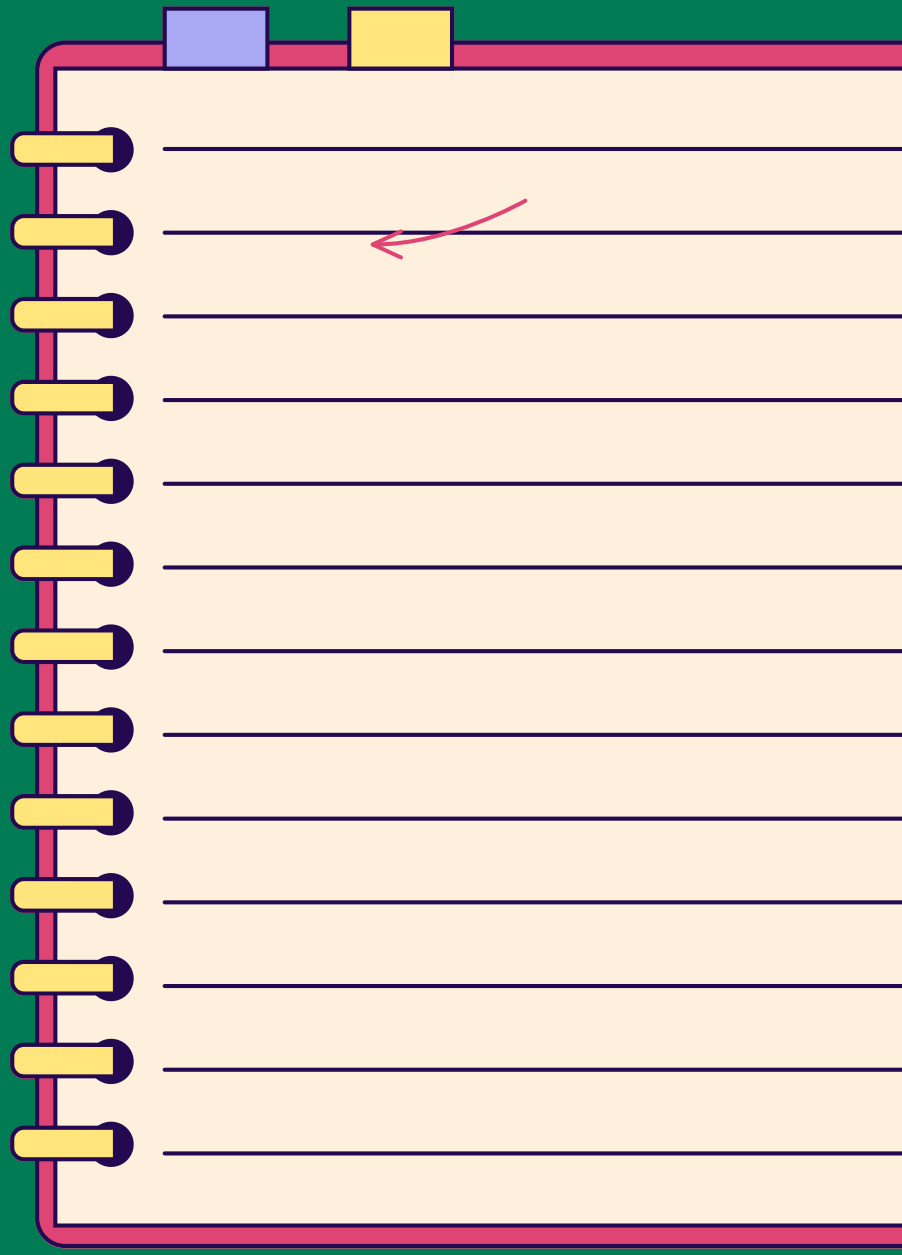
MODULE 12 - ARNAQUES EN LIGNE

CHAPITRE 3

COMMENT RÉAGIR FACE AUX ARNAQUES



Skills to Connect

INTRODUCTION

Dans ce chapitre , vous apprendrez comment réagir face à différentes situations d'arnaques en ligne, que ce soit après avoir cliqué sur un lien frauduleux, être victime d'un spoofing (usurpation d'identité) ou d'une fraude à l'achat. Nous vous guiderons à travers les actions à prendre immédiatement pour sécuriser vos comptes, signaler l'incident, et éviter d'autres conséquences néfastes.
Vous découvrirez également les sites officiels pour signaler les arnaques dans différents pays et les bonnes pratiques à adopter pour protéger vos informations personnelles à l'avenir.

1 COMMENT RÉAGIR FACE AUX ARNAQUES

QUE FAIRE QUAND ON CLIQUE SUR UN LIEN FRAUDULEUX

VOUS AVEZ CLIQUÉ SUR UN LIEN FRAUDULEUX APRÈS UNE TENTATIVE DE PHISHING : QUE FAIRE ENSUITE ?

1 - NE SAISISSEZ AUCUNE DONNÉE

- Si vous entrez vos identifiants sur un faux site, vous offrez au cybercriminel un accès direct à votre compte réel. Une fois connecté, il ou elle peut utiliser votre compte à des fins malveillantes. **La situation devient encore plus grave si vous réutilisez le même mot de passe sur plusieurs comptes, car cela lui permettra d'accéder à ces autres comptes également**.

2 - NE CLIQUEZ SUR RIEN

- Si vous arrivez sur un site suspect, n'y cliquez sur aucun lien, car il pourrait contenir des virus prêts à s'activer. Évitez également de cliquer sur les publicités : elles pourraient contenir des logiciels malveillants, un phénomène appelé « malvertising ». Même un simple clic peut déclencher l'installation d'un programme nuisible sur votre appareil.

3 - DÉCONNECTEZ-VOUS D'INTERNET & CHANGEZ VOS MOTS DE PASSE

- Couper votre connexion Internet permet de bloquer l'accès à distance à votre appareil par le cybercriminel. Cela limite aussi la propagation de logiciels malveillants vers d'autres appareils connectés à votre réseau Wi-Fi. Déconnecter votre appareil rapidement peut réduire considérablement les risques de dommages.
- Une fois votre appareil déconnecté, utilisez un autre appareil fiable (comme un autre ordinateur, une tablette ou un smartphone) pour changer vos mots de passe
  - Connectez vous à un réseau sûr : Évitez les réseaux Wi-Fi publics. Utilisez votre réseau domestique ou partagez la connexion Internet d'un smartphone (mode "partage de connexion" ou "hotspot mobile").
  - Accédez aux sites importants comme votre messagerie, vos comptes bancaires ou vos réseaux sociaux.
  - Cliquez sur "Mot de passe oublié ?" si vous avez des difficultés pour vous connecter. Cela vous permettra de réinitialiser le mot de passe en suivant les instructions envoyées par email ou SMS.

1 COMMENT RÉAGIR FACE AUX ARNAQUES

QUE FAIRE QUAND ON CLIQUE SUR UN LIEN FRAUDULEUX

4 - EFFECTUEZ UN SCAN COMPLET AVEC UN ANTIVIRUS :

- Une fois déconnecté, il est important d'analyser votre appareil à l'aide d'un logiciel antivirus. Si vous n'en avez pas déjà installé un, faites-le sans tarder. L'antivirus va examiner votre appareil pour détecter et supprimer les virus ou logiciels malveillants avant qu'ils ne causent des dégâts importants. Pour cela :
  - Ouvrez votre antivirus installé sur votre appareil.
  - Choisissez l'option "Scan complet" ou "Analyse complète". Cela permet à l'antivirus d'examiner tous les fichiers de votre ordinateur, y compris les zones sensibles où se cachent souvent les virus.
  - Une fois le scan terminé, suivez les recommandations de l'antivirus : supprimez ou mettez en quarantaine les menaces détectées.
  - Après le scan, reconnectez-vous uniquement si votre appareil est propre (aucune menace détectée).
  - Une fois en ligne, mettez à jour votre antivirus pour qu'il ait les dernières protections contre les nouvelles menaces. Ensuite, lancez un nouveau scan pour vérifier que tout est sécurisé.

5 - SURVEILLEZ VOS COMPTES :

- Même après avoir pris ces précautions, restez vigilant en surveillant régulièrement vos comptes pour repérer toute activité suspecte. Le cybercriminel a peut-être eu le temps de récupérer des informations sensibles. Vérifiez attentivement vos relevés bancaires pour repérer des transactions que vous n'avez pas effectuées, ainsi que des connexions inhabituelles ou des changements non autorisés sur vos comptes en ligne.

2 COMMENT RÉAGIR FACE AUX ARNAQUES

QUE FAIRE QUAND ON EST VICTIME DE SPOOFING

QUELQU'UN S'EST FAIT PASSÉ POUR VOTRE BANQUIER ET VOUS A VOLÉ DE L'ARGENT : QUE FAIRE ENSUITE ?

1 - CONTACTEZ IMMÉDIATEMENT VOTRE BANQUE

- Appelez votre banque en utilisant le numéro officiel (celui inscrit sur votre carte bancaire ou sur le site officiel). Expliquez ce qui s'est passé et demandez à :
  - Bloquer vos cartes bancaires si vous avez donné vos numéros,
  - Vérifier vos comptes pour bloquer toute transaction suspecte,
  - Modifier l'accès à vos comptes en ligne pour éviter que l'escroc ne s'y connecte.

2 - CHANGEZ VOS MOTS DE PASSE

- Modifiez immédiatement vos mots de passe pour tous vos comptes sensibles, surtout :
  - Vos comptes bancaires en ligne,
  - Votre boîte email (car elle est souvent utilisée pour récupérer des mots de passe),
  - Vos comptes sur d'autres services (réseaux sociaux, sites d'achat) si vous réutilisez le même mot de passe.

2 COMMENT RÉAGIR FACE AUX ARNAQUES

QUE FAIRE QUAND ON EST VICTIME DE SPOOFING

3 - SURVEILLEZ VOS COMPTES BANCAIRES

- Consultez vos relevés bancaires et vos transactions en ligne pour repérer des paiements ou virements que vous n'avez pas effectués.
  - Activez les notifications SMS ou par email pour être alerté dès qu'une transaction a lieu.
  - Si vous voyez des opérations suspectes, signalez-les immédiatement à votre banque.

4 - DÉPOSEZ PLAINTE

- Rendez-vous au commissariat ou à la gendarmerie pour déposer plainte. Apportez toutes les preuves possibles : Le numéro qui vous a contacté, les messages, emails ou captures d'écran liés à l'arnaque.
- Vous pouvez également signaler l'arnaque en ligne sur des plateformes dédiées :
  - En France : Signalez-le via la plateforme Pharos
  - En Belgique : Faites un signalement sur Safeonweb.be
  - Au Portugal : déposer une plainte auprès de la police de sécurité publique (https://www.policiajudiciaria.pt/queixa-eletronica/) ou de l'Office de lutte contre la cybercriminalité (https://cibercrime.ministeriopublico.pt/pagina/denuncia-0)

voir chapitre 4

3 COMMENT RÉAGIR FACE AUX ARNAQUES

QUE FAIRE QUAND ON EST VICTIME D'UNE FRAUDE À L'ACHAT

VOUS AVEZ RÉALISÉ UN ACHAT SUR UN SITE FRAUDULEUX : QUE FAIRE ENSUITE ?

1 - CONTACTEZ IMMÉDIATEMENT VOTRE BANQUE OU VOTRE FOURNISSEUR DE CARTE

- Si vous avez payé via carte bancaire ou un autre moyen de paiement, contactez immédiatement votre banque ou le fournisseur de carte. Expliquez la situation et demandez à :
  - Annuler la transaction si cela est possible,
  - Faire opposition à votre carte pour éviter d'autres paiements frauduleux,
  - Vérifier les autres transactions récentes pour détecter des paiements non autorisés.

2. CHANGEZ VOS MOTS DE PASSE

- Si vous avez saisi des informations sensibles (comme votre mot de passe ou vos coordonnées bancaires) sur le site frauduleux, changez les mots de passe de vos comptes bancaires en ligne, de votre boîte email et de tout autre compte utilisé avec ce mot de passe.

3 COMMENT RÉAGIR FACE AUX ARNAQUES

QUE FAIRE QUAND ON EST VICTIME D'UNE FRAUDE À L'ACHAT

3 - SURVEILLEZ VOS COMPTES

- Vérifiez vos relevés bancaires et surveillez toute activité suspecte, en particulier si des transactions non autorisées ont lieu.
- Activez les alertes par SMS ou email de votre banque pour être informé en temps réel de toute activité sur vos comptes.
- Vérifiez également vos comptes en ligne (Amazon, PayPal, etc.) pour vous assurer qu'aucune information n'a été utilisée frauduleusement.

4 - SIGNALEZ LE SITE FRAUDULEUX

- Déposez une plainte auprès de la police locale ou en ligne.
- Vous pouvez également signaler l'arnaque en ligne sur des plateformes dédiées :
  - En France : Signalez-le via la plateforme Pharos
  - En Belgique : Faites un signalement sur Safeonweb.be
  - Au Portugal : signalement sur https://queixaselectronicas.mai.gov.pt/
- Vous pouvez aussi signaler le site frauduleux à des organisations de consommateurs
  - Trustpilot
  - Signal-Arnaques
  - ScamDoc

voir chapitre 4

voir chapitre 1

4 QUE FAIRE SI ON REPÈRE UNE ARNAQUE ?

LES PLATEFORMES DE SIGNALEMENT ET DE PRÉVENTIONS

BELGIQUE

- Cybersimple.be : cette plateforme offre des conseils pour prévenir les arnaques en ligne, fournir des informations sur les types de fraudes courants et signaler les incidents de cybersécurité.
- Centre pour la Cybersécurité Belgique : Le Centre pour la Cybersécurité belge (CCB) aide à signaler les incidents de cybersécurité, y compris les attaques par phishing, et fournit des conseils pour protéger votre appareil.
- Safe On Web : Plateforme officielle pour signaler les arnaques et incidents de cybersécurité. Elle fournit aussi des recommandations pour se protéger des risques numériques.

FRANCE

- Thesee : Plateforme officielle du ministère de l'Intérieur permettant de signaler des arnaques en ligne (phishing, fraude bancaire, etc.). Elle permet aussi de déposer des plaintes.
- Cybermalveillance : Plateforme pour signaler les cyberattaques et obtenir de l'aide face aux incidents liés à la cybersécurité. Ce site offre des conseils et ressources pour les victimes.
- Pharos : Plateforme officielle de signalement des contenus illégaux en ligne (arnaques, phishing, cybercriminalité). Elle permet de signaler les fraudes en ligne auprès des autorités compétentes.

4 QUE FAIRE SI ON REPÈRE UNE ARNAQUE ?

LES PLATEFORMES DE SIGNALEMENT ET DE PRÉVENTIONS

PORTUGAL

- Seguranet : Site du gouvernement portugais fournissant des informations pour signaler des fraudes en ligne et des conseils pour se protéger contre les cyberattaques et le phishing.
- Violencia : Site pour signaler des comportements criminels en ligne, y compris les arnaques, les abus et les fraudes. Il permet également de recevoir des conseils de sécurité.

UNION EUROPÉENNE

- Site EU - Droit des victimes : Ce site européen fournit des informations sur les droits des victimes de crimes dans toute l'UE, y compris sur les moyens de signaler les fraudes et les crimes transfrontaliers.

À RETENIR

Si vous êtes victime d'une arnaque en ligne, agissez rapidement en changeant vos mots de passe, contactant votre banque, et en signalant l'incident aux autorités compétentes. Il est essentiel de ne pas cliquer sur de nouveaux liens et de déconnecter votre appareil d'Internet pour éviter toute propagation de logiciels malveillants. En surveillant régulièrement vos comptes et en utilisant des outils de sécurité comme l'antivirus et l'authentification à deux facteurs, vous pouvez limiter les risques et protéger vos informations personnelles. Enfin, restez vigilant face aux tentatives d'escroquerie futures en apprenant à reconnaître les signes d'une arnaque.