



Nous sommes tous "scotchés" à nos ordinateurs et il est bien compliqué aujourd'hui de vivre sans. Les escrocs l'ont bien compris. Les cyberattaques se développent et se multiplient tous les jours, notamment le ransomware et le chantage à la webcam. Alors comment s'en protéger ?

- [Un ransomware, qu'est-ce que c'est ?](#)
- [Le chantage à la webcam, qu'est-ce que c'est ?](#)
- [Comment s'en protéger ?](#)

Un ransomware, qu'est-ce que c'est ?

Un **ransomware** est un programme malveillant utilisé par des **pirates informatiques** pour **piéger votre matériel** (ordinateur, smartphone, tablette...), **bloquer vos fichiers** ou vos accès et vous **extorquer de l'argent**...

Aujourd'hui cette pratique est de plus en plus courante et il en existe plusieurs formes, les plus connues sont :

- le **ransomware crypto**, où vos fichiers, documents, images, vidéos... sont chiffrés et en quelque sorte **pris en otage** ;
- le **ransomware locker**, où l'accès à votre ordinateur (ou à certaines fonctionnalités de celui-ci) vous est refusé.

Pour débloquer l'accès ou pour obtenir une clé qui déchiffrera vos fichiers, on vous demandera de payer une **rançon**, parfois en utilisant des moyens de pression comme un délai relativement court. Et si vous ne répondez pas favorablement à leur demande, vos documents peuvent être perdus à jamais, ou l'accès à votre matériel informatique compromis. Malgré l'insistance du message, il est vivement recommandé de ne **jamais payer la rançon** demandée. En effet, si vous payez, vous n'avez aucune garantie que les **escrocs** vous fourniront la clé qui permettra de déchiffrer vos fichiers ou débloquer votre ordinateur.

Souvent le **ransomware** infecte votre matériel en s'infiltrant à travers un fichier téléchargé sur Internet ou reçu par email. Ces emails peuvent aussi inclure des **pièces jointes piégées** ou des **liens vers des sites malveillants**.

Pour parvenir à leur fin, les **arnaqueurs** ont principalement recours à deux méthodes :

- l'**ingénierie sociale** qui vise à récupérer des données auprès d'un collaborateur par exemple pour ensuite rendre la démarche plus crédible auprès d'un autre collaborateur,
- le **phishing**, ils envoient des emails semblant provenir de sources légitimes comme la [banque](#), la CAF, les impôts... en utilisant leurs codes visuels comme leur logo.

Consultez ici notre [infographie](#).

[Retour haut de page](#)

Le chantage à la webcam, qu'est-ce que c'est ?

Le **chantage à la webcam** est une **escroquerie** qui s'est beaucoup développée ces dernières années. Des **personnes malveillantes** vont vous faire croire qu'elles détiennent des photos ou des vidéos compromettantes de vous et vont ainsi vous faire du **chantage**. Elles vont notamment vous menacer de diffuser ces éléments (sur Internet ou de les envoyer à vos familles, amis, proches...) si vous refusez de payer une **rançon**.

Cette **arnaque** s'opère particulièrement sur les sites de rencontre et sur les réseaux sociaux : les **pirates** vont tenter de gagner votre confiance grâce à un faux profil attractif.

Ne répondez pas et **ne payez pas la rançon** réclamée.

Consultez ici notre [infographie](#).

[Retour haut de page](#)

Comment s'en protéger ?

Voici quelques **réflexes sécurité** à adopter pour vous protéger d'une **cyberattaque** :

- Méfiez-vous des offres trop alléchantes : quand c'est trop beau pour être vrai, alors c'est probablement faux.
- Ne suivez jamais de lien contenu dans un email.
- Tapez vous-même l'adresse du site Internet et vérifiez que l'adresse est sécurisée (présence https ou cadenas fermé).
- N'enregistrez ni vos données client, ni de paiement sur Internet.
- Ne communiquez pas vos identifiant et mot de passe.
- Effectuez régulièrement des sauvegardes externes.
- Protégez votre matériel avec des mises à jour régulières et des antivirus.
- Signalez une **tentative de fraude** sur cybermalveillance.gouv.fr, avertissez votre [banque](#) et faites [opposition](#) si nécessaire.