Hameçonnage : les 6 signaux d'alerte

Repérer un message piégé (phishing) avant de mordre à l'appât.

TC DIGITAL ACADEMY

Le principe : un escroc imite un organisme de confiance (banque, livreur, réseau, administration) pour te faire **donner** tes infos ou **cliquer** sur un lien piégé. Il ne mise pas sur la technique — il mise sur toi, en jouant sur l'émotion.

LES 6 SIGNAUX D'ALERTE

1. **L'expéditeur est bizarre**
   Une adresse e-mail étrange, qui ne correspond pas vraiment à l'organisme annoncé.
2. **On crée l'urgence ou la peur**
   « Compte fermé dans 24h », « connexion suspecte », « amende impayée » — pour t'empêcher de réfléchir.
3. **Des fautes / une mise en forme bâclée**
   Fautes de langue, logo approximatif, présentation étrange : fréquent sur les faux messages.
4. **Un lien douteux**
   L'adresse réelle ne correspond pas au site officiel. Pose le doigt / la souris dessus sans cliquer pour voir où il mène.
5. **On demande des infos sensibles**
   Un vrai organisme ne demande jamais ton mot de passe complet ni ta carte par message.
6. **Une demande inhabituelle**
   Un « patron » ou un « proche » qui réclame un virement ou une carte cadeau en urgence.

L'URGENCE	LA PEUR	L'APPÂT DU GAIN
« Agissez immédiatement »	*« Activité suspecte détectée »*	*« Vous avez gagné… »*

Le bon réflexe face à un message suspect

- ✓ Ne clique pas sur le lien, ne réponds pas, ne donne aucune info.
- ✓ Vérifie par un autre chemin : ouvre toi-même l'appli officielle ou tape toi-même l'adresse. Un doute sur un proche ? Appelle-le.
- ✓ Signale et supprime : bouton « Signaler », signal-spam.fr ou Pharos (internet-signalement.gouv.fr).

Règle d'or : un organisme sérieux ne te demandera jamais tes identifiants ou ta carte en urgence par message. Dans le doute, on ne clique pas — on vérifie soi-même.