CYBERMALVEILLANCE : POURQUOI ET COMMENT SÉCURISER SA MESSAGERIE ? AVEC CYBERMALVEILLANCE

Date de publication : **26/10/2021 - Internet/multimédia**

Stéphane : "J’utilise souvent ma messagerie personnelle et j’aimerais savoir comment la sécuriser ?".

Vous avez bien raison, Stéphane, de vouloir protéger votre compte ! En effet, le piratage de messagerie représente la deuxième menace de cybermalveillance la plus courante pour les particuliers. Les fraudeurs emploient cette méthode pour vous dérober des informations personnelles, professionnelles ou bancaires, et par la suite les revendre, usurper votre identité ou encore effectuer des transactions frauduleuses.

Votre boite mail contient des données sensibles comme des copies de carte d'identité ou encore des mots de passe.

Comment les pirates réussissent-ils à récupérer ces données ?

Les fraudeurs peuvent facilement accéder à votre compte si vous utilisez un mot de passe trop simple, ou si vous utilisez le même mot de passe sur plusieurs sites Internet et que l'un d'entre eux a été piraté. Vous pouvez aussi avoir été victime d'un message de phishing qui aura permis au pirate de vous voler votre mot de passe.

La personne qui accède de cette façon à votre boite mail, peut ensuite récupérer vos documents sensibles (par exemple une copie de carte d'identité, des fiches de paie ou un RIB envoyés à une administration ou à

un propriétaire pour une demande de location). Tout le nécessaire pour utiliser votre identité à votre insu et demander un crédit à la consommation par exemple !

Alors comment sécuriser correctement sa messagerie ?

Tout d'abord, utilisez un mot de passe complexe et différent pour chaque compte. Puis activez la double authentification qui vous demandera un code de confirmation en cas de tentative de connexion d'un appareil inconnu. La double authentification est un système de sécurité qui nécessite, en plus de votre mot de passe, un code envoyé par téléphone ou sur un autre compte lors d'une tentative de connexion d'un autre appareil)

Veillez également à effectuer les mises à jour de votre machine et de votre antivirus.

De plus, pour éviter d'être victime d'hameçonnage, n'ouvrez pas les courriels, pièces jointes ou liens provenant d'expéditeurs inconnus, dont le contenu du message est inhabituel ou alarmiste.

Evitez aussi de vous connecter à un ordinateur ou à un réseau Wifi publics. Et enfin, déconnectez-vous systématiquement de votre compte après utilisation. Et si malgré tout, vous vous faites pirater votre messagerie, vous pourrez trouver de l'assistance sur le site Cybermalveillance.gouv.fr.

En résumé :

- Le piratage de messagerie est la deuxième menace de cyber malveillance la plus courante,
- évitez les mots de passe trop simples et communs à plusieurs comptes,
- utilisez un mot de passe complexe et différent pour chaque compte,
- activez la double authentification,
- effectuez les mises à jour,
- n'ouvrez pas les messages inhabituels,
- déconnectez-vous.
