

QUE FAIRE SI VOUS ÊTES VICTIME D'UNE CYBERATTAQUE OU D'UNE ARNAQUE

SOURCE OFFICIELLE À SUIVRE LU-Alert · RTL, 100.7 · 112

À FAIRE MAINTENANT

- 1 Déconnectez l'appareil touché d'internet : coupez son Wi-Fi ou débranchez le câble. N'effacez et ne supprimez rien pour l'instant ; les messages, les e-mails et les captures d'écran sont vos preuves.
- 2 Protégez d'abord votre argent. Si vous avez saisi des données de carte, payé ou donné des codes bancaires, appelez tout de suite votre banque, et l'opérateur de cartes indiqué sur votre carte (au Luxembourg, généralement Worldline), pour bloquer les cartes.
- 3 Changez vos mots de passe depuis un appareil de confiance, en commençant par votre e-mail et votre banque. Déconnectez tous les appareils que vous ne reconnaissez pas et activez la connexion en deux étapes.
- 4 Stoppez la propagation. Dites à vos contacts que votre compte ou votre numéro a été piraté, pour qu'ils ignorent les messages qui semblent venir de vous.
- 5 Signalez-le. Utilisez le service national d'aide contre la cyberfraude (cyberfraud.lu), prévenez votre banque, et déposez plainte à la police si de l'argent ou des documents ont été pris. Gardez les numéros de référence.
- 6 Ne faites confiance à aucun message sur la crise qui demande de l'argent, des codes ou des documents. Les autorités ne demandent jamais d'argent, les dons passent uniquement par des canaux annoncés à l'avance, et vous ne remettez jamais vos papiers d'identité à quelqu'un qui propose de l'aide.
- 7 Si quelqu'un en uniforme ou avec un badge est à votre porte et que quelque chose vous semble bizarre, gardez la porte fermée et appelez la police au 113. Les imposteurs copient les uniformes et les insignes.

AVANT

VERROUILLEZ VOS COMPTES

- Utilisez un mot de passe long et unique pour chaque compte et laissez un gestionnaire de mots de passe les retenir. Activez la connexion en deux étapes partout où elle existe, avant tout pour l'e-mail, la banque et les services publics.
- Activez les mises à jour automatiques sur les téléphones, les ordinateurs et le routeur, et gardez l'antivirus actif. Changez le mot de passe par défaut de chaque nouvel appareil.
- Verrouillez chaque appareil avec un code PIN, un mot de passe ou votre empreinte. Ne donnez aux applications que les autorisations dont elles ont besoin.
- Ayez plus d'un moyen de vous connecter à votre banque et aux services publics, pour qu'un téléphone ou une carte perdus ne vous bloquent pas.

- Partagez moins sur vous en ligne. Les adresses, les dates de vacances et les photos de documents aident les escrocs à paraître crédibles.

SAUVEGARDEZ CE QUE VOUS NE POUVEZ PAS PERDRE

- Copiez vos photos, vos documents et vos contacts sur un disque externe, et gardez-le débranché quand vous ne l'utilisez pas. Renouvelez la copie quand vous vérifiez votre kit, **deux fois par an, au changement d'heure**.
- Gardez sur papier les numéros dont vous auriez besoin : la ligne de blocage de carte de votre banque, votre assureur, votre médecin, les personnes que vous appelleriez. Gardez-les avec votre plan.

APPRENEZ LES SIGNES D'UNE ARNAQUE

- L'urgence, les menaces, un gain, ou une demande de cliquer, de payer ou d'envoyer une copie de

votre pièce d'identité sont des signaux d'alarme. Tout comme les fautes d'orthographe, les adresses d'expéditeur étranges et les adresses web qui ressemblent presque à la vraie.

- Ne cliquez jamais sur un lien dans un message inattendu. Tapez l'adresse vous-même, ou rappelez à un numéro que vous avez cherché, pas celui donné par le message.
- Les avertissements officiels vous parviennent par LU-Alert, la radio et les sites officiels, jamais par un message qui vous demande de payer. Voir **Alertes et sirènes**.
- Avant de transférer un avertissement, vérifiez qui l'a publié, quand et d'où, et si des sources fiables le confirment. Les images et les vidéos peuvent être créées par IA.

APRÈS

- Surveillez vos relevés bancaires et vos comptes pendant plusieurs semaines, et signalez tout de suite tout débit que vous ne reconnaissez pas.
- Nettoyez l'appareil avant de le reconnecter : lancez une analyse antivirus complète, ou

réinitialisez-le et restaurez une sauvegarde faite avant l'attaque.

- Repassez sur chaque compte : changez les mots de passe oubliés dans la précipitation, et vérifiez que l'e-mail et le numéro de récupération sont toujours les vôtres.

- Si un appareil ou un compte professionnel est concerné, prévenez le contact informatique de votre travail le jour même.
- Se sentir bête, en colère ou anxieux après une arnaque est fréquent. Parlez-en avec quelqu'un de confiance ; cela le met aussi en garde.

SI VOUS ÊTES...

AVEC DES ENFANTS

- Convenez que les enfants ne partagent jamais de mots de passe, ne paient jamais en ligne et n'envoient jamais de photos d'eux-mêmes ou de documents sans vous demander d'abord. BEE SECURE, le service national pour un usage plus sûr d'internet, a du matériel pour les familles.

ÂGÉ, OU VIVANT SEUL

- Fixez une règle de famille : personne qui tient à vous ne vous demandera jamais d'argent, un code ou une carte par téléphone ou par message. Si un appelant dit être de votre banque ou de la police, raccrochez et appelez le numéro imprimé sur votre carte.
- Gardez une carte avec ces règles à côté du téléphone.

PENDANT UNE CRISE PLUS LARGE

- Quand le courant ou les réseaux sont coupés, les cartes et les distributeurs peuvent ne plus fonctionner. Gardez de l'argent liquide à la maison : **€70** par adulte et **€30** par enfant.
- Les arnaques se multiplient en temps de crise : fausses collectes, faux agents, fausses offres d'aide. Vérifiez qui collecte, et ne donnez que par les canaux annoncés par les autorités.

RÉSUMÉ FACILE À LIRE



Déconnectez l'appareil piraté d'internet.



Appelez votre banque pour bloquer vos cartes.



Les autorités ne vous demandent jamais d'argent.



Dites à vos contacts que votre compte a été piraté.



Les vraies alertes viennent de LU-Alert et de la radio, pas d'un SMS qui demande de l'argent.