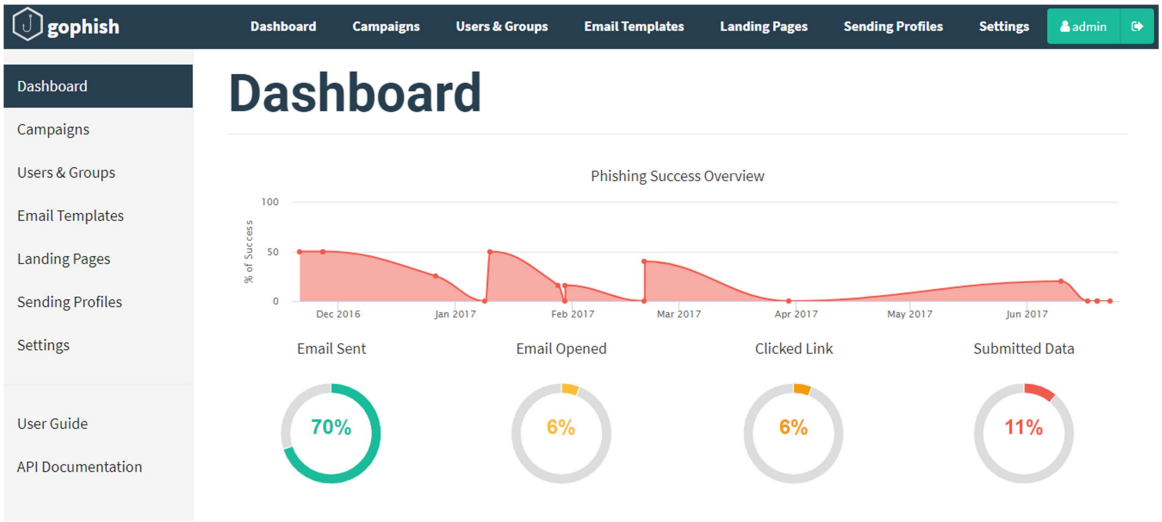


Schéma traduit et adapté de : https://www.elie.net/blog/anti_fraud_and_abuse/how-phishing-works

Outil open source sous linux pour faire du phishing :

Il y a le logiciel Gophish qui consiste à tester facilement l'exposition de son organisation au phishing.



https://getgophish.com/

Comment faire pour éviter le succès des attaques par PHISHING dans les entreprises :

- Ne pas cliquer sur les pièces jointes ou les liens dans les mails douteux
- Pour les achats en ligne, vérifier si le site est bien sécurisé par https
- Ne pas communiquer d'informations personnelles en ligne
- Anti-virus à jour
- Utiliser le filtre contre le filoutage du navigateur internet
- logiciel de filtre anti-pourriel : mettre au spam ce qu'il considère comme spam.

Ce que dit la loi au niveau du PHISHING :

Le cas d'espèce change en fonction de l'infraction :

- **escroquerie** : peine d'emprisonnement de cinq ans et de 375 000 euros d'amende.

- **Collecte de données à caractère personnel par un moyen frauduleux, déloyal ou illicite** : peine d'emprisonnement de cinq ans et de 300 000 euros d'amende.

- **Accès frauduleux à un système de traitement automatisé de données** : cinq ans d'emprisonnement et 150 000 euros d'amende.

- **Contrefaçon et usage frauduleux de moyen de paiement :** peine d'emprisonnement de sept ans et de 750 000 euros d'amende.

- **Usurpation d'identité :** un an d'emprisonnement et de 15 000 euros d'amende.

- **Contrefaçon des marques utilisées lors de l'hameçonnage :** emprisonnement de trois ans et de 300 000 euros d'amende.

Conclusion :

Le Phising peut être repéré, et on peut s'en défendre, il existe plusieurs manière de s'en défendre, ainsi en reconnaissant ces arnaques on peut éviter ses risques.