Ransomware

Votre ordinateur, vos appareils mobiles ou vos fichiers numériques sont verrouillés et une rançon vous est demandée pour les récupérer.

Que faire ?

- Interrompez votre connexion Internet (WiFi ou câblée).
- Déconnectez immédiatement tous vos autres appareils.
- Si votre appareil est totalement bloqué et qu'une rançon est réclamée, vérifiez sur www.nomoreransom.org si la clé de ce ransomware est disponible.
- Réinstallez votre appareil et utilisez une copie de sauvegarde ou de réserve pour récupérer vos données.
- N'effectuez aucun paiement : rien ne vous garantit que vous récupérerez effectivement vos données en toute sécurité.

Comment se protéger ?

- Utilisez un logiciel anti-ransomware.
- Effectuez des mises à jour.
- Scannez votre ordinateur régulièrement avec un logiciel anti-virus.
- Apprenez à reconnaître les faux messages (phishing).

Fraude à la demande d'aide financière et à l'amitié

Une personne de votre entourage ou une personne rencontrée sur Internet vous demande de l'argent.

Que faire ?

- Contactez le membre de votre famille ou la connaissance via un autre canal afin de vérifier si la demande d'aide vient de lui ou d'elle.
- Ne versez aucune somme à des personnes rencontrées en ligne ou à des gens qui subitement présentent un autre numéro de compte.
- Stoppez tout contact avec le fraudeur.

Comment se protéger ?

- Niez les demandes d'amitié de la part d'inconnus.
- Ne partagez aucune photo ou vidéo à caractère sexuel.

Phishing

Le phishing est une escroquerie en ligne à l'aide de faux e-mails, sites Internet ou messages. Les cybercriminels tentent d'abuser de votre confiance. Ils jouent avec le spectre des émotions et tentent de profiter de l'envie et de la peur.

Que faire ?

- *Si vous avez communiqué un mot de passe que vous utilisez également sur d'autres comptes, modifiez-le immédiatement.*
- *Si vous avez cliqué sur un lien qui ouvre un site Internet vous enjoignant de saisir vos données bancaires, contrôlez d'abord s'il s'agit du site officiel de votre banque. Au moindre doute, ne procédez à aucun paiement.*
- *Si vous avez effectué un téléchargement, supprimez-le et passez votre ordinateur au crible de l'anti-virus.*

Comment se protéger ?

- Apprenez à reconnaître les messages suspects.
- Réfléchissez à deux fois avant de cliquer dessus.

Piratage de compte

On parle de piratage de compte lors qu'un cyberpirate a accès aux données de connexion d'un compte en ligne. Le pirate peut alors publier des messages en votre nom ou communiquer avec vos contacts.

Que faire ?

- Vous y avez encore accès ? Modifiez votre mot de passe (aussi sur tous les autres comptes où vous utilisez ce mot de passe) et avertissez vos contacts.
- Vous n'y avez plus accès ? Utilisez les options de restauration afin de le recouvrer et modifiez ensuite tous vos mots de passe.

Comment se protéger ?

- Activez la vérification en deux étapes.
- Utilisez pour chaque compte un mot de passe (fort) différent et conservez-le dans un gestionnaire de mots de passe.
- Ne partagez jamais vos mots de passe avec des tiers.

Tech Scam

Quelqu'un qui se fait passer pour un collaborateur d'une firme ICT (Microsoft, Apple, votre service ICT) prend contact avec vous sur votre ligne fixe. L'escroc vous fait croire que votre ordinateur est confronté à un problème de sécurité et vous propose de vous aider.

Comment se protéger ?

- Méfiez-vous des appels téléphoniques provenant de sociétés qui vous demandent d'effectuer une série d'actions sur votre ordinateur.
- Ne laissez jamais quelqu'un que vous ne connaissez pas prendre le contrôle de votre ordinateur.
- N'effectuez pas de paiement lorsqu'un inconnu a pris le contrôle de votre ordinateur.

Fraude au CEO

La fraude au CEO est une forme d'escroquerie : les cybercriminels contactent une entreprise en lui demandant d'effectuer un paiement important. Les cybercriminels usurpent l'identité du CEO, du CFO ou d'une personne de confiance et demandent à un collaborateur du service financier ou comptable d'effectuer un paiement urgent.

Comment se protéger ?

- Assurer une bonne information de leurs collaborateurs et en les alertant sur ce modus operandi.
- Le service comptable applique des procédures et conventions claires pour les paiements.

Sextortion scam

Vous recevez un mail dans lequel les escrocs affirment avoir piraté votre ordinateur et avoir pris des photos intimes de vous. Les escrocs menacent de diffuser les images sur Internet si vous ne versez pas une somme d'argent.

Que faire ?

- Ne cédez pas aux demandes d'argent.
- Supprimez le message.
- Marquez le message comme SPAM ou indésirable.
- Bloquez l'expéditeur.

Qui contacter après une cyberattaque ou une escroquerie en ligne ?

La police

Si vous avez perdu de l'argent ou que vous êtes victime d'une escroquerie, déposez plainte auprès de la police locale.

Il est important de transmettre ces informations à la police:

- L'argent a disparu de votre compte en banque ? Prenez les extraits de compte.
- Vous avez eu des contacts avec quelqu'un sur les réseaux sociaux ? Faites une capture d'écran du profil du suspect et d'autres des discussions que vous avez eues.
- Vous avez ouvert un faux site Internet qui ressemblait par exemple à celui de votre banque ou d'une autre institution ? Faites une capture d'écran et emportez-la.
- Vous avez été escroqué par un site de vente en ligne ? Faites une capture d'écran de l'annonce ou de l'offre à laquelle vous avez réagi et du profil de l'escroc.
- Vous avez reçu un mail de l'escroc ? Conservez-le et imprimez-le.

Votre banque et Card Stop

Contactez votre banque et Card Stop au 070 344 344 si vous avez transmis des coordonnées bancaires, si de l'argent a disparu de votre compte bancaire ou si vous avez transféré de l'argent à un escroc.

De cette façon, les éventuelles transactions frauduleuses pourront être bloquées. Si vous souhaitez communiquer une fraude, adressez-vous à votre banque. Vous trouverez le numéro en cliquant sur ce lien : https://protegezvousenligne.be/contacter-la-banque-pour-assistance

Safeonweb

Vous avez reçu un mail ou un message suspect ?

Envoyez-le à l'adresse suspect@safeonweb.be et supprimez-le ensuite. Vous ne recevrez pas de réponse personnelle à ce mail. Les liens figurant dans le mail seront bloqués, grâce à quoi les internautes moins prudents ne tomberont pas dans le panneau. Si vous recevez un message suspect au travail, vous devez suivre les procédures en vigueur pour le phishing, comme transférer le message au service ICT.

Point de contact

Vous êtes victime d'une tromperie, d'une arnaque, d'une fraude ou d'une escroquerie ?

Faites un signalement via meldpunt.belgie.be du SPF Économie.
Votre signalement fera à chaque fois l'objet d'une réponse. Les services compétents analyseront le signalement et effectueront éventuellement une enquête.

Le Centre pour la Cybersécurité Belgique

Si votre organisation est victime d'une cyberattaque ou d'un ransomware et souhaite le signaler ou demander un avis en toute confiance, elle peut s'adresser à CERT.be, la « Cyber Emergency Respons Team » du CCB via www.cert.be.

CENTRE FOR CYBER SECURITY BELGIUM

Safeonweb.be

.be

Cyberattaques et escroquerie en ligne

De quoi s'agit-il ? Que faire en cas d'attaque ? Comment se protéger ?

Safeonweb.be