



Club Informatique & Multimédias du Plessis-Pâté

LA CULTURE NUMÉRIQUE POUR TOUS !



Reconnaître un piratage

Les signes qui doivent vous alerter, et les bons réflexes à adopter

Cours de sensibilisation à la cybersécurité

Un support conçu pour être simple, concret et utile au quotidien

Ce que vous allez apprendre dans ce cours

- Reconnaître les signes qu'un compte (email, réseau social, banque) a été piraté
- Reconnaître les signes qu'un ordinateur, une tablette ou un téléphone a été piraté
- Savoir quoi faire, dans l'ordre, si vous pensez être piraté
- Connaître les bons réflexes pour éviter que cela n'arrive



1. Pourquoi ce cours ?

Internet fait aujourd'hui partie de la vie de tous les jours : la messagerie électronique, les réseaux sociaux, la banque en ligne, les démarches administratives. Cela apporte beaucoup de confort, mais attire aussi des personnes malveillantes qui cherchent à profiter de la confiance des gens.

Les seniors sont particulièrement visés par les escroqueries en ligne, non pas parce qu'ils seraient moins capables, mais parce que les arnaqueurs pensent, parfois à tort, qu'ils sont moins familiers avec les outils numériques et plus enclins à faire confiance à un interlocuteur poli et rassurant.

La bonne nouvelle : il existe des signes simples qui permettent de repérer un piratage, et des réflexes faciles à retenir pour réagir vite et bien. C'est tout l'objet de ce cours.

2. Un piratage, qu'est-ce que c'est exactement ?

On parle de piratage quand une personne malveillante prend le contrôle, sans votre accord, d'un de vos comptes en ligne (messagerie, réseau social, banque...) ou d'un de vos appareils (ordinateur, tablette, téléphone).

Il existe deux grandes familles de signes à surveiller :

- Les signes qui concernent vos comptes en ligne : votre messagerie, vos réseaux sociaux, votre espace bancaire, vos abonnements.
- Les signes qui concernent vos appareils : votre ordinateur, votre tablette ou votre smartphone lui-même.

Nous allons voir ces deux familles l'une après l'autre.

3. Les signes d'alerte sur vos comptes en ligne

Voici les signes les plus fréquents qui doivent vous mettre la puce à l'oreille. Un seul signe suffit déjà pour être vigilant ; plusieurs signes ensemble doivent vous alerter fortement.

Sur votre messagerie électronique (email)

- Vous ne parvenez plus à vous connecter avec votre mot de passe habituel, alors que vous êtes certain de ne pas l'avoir changé.
- Des messages envoyés depuis votre adresse apparaissent, alors que vous ne les avez pas écrits (vos proches vous en parlent parfois avant vous).
- Vous recevez une notification de connexion « depuis un nouvel appareil » ou « depuis un lieu inhabituel ».



- Des messages que vous receviez d'habitude (banque, administration) n'arrivent plus : ils ont peut-être été redirigés en cachette vers une autre boîte.
- Votre signature, votre photo de profil ou vos paramètres (transfert automatique, réponse automatique) ont changé sans que vous y touchiez.

Sur vos réseaux sociaux (Facebook, WhatsApp, Instagram...)

- Des publications, des messages privés ou des demandes d'amis partent de votre compte sans votre accord.
- Un proche vous signale avoir reçu, « de votre part », une demande d'argent urgente ou un lien étrange.
- Votre photo, votre nom ou votre description de profil ont été modifiés.
- Vous êtes soudainement ajouté à des groupes que vous ne connaissez pas.

Sur votre compte bancaire ou vos paiements en ligne

- Des prélèvements, virements ou achats que vous n'avez pas faits apparaissent sur votre relevé.
- Vous recevez un code de validation par SMS que vous n'avez pas demandé (quelqu'un tente peut-être de valider un paiement à votre place).
- Votre banque vous contacte pour confirmer une opération que vous n'avez jamais effectuée.

Les faux appels de « votre banque » (arnaque au « faux conseiller »)

Cette arnaque par téléphone, aussi appelée « vishing », touche de plus en plus de seniors. Voici comment elle se déroule, et les signaux qui doivent vous alerter :

- Une personne vous appelle en se présentant comme votre conseiller bancaire, ou comme le service sécurité / fraude de votre banque.
- Elle affirme qu'une opération suspecte est en cours sur votre compte et qu'il faut agir « immédiatement » pour la bloquer : ce sentiment d'urgence est lui-même un signal d'alarme.
- Elle vous demande de valider une opération sur votre application bancaire, de lui confirmer un code reçu par SMS, ou de communiquer des informations personnelles ou bancaires.
- Elle peut aussi vous demander de faire un virement vers un « compte sûr », d'installer une application de prise en main à distance, de retirer de l'argent liquide, ou de remettre votre carte bancaire à un coursier envoyé « par la banque ».

À retenir : un site, une banque ou une administration sérieuse ne vous demandera jamais votre mot de passe complet, votre code de carte bancaire ou un code reçu par SMS, que ce soit par téléphone, par email ou par SMS. Le numéro affiché sur votre téléphone peut être falsifié (« spoofing ») : même s'il ressemble au vrai numéro de votre banque, ce n'est pas



une preuve. Face à un appel qui crée l'urgence, raccrochez et rappelez vous-même votre banque avec le numéro inscrit au dos de votre carte bancaire ou sur un relevé papier — jamais un numéro donné par votre interlocuteur.

4. Les signes d'alerte sur votre ordinateur, tablette ou téléphone

Un appareil piraté ou infecté par un « virus » (on dit aussi un logiciel malveillant) donne souvent des signes visibles, même s'ils ne sont pas toujours spectaculaires.

Le comportement général de l'appareil

- L'appareil devient beaucoup plus lent qu'avant, met du temps à démarrer ou plante souvent.
- La batterie se vide anormalement vite, ou l'appareil chauffe alors que vous ne l'utilisez pas beaucoup.
- L'appareil redémarre tout seul ou des fenêtres s'ouvrent et se ferment sans que vous y touchiez.

Des changements que vous n'avez pas faits

- De nouvelles applications ou icônes apparaissent sur l'écran, sans que vous les ayez installées.
- La page qui s'ouvre au démarrage de votre navigateur internet a changé.
- Des fenêtres publicitaires apparaissent tout le temps, même quand vous n'êtes pas en train de naviguer sur internet.
- Votre antivirus ou votre pare-feu s'est désactivé tout seul, ou affiche un message inhabituel.

Des signes plus discrets, mais importants

- Le petit voyant de la caméra ou du micro s'allume alors que vous n'utilisez aucune application qui en a besoin.
- Un message s'affiche pour vous réclamer de l'argent en échange du « déblocage » de votre appareil (rançongiciel) : ne payez jamais et demandez de l'aide.

À retenir : ne cliquez jamais sur un lien ou un bouton dans une fenêtre qui vous fait peur (« Votre appareil est infecté, cliquez ici ! »). Fermez la fenêtre, ou éteignez l'appareil si besoin, puis demandez conseil à une personne de confiance ou à cybermalveillance.gouv.fr.



5. Mises en situation : à vous de jouer

Voici quatre petites histoires. Pour chacune, demandez-vous : « Est-ce que je repère un signe de piratage ou d'arnaque ? Que ferais-je ? » Ces situations peuvent être discutées en groupe.

Situation 1 — Le message de la banque

Vous recevez un SMS qui semble venir de votre banque : « Votre carte a été bloquée pour raison de sécurité, cliquez ici pour la réactiver. » Le lien ressemble à celui de votre banque, mais avec une petite différence dans l'adresse.

→ Réflexe à avoir : ne cliquez pas sur le lien. Contactez votre banque directement, en utilisant le numéro habituel inscrit sur votre carte ou vos relevés, jamais celui indiqué dans le message reçu.

Situation 2 — Le message d'un ami sur WhatsApp

Un ami vous écrit sur WhatsApp qu'il a un souci urgent et vous demande de lui envoyer de l'argent rapidement, sans donner beaucoup de détails, avec un ton qui ne lui ressemble pas.

→ Réflexe à avoir : appelez cette personne directement par téléphone pour vérifier que c'est bien elle qui écrit. Son compte a peut-être été piraté par quelqu'un qui se fait passer pour elle.

Situation 3 — L'ordinateur qui affiche une alerte

Une fenêtre s'affiche brusquement sur votre écran d'ordinateur : « ALERTE ! Votre ordinateur est infecté par 5 virus, appelez immédiatement ce numéro pour une assistance technique. »

→ Réflexe à avoir : ne pas appeler ce numéro et ne rien télécharger. Il s'agit très probablement d'une fausse alerte destinée à vous faire payer une « réparation » inutile ou à prendre le contrôle de votre appareil à distance. Fermez la fenêtre ou éteignez l'ordinateur, puis faites-le vérifier par une personne de confiance.

Situation 4 — L'appel du « conseiller bancaire »

Une personne vous appelle, semble bien informée à votre sujet, et affirme travailler pour le service fraude de votre banque. Elle vous dit qu'une opération suspecte vient d'être détectée et vous demande de lui confirmer le code que vous venez de recevoir par SMS « pour l'annuler ». Le numéro affiché sur votre téléphone est bien celui de votre banque.

→ Réflexe à avoir : ne communiquez jamais ce code, même si le numéro affiché semble correct — il peut être falsifié. Raccrochez, puis rappelez vous-même votre banque en utilisant le numéro inscrit au dos de votre carte bancaire ou sur un relevé papier, jamais un numéro donné par votre interlocuteur ou rappelé directement sans raccrocher.



6. Que faire si vous pensez être piraté ?

Si un ou plusieurs signes vous inquiètent, voici les étapes à suivre, dans l'ordre :

1. Gardez votre calme. Il n'y a pas d'urgence à agir dans la panique : mieux vaut agir posément mais rapidement.
2. Déconnectez l'appareil d'internet si vous pensez qu'il est infecté (Wi-Fi ou câble), le temps d'y voir plus clair.
3. Changez immédiatement le mot de passe du compte concerné, depuis un autre appareil si possible, en choisissant un mot de passe différent de celui piraté.
4. Activez la double authentification si ce n'est pas déjà fait (un code envoyé par SMS ou une application, en plus du mot de passe).
5. Vérifiez les paramètres du compte : transfert automatique des e-mails, appareils connectés, informations personnelles.
6. Prévenez vos proches si des messages ont pu être envoyés en votre nom, pour qu'ils ne tombent pas dans le piège.
7. Surveillez vos comptes bancaires et faites opposition sans attendre en cas de mouvement suspect.
8. Faites contrôler votre appareil (antivirus, ou par une personne compétente) si vous pensez qu'il est infecté.
9. Signalez la situation aux organismes compétents (voir la partie suivante).



7. Qui contacter et comment signaler ?

En France, plusieurs services officiels et gratuits existent pour vous aider. Voici les principaux, avec leur rôle.

Organisme	Pour quel besoin	Comment le contacter
Cybermalveillance.gouv.fr	Assistance et conseils en cas de piratage d'un compte ou d'un appareil ; met en relation avec un professionnel de confiance près de chez vous.	Site internet : cybermalveillance.gouv.fr
3018	Numéro national contre les violences numériques : harcèlement en ligne, chantage, usurpation d'identité, sextorsion.	Appel ou SMS gratuits au 3018, 7 jours sur 7
THESEE	Porter plainte en ligne pour une escroquerie ou une arnaque subie sur internet.	Via masecurite.interieur.gouv.fr
Signal Conso	Signaler une arnaque ou un problème avec un site marchand ou un service en ligne.	Site internet : signal.conso.gouv.fr
Votre banque	Faire opposition immédiatement en cas de paiement ou de mouvement d'argent suspect.	Numéro indiqué au dos de votre carte bancaire
Police ou gendarmerie	Déposer plainte ; en cas de danger immédiat ou de situation grave en cours.	Commissariat ou gendarmerie le plus proche ; le 17 pour une urgence



8. Les bons réflexes au quotidien pour se protéger

- Utilisez un mot de passe différent pour chaque compte important, si possible long (plus de 12 caractères) et facile à retenir pour vous seul(e).
- Activez la double authentification dès que le service la propose (banque, messagerie, réseaux sociaux).
- Mettez à jour régulièrement votre ordinateur, votre tablette et votre téléphone : les mises à jour corrigent des failles de sécurité.
- Ne communiquez jamais un mot de passe, un code reçu par SMS ou vos coordonnées bancaires par téléphone, email ou SMS, même si votre interlocuteur semble sérieux.
- Prenez le temps de vérifier avant d'agir : un message ou un appel qui crée l'urgence ou la peur (« Agissez maintenant ! ») est souvent le signe d'une arnaque.
- Ne validez jamais une opération bancaire et ne communiquez jamais un code pendant un appel non sollicité, même si votre interlocuteur se présente comme votre banque et semble légitime : raccrochez et appelez vous-même avec le numéro officiel.
- En cas de doute sur un appel, un email ou un message, raccrochez ou n'y répondez pas, puis contactez l'organisme concerné par un numéro ou un site que vous connaissez déjà.
- N'installez des applications que depuis les magasins officiels (Google Play, App Store).
- Parlez-en autour de vous : un proche, une association ou un point numérique local peut vous aider et vous rassurer en cas de doute.



9. Fiche mémo à garder près de vous

Les 10 signes à connaître qu'un compte ou un appareil est peut-être piraté :

1. Vous ne pouvez plus vous connecter à un compte habituel
2. Des messages partent de votre compte sans que vous les ayez écrits
3. Une notification de connexion inhabituelle apparaît
4. Des paramètres ou informations ont changé sans votre accord
5. Des mouvements d'argent que vous n'avez pas faits apparaissent
6. Vous recevez un code SMS que vous n'avez pas demandé
7. L'appareil est anormalement lent, chauffe ou plante souvent
8. De nouvelles applications ou fenêtres publicitaires apparaissent
9. L'antivirus se désactive tout seul
10. Une fenêtre ou un message vous réclame de l'argent ou vous fait peur

En cas de doute : ne cliquez pas, ne payez pas, ne communiquez aucun code. Contactez une personne de confiance du CIM.PP ou cybermalveillance.gouv.fr, et gardez ce document à portée de main.

10. Pour aller plus loin

Ce cours s'appuie notamment sur les ressources officielles suivantes, que vous pouvez consulter à tout moment :

- **cybermalveillance.gouv.fr** — conseils et assistance en cas de piratage
- **masecurite.interieur.gouv.fr** — fiches pratiques du ministère de l'Intérieur sur les arnaques en ligne
- **signal.conso.gouv.fr** — signaler une arnaque ou un litige avec un site marchand