CYBERCRIMINALITÉ

Arnaques et escroqueries en ligne : comment les identifier et agir ?

Les escroqueries en ligne peuvent prendre plusieurs formes mais leur but est toujours le même : vous extorquer des informations et de l'argent. Mots de passe, données personnelles, coordonnées bancaires, accès à vos comptes en ligne... Même si vous pensez être un cas isolé, n'oubliez pas qu'un cybercriminel peut toucher des milliers de personnes par jour.

Comment identifier une arnaque ?

Les sujets des arnaques en ligne se renouvellent régulièrement, mais le fonctionnement reste souvent le même : vous recevez une fausse information et vous êtes invité à cliquer sur un lien pour corriger une situation qui n'existe pas. Les exemples sont nombreux :

- vous recevez un courriel ou un SMS provenant d'un expéditeur ou d'un organisme de confiance, vous invitant à cliquer sur un lien pour mettre à jour votre compte, toucher une somme ou affranchir un colis ;
- lors de votre navigation, vous découvrez un juteux filon pour investir simplement dans une crypto-monnaie (bitcoin, ethereum) ;
- quelqu'un vous contacte par téléphone ou par SMS pour vous proposer une formation grâce à vos droits et on vous accompagne dans la création de votre compte ;
- un courriel vous indique qu'on a piraté votre webcam, enregistré votre historique de navigation sur des sites pornographiques et, bien entendu, recueilli la liste de tous vos codes et contacts.


© D.R.

Vous pouvez consulter la liste noire des sites ou entités non autorisés, tenue et mise à jour par l'ACPR et l'autorité des marchés financiers (AMF).

Que signifie rançongiciel ?

Entreprises, particuliers, collectivités... Tout le monde peut subir une attaque par rançongiciels (ransomware en anglais), ces logiciels malveillants bloquent un ordinateur ou l'accès à ses fichiers et réclament le paiement d'une rançon en échange d'un code permettant de le déverrouiller. Après le paiement de la rançon (le plus souvent sous forme de cryptoactifs comme les bitcoins), les cybercriminels communiquent généralement la clé de déchiffrement, permettant de débloquer l'ordinateur ou de récupérer ses données (sans aucune garantie que cela ne se reproduise pas). Chaque logiciel malveillant a son propre fonctionnement et les méthodes de désinfection diffèrent selon le type de logiciel.

Comment réagir ?

Vous avez un doute sur le message que vous avez reçu :

- ne paniquez pas ! Vous n'avez sans doute rien de compromettant à vous reprocher ;
- ne cliquez pas sur un lien ou une pièce jointe sans être sûr de la fiabilité de son expéditeur ;
- vérifiez l'adresse de l'expéditeur : contactez-le par un autre canal ou regardez l'adresse d'expédition. Un organisme officiel aura presque systématiquement une adresse de type «ne-pas-repondre@ministere.gouv.fr» ;
- ne répondez jamais à un courriel suspect ou à du chantage, ne montrez pas à l'expéditeur que vous êtes réceptif au message et ne payez pas de demande de rançon;
- changez vos mots de passe régulièrement, évitez d'avoir le même mot de passe pour chaque compte pour empêcher les contaminations en chaîne et si possible, activez l'authentification à double facteur ;
- faites des captures d'écran et signalez le courriel ou le SMS sur le site Signal-spam.

Vous avez déjà payé ou communiqué des informations personnelles ? Vous êtes victime d'une escroquerie. Dans ce cas :

- vérifiez qui a accédé aux comptes dont vous avez communiqué les identifiants ;
- changez immédiatement les mots de passe des comptes compromis ;
- adressez-vous à votre banque pour tenter de faire annuler le paiement ;
- déposez plainte en ligne sur la plateforme THESEE ;
- présentez-vous au commissariat de police ou à la gendarmerie de votre lieu de résidence.

Bon à savoir

Vous pouvez également déposer plainte par le biais d'un courrier papier adressé au procureur de la République (« www.service-public.fr/simulateur/calcul/Porter_plainte »).

Source : masecurite.interieur.gouv.fr