Protégez votre smartphone

1. Choisissez un code d'accès à votre appareil d'au moins 6 chiffres, utilisez l'empreinte digitale ou la reconnaissance faciale. Ainsi, si quelqu'un trouve ou vole votre smartphone, il n'aura pas accès à vos données.

2. Assurez-vous que votre smartphone et vos applications sont toujours à jour. La question de l'exécution des mises à jour vous est-elle posée ? Faites-le dès que possible. Éteignez régulièrement votre smartphone. Certaines mises à jour se font automatiquement lorsque vous redémarrez.

3. Téléchargez des applications uniquement depuis les boutiques d'applications officielles : l'App Store si vous utilisez un iPhone, le Google Play Store si vous utilisez un appareil d'une autre marque.

4. Méfiez-vous des faux SMS ou messages WhatsApp. Ils semblent provenir d'une entreprise ou d'un service public (banque, Itsme®, service des pensions,…) ou vous promettent un bonus, et ils vous incitent à cliquer sur les liens qu'ils contiennent pour obtenir vos codes bancaires afin de vider vos comptes. Soyez toujours sur vos gardes si vous recevez un message d'un numéro que vous ne connaissez pas.

5. Utilisez un antivirus sur votre appareil.

Protégez votre ordinateur

1. Apprenez à reconnaître les messages suspects. De nombreux courriels que vous recevez sont des tentatives d'escroquerie. Réfléchissez toujours à deux fois si vous recevez un message d'un inconnu et ne cliquez jamais sur un lien dans un message suspect.

2. Installez un antivirus sur votre ordinateur.

3. Mettez régulièrement à jour votre système d'exploitation et vos programmes.

4. Protégez votre ordinateur et vos comptes (par exemple, e-mail, Facebook) avec un mot de passe long d'au moins 13 caractères. Utilisez des mots de passe différents.

5. Avez-vous entendu parler de l'authentification à deux facteurs (2FA) ? Ce n'est pas difficile et c'est très sûr. Vous protégez vos comptes importants avec un double verrouillage. En plus d'un mot de passe, vous utilisez une deuxième clé, par exemple un code qui vous est envoyé par SMS.

Ne vous faites pas avoir au téléphone

1. Vous recevez un appel d'un numéro que vous ne reconnaissez pas ? Alors soyez toujours sur vos gardes.

2. Ne donnez jamais de détails personnels, de mots de passe, de codes de carte bancaire ou de codes de réponse lors d'un appel téléphonique.

3. Ne rappelez jamais les numéros inconnus. Ne répondez jamais aux appels de numéros étrangers que vous ne connaissez pas. Ne rappelez surtout pas ces numéros. Si quelqu'un a besoin de vous, il laissera un message.

4. Ne croyez pas toujours ce qu'on vous dit au téléphone. Microsoft ou toute autre entreprise technologique ne vous appellera jamais. Votre banque ne vous demandera jamais vos codes ou d'ouvrir un nouveau compte par téléphone.

5. Enregistrez les numéros des personnes que vous connaissez. Bloquez les numéros des appelants indésirables.

Que pouvez-vous faire de plus ?

Liste de contrôle

✓Je ne donne jamais d'informations personnelles, de mots de passe, de codes de carte bancaire ou de codes de réponse par courrier électronique, appel téléphonique, SMS ou médias sociaux.

✓Je télécharge l'application Safeonweb pour être alerté des nouvelles formes d'escroquerie en ligne et je suis les conseils du site safeonweb.be.

✓Je définis un code d'accès sur mon smartphone.

✓Je configure les mises à jour automatiques sur mon smartphone et mon ordinateur.

✓J'installe un antivirus sur mon smartphone et sur mon ordinateur, si je n'en ai pas déjà un.

✓J'enregistre les numéros de mes amis et de ma famille dans mon smartphone. J'enregistre également les numéros de ma banque et d'autres entreprises que je dois souvent contacter ou qui peuvent me contacter.

✓Je protège ma boîte aux lettres électronique avec l'authentification à deux facteurs (2FA).

✓Je protège mes autres comptes (Facebook, Instagram,...) avec l'authentification à deux facteurs (2FA), quand c'est possible.

ER : Miguel De Bruycker, Rue de la Loi 18, 1000 Bruxelles

Demandez de l'aide !

Vous ne savez pas par où commencer avec ces conseils ? Vous avez un doute sur un message ? Vous remarquez quelque chose d'étrange sur votre ordinateur ? Ne restez pas dans le doute ! Demandez de l'aide à vos amis ou à votre famille qui ont plus d'expérience.

Vous avez besoin de plus d'informations ? Jetez un coup d'œil à www.safeonweb.be et à notre brochure « Cyberattaques et escroquerie en ligne ». Téléchargez notre app Safeonweb pour être averti des dernières menaces.

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.

Point de contact

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

Faites un signalement via pointdecontact.belgique.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

Safeonweb est un service du Centre pour la Cybersécurité Belgique.

CENTRE FOR CYBER SECURITY BELGIUM

Safeonweb.be

.be

Comment déjouer les escrocs ?

Voici 3 x 5 conseils pour vous protéger

Safeonweb.be