Que faire si je me fais prendre à un hameçonnage ?

1. Tout de suite : je STOPPE

- Je ferme le courriel / le SMS / la fenêtre du navigateur.
- Je ne clique plus nulle part, je ne réponds pas, je ne télécharge rien.
- Si j'ai un doute, je coupe Internet (Wi-Fi ou données mobiles) le temps de réfléchir calmement.

---

2. Est-ce que j'ai donné quelque chose ?

Cochez ce qui est arrivé :

- J'ai seulement cliqué sur le lien.
- J'ai entré un mot de passe.
- J'ai donné des infos personnelles (nom, date de naissance, NAS, etc.).
- J'ai donné des infos de carte de crédit ou bancaires.
- J'ai ouvert une pièce jointe / installé quelque chose.

Plus il y a de cases cochées, plus il faut agir vite.

---

3. Je protège mes COMPTES

- Si j'ai entré un mot de passe :
    - Je change ce mot de passe **tout de suite** à partir d'un appareil de confiance.
    - Si je réutilisais ce mot de passe ailleurs, je le change aussi sur tous les autres sites.
- J'active la double authentification (2FA) sur mes comptes importants (courriel, banque, réseaux sociaux).

---

4. Je protège mon ARGENT

- Si j'ai donné les infos de ma carte ou accès à mon compte :
    - J'appelle ma banque ou l'émetteur de ma carte (numéro au dos de la carte ou sur le site officiel).
    - Je demande : blocage de la carte, surveillance ou annulation des opérations suspectes.

- Je surveille mes relevés bancaires et mes achats en ligne dans les jours et semaines qui suivent.

---

5. Je vérifie mon APPAREIL

- Je lance un scan complet avec mon antivirus (ordinateur et/ou mobile).
- Je supprime le message frauduleux (et je vide la corbeille du courriel si nécessaire).
- Je fais une sauvegarde de mes documents importants régulièrement (avant qu'un problème arrive).

---

6. Je SURVEILLE mes comptes

- Je regarde si :
    - Des connexions viennent de pays ou d'horaires bizarres.
    - Des messages ont été envoyés à mes contacts à mon insu.
    - Des changements ont été faits dans mes profils ou paramètres.
- Si quelque chose cloche, je change le mot de passe du compte et je vérifie les options de sécurité.

---

7. Je SIGNALE

- J'utilise les boutons « Signaler comme hameçonnage » ou « Courriel indésirable » dans ma messagerie.
- Je préviens l'organisme imité (banque, fournisseur, gouvernement) en allant sur leur vrai site ou en appelant leur vrai numéro.
- Au Canada, je peux aussi déclarer la fraude ou la tentative au Centre antifraude du Canada et, en cas de pertes importantes, contacter la police.

---

8. Pour éviter la prochaine fois

3 questions à se poser avant de cliquer sur un lien ou une pièce jointe :

1. Est-ce que j'attendais vraiment ce message ?
2. Est-ce que l'adresse de l'expéditeur et le lien ont l'air normaux ?
3. Est-ce que je pourrais passer plutôt par le site officiel (en tapant l'adresse moi-même) ?

Si un doute subsiste, on NE clique pas.