



RAPPEL :  **La cybersécurité**, c'est l'ensemble des mesures visant à protéger les systèmes informatiques, les réseaux et les données contre le vol, les dommages, les interruptions ou les accès non autorisés.

Le hameçonnage ou phishing

Définition

Le **phishing**, ou **hameçonnage**, est une technique de cyberattaque utilisée pour tromper une personne. Un pirate informatique se fait passer pour une entité de confiance (banque, réseau social, un jeu vidéo, un service de livraison ou même un ami!) pour te pousser à faire quelque chose afin de voler des informations confidentielles.

Les pirates cherchent notamment à obtenir :

- un mot de passe
- des informations personnelles
- des coordonnées bancaires
- un code de sécurité reçu par SMS
- l'accès à un compte de jeu, de messagerie ou de réseau social

Les indices pour détecter un message suspect



Indices liés au message

- Urgence ou Menace : "Votre compte va être fermé !", "Action immédiate requise !"
- Demande de Secret : "Veuillez confirmer votre mot de passe."
- Demande de Code : "Entrez le code reçu par SMS pour valider."
- Gain Inattendu : "Vous avez gagné un iPhone ! Cliquez ici pour le réclamer."
- Message Inhabituel : La façon de parler ou les fautes d'orthographe sont bizarres pour l'expéditeur supposé.



Indices liés à l'expéditeur

- Faux Expéditeur : L'adresse email ressemble mais n'est pas la bonne (ex: dupond@gmail.com).



Indices liés aux liens

- Lien Étrange : L'adresse du lien ne correspond pas au site annoncé (ex: au lieu de).

Les informations collectées peuvent être utilisées pour voler un compte, usurper une identité ou tenter de voler de l'argent.

exemples

Un SMS vous informant que votre colis est bloqué et qu'il faut cliquer sur un lien pour payer des frais de douane.

Un message sur les réseaux sociaux d'un ami disant qu'il a besoin d'argent urgemment et vous demande un virement.

Un pop-up sur un site vous annonçant que vous avez gagné un smartphone et qu'il suffit de remplir un formulaire avec vos informations personnelle.

Un cadenas ou une adresse commençant par HTTPS ne suffit pas à prouver qu'un site est fiable. Il faut aussi vérifier le nom exact du site et le contexte du message.

un peu de vocabulaire

L'**authentification** est le processus de vérification de l'identité d'un utilisateur (souvent par mot de passe).

Une **donnée personnelle** est une information permettant d'identifier directement ou indirectement une personne (nom, prénom, adresse email, numéro de téléphone, etc.).

Une **trace numérique** est une donnée enregistrée par un appareil connecté concernant l'activité ou l'identité d'un utilisateur sur le Web ou à travers l'usage d'outils électroniques (cartes de transport)

Nous laissons tous des traces numériques



Comment se protéger ?

Les 7 règles d'or anti-phishing



1. Je m'arrête avant de cliquer

Un message urgent ou inquiétant peut être conçu pour me faire agir trop vite. Je prends le temps de réfléchir.



2. Je vérifie l'expéditeur

Je regarde l'adresse complète de l'expéditeur et pas seulement son nom affiché. Une adresse étrange ou mal écrite doit m'alerter.



3. Je vérifie le lien sans l'ouvrir

Je vérifie l'adresse du lien avec prudence. Si elle semble différente du site officiel ou contient des fautes, je ne clique pas.



4. Je ne communique jamais mes mots de passe

Un mot de passe est secret. Je ne le donne jamais par e-mail, SMS, message privé ou formulaire reçu dans un message inattendu.



5. Je ne transmets jamais un code de sécurité

Un code reçu par SMS ou dans une application est personnel. Même un ami ou un service officiel ne doit pas me demander de lui transmettre ce code.



6. Je vérifie par un autre moyen

J'ouvre directement l'application officielle, je saisis moi-même l'adresse connue du site ou je contacte le service avec un numéro officiel.



7. Je signale et je demande de l'aide

Je ne réponds pas au message. Je le signale et j'en parle à un adulte de confiance, au collègue ou au service concerné.