CYBERCRIMINALITÉ
RISQUES ET RECOMMANDATIONS

Comment prévenir les arnaques,
se protéger et réagir

Brigade de Criminalité Informatique (BCI)
Brigade des Cyber Enquêtes (BCE)
Service communication et relations publiques (SCRP)

REPUBLIQUE ET CANTON DE GENEVE
POST TENEBRAS LUX

POLICE GENÈVE

Les arnaques fréquentes

Phishing / Hameçonnage

Faux SMS ou e-mails (poste, banque, police, opérateur...).
Objectif : voler vos mots de passe ou argent.

Ne cliquez jamais sur un lien reçu par message.

Faux support technique

Appel Microsoft, Swisscom, fenêtre annonçant un virus...

Objectif : prendre le contrôle de votre ordinateur.

Aucun service ne vous contacte spontanément.

Romance scam

Faux profils, déclarations d'amour rapides, demandes d'argent.

Si la personne ne vous a jamais rencontré, **c'est une arnaque.**

Arnaques aux investissements

Bitcoin, placements « garantis », rendements rapides.

Si c'est trop beau pour être vrai, c'est faux.

Money mule / colis

On vous demande de transférer de l'argent ou un colis.

Vous pouvez être pénalement responsable.

Comment reconnaitre une arnaque?

L'urgence

Les escrocs créent la panique : "aidez-moi vite", "votre compte va être bloqué", "investissez maintenant".
Toute urgence imposée doit alerter.

Le contact non sollicité

Un message, mail ou appel inattendu est souvent le point de départ d'une arnaque.

Une demande d'argent inhabituelle

Amende, aide urgente, frais de colis ou récupération d'argent : **toute demande soudaine est suspecte.**

Une prise en main à distance

Ne laissez jamais quelqu'un contrôler votre ordinateur à distance si vous n'avez rien demandé.

Faute d'orthographe ou style étrange

Fautes, logos flous, mise en page douteuse : signes fréquents d'escroquerie.

Trop beau pour être vrai

Gains rapides, amour immédiat, rendements miraculeux = **arnaque assurée.**

Attention

Ce qu’il ne faut pas faire

Ne pas cliquer sur les liens reçus

Même si le message semble officiel, évitez de cliquer : allez directement sur le site réel.

Ne pas donner ses identifiants

Ne partagez jamais mots de passe ou codes, ni par téléphone, ni par e-mail.

Ne pas installer de programme demandé par un inconnu

Refusez toute installation, surtout les logiciels de prise en main à distance.

Ne pas envoyer sa carte d’identité

Un document d’identité peut servir à usurper votre identité.

Ne pas payer pour résoudre un problème

Colis bloqué, amende ou compte suspendu : ce sont de fausses alertes.

Ne pas transférer d’argent

Vous pourriez devenir complice malgré vous (recel, blanchiment).

Ne pas se fier uniquement à la gentillesse

Les escrocs paraissent souvent aimables pour mieux manipuler.

Réagissez

Ce qu’il faut faire

Vérifier par soi-même

Ne cliquez pas sur les liens suspects. Ne donnez aucune information privée. Vérifiez directement sur le site officiel ou en appelant le numéro connu (banque, opérateur, poste).

Demander l’avis d’un proche

En parler aide à repérer l’arnaque. Les escrocs jouent sur l’isolement.

Mettre à jour ses appareils

Système, applications et antivirus à jour empêchent de nombreuses attaques.

Utiliser des mots de passe solides

Minimum 12 caractères, un mot de passe différent pour chaque service. Un gestionnaire de mots de passe est idéal.

Sauvegarder régulièrement ses données

Sur un disque externe ou un cloud sécurisé pour éviter la perte de données.

En cas de doute : STOP

Ne cliquez pas. Ne répondez pas. Ne payez rien. Ne laissez personne accéder à votre appareil. Parlez-en et demandez conseil.

Contacts et ressources

Numéros utiles

Police : 022 427 81 11

Swisscom : 0800 800 800

Sunrise : 0800 707 707

Salt : 0800 700 700

UBS : 0848 848 051

BCGe : 058 211 21 00

Raiffeisen : 0848 847 222

La Poste : 0848 888 888

Liens utiles

www.cybercrimepolice.ch

www.ncsc.admin.ch

www.skppsc.ch

www.stop-cyberfraude.ch

En cas de doute

Parlez-en, demandez conseil : Vous n’êtes jamais seul face à une arnaque !