SENSIBILISATION

Cours en plus

FERRANDEZ BENJAMIN

AUJOURD'HUI, LA PLUS PARS DES ATTAQUES RÉUSSIES VIENNENT D'UNE ERREUR HUMAINE, PAS D'UN PIRATAGE ULTRA-COMPLEXE.

L'ESSENTIEL SONT SURTOUT DES PIÈGES, DES ARNAQUES, ET DES MANIPULATIONS PSYCHOLOGIQUES.

LE PHISING

LE PHISING : L'ATTAQUE LA PLUS COURANTE

L'hameçonnage ou phishing est **une forme d'escroquerie sur internet**. Le fraudeur se fait passer pour un organisme que vous connaissez (banque, service des impôts, CAF, etc.), en utilisant le logo et le nom de cet organisme.

COMMENT RECONNAÎTRE UN PHISHING ?

- Être attentif
- Observer les fautes d’orthographe ou formulation étrange
- Être prudent avec les pièces jointes inattendues
- Ne jamais fournir d’informations sensibles

LES MOTS DE PASSE

LES MOTS DE PASSE ; LE PROBLEME DE TOUT LE MONDE

- Pourquoi « 123456 » ou « Azerty » sont catastrophiques ?

- Pourquoi réutiliser le même mot de passe partout est dangereux

SOLUTION : GESTIONNAIRE DE MOT DE PASSE

Un gestionnaire de mots de passe est un outil qui stocke tous les mots de passe en sécurité dans un coffre-fort numérique.

Un mot de passe « maitre », le gestionnaire s'occupe du reste.

bitwarden

1Password

NordPass®

LES MISES À JOURS

CORRECTION DE FAILLE DE SÉCURITÉ

Les pirates recherchent constamment des “portes ouvertes”. Quand une faille est identifiée, les équipes techniques l’examinent, développent un correctif, le testent, puis diffusent une mise à jour pour protéger les utilisateurs.

- **CVE – Common Vulnerabilities and Exposures**

  Il est géré par MITRE, et c’est la base de référence mondiale pour les vulnérabilités. https://www.cve.org/

LES WI-FI PUBLICS

LES WIFI PUBLICS : ON OUBLIE

- **Se connecter à un Wi-Fi gratuit (café, gare, hôtel…) peut sembler pratique, mais ça peut être dangereux. Un pirate peut intercepter tes données ou te faire visiter de faux sites.**

- **Faux Wi-Fi (« Evil Twin ») : un pirate crée un réseau avec le même nom que le Wi-Fi public et attend que tu te connectes.**

LE HTTP(S) : OUI MAIS ATTENTION !

- Il peut être un site de phishing avec un certificat valide.
- Il peut contenir des malwares ou liens douteux !

- Le chiffrement protège la transmission, pas la légitimité du site.
- Une connexion sécurisée et un site sécurisé, ce n’est pas la même chose

LE HTTP(S)

HTTPS = CHIFFREMENT, PAS GARANTIE ABSOLUE

✅ Cela signifie que la communication entre ton navigateur et le site est chiffrée.

❌ Cela ne garantit pas que le site est légitime.

Le site peut être créé par un pirate pour voler tes informations,

Il peut avoir un certificat HTTPS valide, mais être un faux site imitant un site officiel.

POURQUOI LE VOLEUR PEUT QUAND MÊME RÉCUPÉRER MON MOT DE PASSE ?

Le navigateur chiffre les données vers le site… mais le site les reçoit en clair.

1. **On rentre notre mot de passe.**
2. **Le navigateur chiffre la requête.**
3. **Le faux site reçoit la requête.**
4. **Comme c’est LUI le destinataire, il décrypte la requête normalement (puisqu’il possède les clés de son propre certificat).**
5. **Il voit ton mot de passe en clair.**