Réagir à un e-mail ou un SMS douteux

Repérer une demande suspecte, suspendre l’action et choisir une vérification indépendante. Les exemples sont inventés et ne renvoient vers aucun organisme réel.

Le geste à reprendre : Réagir à un e-mail ou un SMS douteux

Temps indicatif : 10 à 15 minutes ; pauses possibles.

Matériel : Lecture du cas dans le navigateur ou le fichier texte ; aucun clic ni échange réel.

Le cas fictif

DEUX MESSAGES FICTIFS À COMPARER

A — Votre dossier sera supprimé dans dix minutes. Envoyez votre code de connexion pour éviter la fermeture.

B — La rencontre du club est décalée ; consultez le programme par votre accès habituel.

Travail : relever les demandes et signes d’alerte, puis écrire comment vérifier séparément. Même un message bien écrit ou familier ne suffit pas à prouver l’identité de son auteur.

1. Lire la demande avant d’agir

Lisez les deux messages du fichier d’exercice. Pour chacun, écrivez ce que l’expéditeur veut vous faire faire. Une demande urgente, un code ou un accès à votre compte nécessitent un contrôle particulier, même si le nom affiché semble connu.

2. Relever plusieurs indices

Notez la pression du temps, les informations demandées et une éventuelle incohérence de contexte. La présence ou l’absence de faute n’est pas une preuve suffisante. Un cadenas ou HTTPS indique une connexion chiffrée, pas l’honnêteté d’un message ou d’un site.

3. Suspendre l’action demandée

Pour le cas suspect, choisissez de ne pas répondre, ouvrir de pièce jointe ou utiliser de lien fourni par le message. Ne transmettez pas de code. L’exercice porte sur cette décision ; il ne faut pas tester un vrai message dangereux pour savoir ce qui arriverait.

4. Vérifier par un accès déjà connu

Décrivez un moyen de contrôle indépendant : application habituelle, adresse officielle déjà vérifiée ou contact connu séparément. Un numéro ou un lien indiqué dans le message contesté ne constitue pas cette vérification indépendante. Le message B doit lui aussi être recoupé si vous n’attendiez pas ce changement.

5. Préparer la bonne suite

Écrivez une courte note expliquant les indices et le contrôle prévu. Si vous avez déjà communiqué des informations lors d'un incident réel, utilisez les démarches officielles adaptées dans le module arnaques et demandez de l'aide rapidement ; supprimer le message ne répare pas une exposition.

Vérifier votre résultat

• Je décris la demande de chaque message.

• Je relève plusieurs indices et pas seulement l'orthographe.

• Je ne transmets aucun code.

• La vérification utilise un canal indépendant.

• Je distingue prévention et réaction après un incident réel.

Ces contrôles préparent l'autonomie et ne remplacent pas l'observation d'une manipulation. Les documents formateur restent dans le dossier privé.

Pour retrouver les commandes officielles

Cybermalveillance.gouv.fr — Identifier et déjouer l'hameçonnage