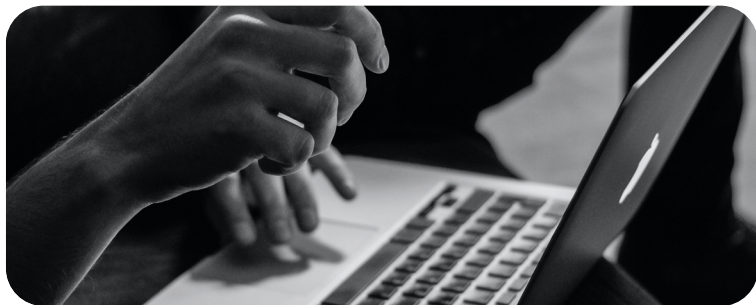


Cybersécurité

La protection numérique,
un réflexe à adopter



Bienvenue dans l'EDUbox Cybersécurité !

Une bonne part de notre vie se déroule en ligne. C'est très pratique ! Mais cela demande aussi d'être très prudent(e), car partout, des hackers nous guettent pour s'emparer de nos données ou nos biens. Mais comment procède exactement un hacker ? Et comment se protéger contre eux ? Mets-toi dans la peau d'un hacker éthique et apprend tout ce qu'il faut savoir !

Bonne chance !

Notre EDUbox a pu être réalisée avec l'appui de



Ce projet a été financé avec le soutien de la Commission européenne. Cette publication reflète uniquement les opinions de l'auteur et le comité ne peut être tenu responsable de l'utilisation qui pourrait être faite des informations qu'elle contient.

01

J'ai été piraté(e) !

1. Empreinte numérique

Une bonne part de notre vie se déroule en ligne. Il suffit de penser aux photos et aux histoires qu'on partage sur les réseaux sociaux. Ou encore aux messages envoyés à des ami(e)s, aux courriels adressés aux profs, à la musique et aux séries qu'on écoute ou regarde...

Toutes ces activités **laissent des traces sur internet**. La quantité de traces et de données qu'on laisse derrière soi, c'est ce qu'on appelle **l'empreinte numérique**. Et plus on peut retrouver de données, plus l'empreinte numérique est importante.

Examinons un peu l'importance de ton empreinte numérique !

À faire

Tester son empreinte numérique

1. **Ouvre** un moteur de recherche (comme Google) et introduis ton nom complet.
2. **Examine les résultats.** Pas seulement la première page mais aussi les suivantes. Et vérifie aussi les images et les vidéos.
3. Essaie de trouver **au moins 1 trace surprenante.**

À faire

Poussons un peu la recherche et voyons si on trouve tes mots de passe sur internet. Le **site web 'Have I Been Pwned?'** rassemble toutes les données piratées avec des éléments personnels.



1. **Ouvre un moteur de recherche.**
 2. Donne d'abord ton **adresse e-mail personnelle**, ensuite **l'adresse e-mail de ton école**.
 3. Même chose pour ton **numéro de téléphone**, avec le code du pays (par ex. +32470123456).
 4. Enfin, vérifie aussi **l'adresse e-mail de tes parents**.
- ☒ Si l'écran devient **vert** en bas, ton adresse e-mail ou numéro de téléphone ne sont pas impliqués dans une fuite de données.
 - ☐ Si l'écran devient **rouge**, tes données ont été piratées. Il est urgent de changer tes mots de passe !

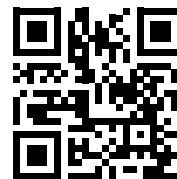
Tu as trouvé **beaucoup de traces de toi-même** en ligne ? Des infos privées ou même un mot de passe ?

On ne laisse pas ces traces uniquement par nos activités sur les réseaux sociaux. Il suffit de signer une pétition ou de réagir à une vidéo pour augmenter son empreinte numérique. En faisant du shopping en ligne, on révèle ce qu'on aime et on laisse ses données de paiement.

À faire

Es-tu à l'abri des hackers ?

- ☐ Scanne le code QR et **réponds au questionnaire.**
- ☐ Découvre ensuite **les résultats** sur l'écran.



Discute en groupe des questions suivantes



- ☐ Es-tu surpris(e) par le résultat du questionnaire ? Pourquoi (pas) ?
- ☐ Quelles données personnelles doivent absolument être protégées des abus ?
- ☐ Quelles infos voudrais-tu protéger davantage ?



2. Qu'est-ce qu'un hacker ?

Les informations que tu trouves sur toi-même, sont aussi accessibles à d'autres. Les réseaux sociaux et des entreprises s'intéressent à ces données, par ex. pour t'adresser de la publicité personnalisée.

Mais il y a aussi **des gens malintentionnés** qui recherchent ces données. Soit ces hackers les scrutent sur internet, soit ils les volent dans les entreprises. Grâce à ces infos, ils arrivent à te pirater bien plus facilement.



Exemples d'entreprises qui ont déjà été piratées



2014

Snapchat

4,6 millions de comptes

Aux débuts de Snapchat, des hackers ont réussi à voler les **noms et numéros de téléphone** de 4,6 millions d'utilisateurs.



2019

Facebook

533 millions d'utilisateurs

Les numéros de téléphone et les noms de 533 millions d'utilisateurs de Facebook ont fuité à la suite d'un piratage.



2019

Alibaba

1,1 milliard de éléments d'information

Un hacker a su voler au total plus de **1 milliard de données personnelles** du géant de l'e-commerce chinois Alibaba. Il s'agissait entre autre de numéros de téléphone.

Mais en quoi consiste exactement le hacking ou piratage ?

Le mot 'hacker' n'a toujours pas de définition précise. On parle en général d'un hacking ou piratage **quand quelqu'un s'introduit illégalement dans un système ou un compte informatique**. Le but des hackers est de voler des données, d'installer des virus, d'espionner, etc.

Ces piratages se font à trois niveaux différents. On les classe en **3 catégories**.



**Un hacking dans la
vie personnelle**



**Une cyberguerre
internationale**



**Des cyberattaques contre
notre style de vivre**

À faire

Tu vas découvrir **différents exemples** des 3 catégories de piratage. Explique-les aux autres. Mais d'abord, l'ordinateur doit décider à qui revient quel exemple !

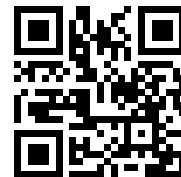
Étape n° 1 : Répartir les exemples

1. Ouvre le site web sur un ordinateur portable pour répartir les exemples.
2. Imagine un nom pour votre groupe et crée une pièce.
3. Scanne tous le code de la pièce avec ton smartphone et suis les étapes.

Étape n° 2 : Explique aux autres

1. Ouvre la pièce quand tous les noms apparaissent à l'écran.
2. Explique l'exemple quand c'est à toi. Utilise tes propres mots.
3. Clique sur la navigation en haut pour passer à l'exemple suivant.

nws.vrt.be/3Pq3I4m

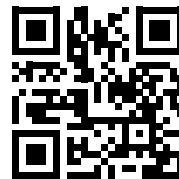


Dans la société, il y a **des problèmes** de cybersécurité **à tous les niveaux**. C'est pourquoi le Ministère de la Défense a créé une nouvelle section pour combattre les hackers.



Vidéo

Maintenant, regarde la vidéo suivante.
le Ministère de la Défense belge lutte quotiennement contre des cyberattaques.



Discussion en classe

Il t'est déjà arrivé(e) d'être victime d'un piratage ? **Discute des questions suivantes en classe.**

- ☐ As-tu déjà été piraté(e) ? Ou as-tu déjà vécu(e) un truc suspect sur un de tes comptes sur les réseaux sociaux ?
- ☐ As-tu des ami(e)s ou des proches qui ont déjà été piraté(e)s ?
- ☐ Que s'est-il passé exactement ? Accès bloqué ? Appels téléphoniques bizarres ? Argent volé ? Messages envoyés sous ton nom ?
- ☐ Comment ces hackers ont-ils obtenu ces informations selon toi ?



02

**Dans la tête
d'un hacker**

1. Criminel ou non ?

Il y a tous les jours des victimes de hacking ou piratage. Parfois parce que leurs données ont été volées, parfois parce qu'elles ont été imprudentes. C'est pourquoi tout le monde doit **participer à la lutte pour la protection de notre identité.**

C'est comparable à **la sécurité d'une habitation.** Les gens ferment toutes les fenêtres et les portes quand ils sortent. Certains ont même des systèmes d'alarme. Cela effraie les cambrioleurs.

Dans cette partie, on t'apprend à penser comme un hacker.

Sois bien attentif(ve) ! Plus tard, tu auras besoin de ces connaissances pour démasquer des hackers.



Les cybercriminels

Les cybercriminels ou “black hats” sont des hackers qui dérobent nos données numériques ou s’introduisent dans nos systèmes. **C’est illégal.** Ces délits risquent de leur coûter une amende ou même une peine de prison.

En améliorant la cybersécurité de nos systèmes, on complique les choses pour ces criminels.

Le groupe cybercriminel ransomware Lockbit menace de diffuser des données volées à Vivalia, l’intercommunale réagit

Australie : des hackers menacent de divulguer les données médicales de célébrités

Les jeunes sont plus susceptibles que leurs aînés de se faire arnaquer en ligne

Les pirates informatiques exigeraient de Mediamarkt une rançon de 50 millions de dollars

Tentative de piratage de la chancellerie du Premier ministre : une plainte a été déposée

Tentative de phishing : des escrocs usurpent l’identité de la présidente d’Europol



Les hackers éthiques

Il existe cependant aussi des **hackeurs éthiques** ou **“white hats”**.

Ceux-ci détectent les lacunes dans notre sécurité numérique. Eux aussi essaient de s’infiltrer dans les systèmes ou appareils d’entreprises ou de pouvoirs publics.

Mais au lieu d’abuser de ces données, **ils informent l’entreprise ou l’administration concernée**.

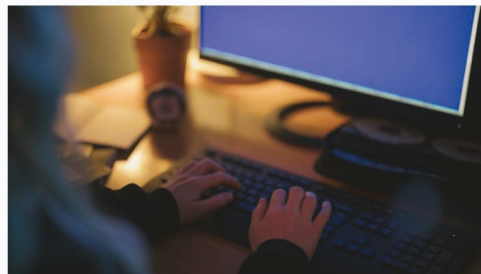
S’ils détectent une lacune importante dans un système, ils obtiennent parfois **une récompense**. Cela aide les entreprises et les administrations à améliorer leurs systèmes.

À Tournai, des hackers éthiques veulent partager leurs connaissances pour mieux lutter contre les menaces



Quézac : les hackers éthiques, ces pros de la cybersécurité au rôle primordial mais encore méconnu

Un hacker tournaisien vous révèle ses secrets pour éviter le piratage



© Pexels

Où se situe la limite ?

Un hacker de Malines s'est retrouvé en prison pour avoir piraté le site web de la compagnie aérienne American Airlines. Il a commandé pour plus de 100 000 dollars de billets d'avion sans les payer. Malgré qu'il n'ait pas utilisé ces billets, le juge l'a condamné.

Un Malinois condamné pour avoir piraté le site d'American Airlines

Pour en savoir plus sur cette histoire :



À faire

Discute en groupe des questions suivantes.

- ☐ Penses-tu que ce hacker flamand soit un cybercriminel ?
- ☐ Qu'aurait-il dû faire pour être un hacker éthique ?
- ☐ Où se situe à tes yeux la limite entre un criminel et un hacker éthique ?



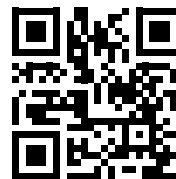
Certaines entreprises permettent de faire quelques tests, mais le mieux, c'est de demander l'autorisation d'examiner leur cybersécurité.

Inti De Ceukelaire

Vidéo

Maintenant, regarde la vidéo suivante.

Notre hacker éthique Inti De Ceukelaire explique ce qu'est le piratage éthique et comment il procède.



2. Les astuces du hackeur

Les hackers disposent d'un arsenal de trucs et astuces, et un hacking est souvent une combinaison de plusieurs astuces. Cela vaut tant pour les cybercriminels que pour les hackers éthiques. **La différence se situe dans ce qu'ils en font** : leur objectif est-il de nuire ou non ?

Ces astuces se divisent en **2 catégories** :

- ☐ Pour les **astuces techniques** le hacker se sert d'outils techniques. Tout système d'ordinateur fonctionne selon un code avec des 0 et des 1. Ce code peut être déchiffré.
- ☐ En outre, un hacker emploie des **ruses sociales** pour nous duper, par ex. en nous convainquant par la ruse à partager des données personnelles.

Comment les hackers se servent-ils de ces astuces ?

Entraîne-toi avec les cartes suivantes et deviens un hacker éthique ! Suis ta progression sur la barre en bas.

Comment un hacker sait-il quels sites je visite ?

Astuce technique : un **logiciel malveillant ou maliciel**

On appelle maliciel **tout programme ou fichier endommageant intentionnellement** un appareil ou un réseau. Ouvert ou installé généralement par accident, il peut espionner notre comportement sur Internet et récolter des données personnelles.

Il en existe **plusieurs sortes** : certains maliciels installent un virus qui enregistre par ex. quelles touches on utilise pour taper un mot de passe, d'autres te conduisent toujours vers des sites bizarres pleins de publicités.



Parfois, des bouts de maliciels sont cachés dans des programmes utiles en soi. On les appelle des **chevaux de Troie**. Télécharge donc toujours des programmes à partir des de appstores officiels !



Maliciel



Comment un hacker augmente-t-il ses chances de succès ?

Astuce technique : le spam

Un hacker veut gagner de l'argent. Pour augmenter ses chances de succès, il essaie d'atteindre un maximum de gens. Il envoie donc des spams en masse à des adresses récupérées en ligne. Par ce biais, il essaie de vendre quelque chose ou il demande de l'argent, soi-disant pour une bonne cause.

En soi, ces courriels ne sont pas nuisibles. Mais parfois, ils contiennent un lien et en cliquant sur ce lien, on risque d'installer un maliciel sur son ordinateur.



La plupart des comptes de messagerie prévoient **un dossier recueillant automatiquement les spams.** Cela n'exclut pas que certains spams arrivent quand même dans la boîte de réception normale.



Maliciel



Spam



Comment un hacker triche-t-il dans un nouveau jeu ?

Astuce technique : **surcharge du système**

Quand **beaucoup de monde surfe en même temps** vers un site web, il risque au pire de n'être plus accessible. Un hacker peut simuler intentionnellement cette situation en dirigeant massivement **un réseau d'ordinateurs piratés** vers un site web. On appelle cela une **attaque DDOS**.

Un gamer peut donc tricher en lançant une attaque DDOS vers son adversaire, qui ralentit ou bloque même son serveur. D'autres gamers essaient d'adapter le logiciel.



Cyberattaque contre Belnet : investir dans la cybersécurité est primordial, selon le patron des renseignements militaires

06 mai 2021 à 09:36 · ⌚ 3 min

Par Africa Gordillo

Belgique

Info

Internet

CYBERATTQUE

Informatique



Maliciel



Spam



Surcharge
du système



Comment un hacker devine-t-il mon mot de passe ?

Astuce technique : **Scripts à haute puissance de calcul**

Un script est un programme de hacker capable **d'exécuter automatiquement certaines actions**. Il existe des scripts qui testent très vite et par eux-mêmes toutes les combinaisons de lettres pour trouver un mot de passe.

Ces scripts ont de multiples fonctions : certains envoient automatiquement des spams à toute une série d'adresses e-mail.



Maliciel



Spam



Surcharge
du système



Scripts



Comment un hacker sait-il où j'habite ?

Astuce technique : **recherche de métadonnées**

Outre l'image en elle-même, une photo comprend de nombreuses autres infos, comme la date et l'heure de la prise et les réglages de la caméra. On appelle ça les métadonnées. Si la géolocalisation de l'appareil est enclenchée, le lieu où la photo a été prise également. Un hacker peut s'emparer de cette information à partir d'une photo de chez toi.



Jeudi 1 décembre 2022 à 08:28

[Ajuster](#)

IMG_3369

Apple iPhone 13 mini

HEIF



Appareil photo grand angle — 26 mm f1.6

12 MP • 3024 × 4032 • 1,9 Mo

ISO 500

26 mm

0 ev

f1.6

1/33 s



[Charleroi >](#)

[Ajuster](#)



Maliciel



Spam



Surcharge
du système



Scripts



Recherche de
métadonnées



Comment un hacker trouve-t-il mes données de connexion ?

Ruse sociale : l'hameçonnage

Un hacker **se présente comme une entreprise ou une autre personne** et il nous contacte par **e-mail, téléphone ou SMS**. En nous faisant cliquer sur un lien et en demandant des infos personnelles, il connaît nos données de connexion.

Les hackers imitent de mieux en mieux les sites web, de sorte qu'on ne se rend pas facilement compte qu'on est sur un faux site web.



Décrouve ici une nouvelle vague de SMS frauduleux:



Maliciel



Spam



Surcharge
du système



Scripts



Recherche de Hameçonnage
métadonnées



Comment un hacker vole-t-il de l'argent de mon compte ?

Ruse sociale : **spoofing** ou **usurpation d'identité**

Spoofing signifie littéralement 'imiter'. Par cette astuce, l'escroc adopte **une autre identité**. Il se présente, par ex. au téléphone, comme un collaborateur de la banque. Il manipule aussi le numéro de téléphone de sorte qu'on croit vraiment que l'appel vient de la banque. Si on confie ses données de carte bancaire à cette personne, elle peut voler l'argent de notre compte.



Chaque mois on compte en moyenne **700 cas de fraude à l'identité en Belgique**. Des documents falsifiés ou volés servent à commettre différents types de délits: immigration illégale, fraude sociale ou escroquerie. Depuis dix ans, cette pratique est d'ailleurs en recrudescence.

Lorsque ces documents sont volés, la personne dont l'identité a été usurpée se retrouve alors dans une situation très peu confortable. Michel en a fait l'amère expérience. Et pourtant... sa mésaventure a débuté d'une façon tout à fait banale: par un simple vol de portefeuille.

” Je devais sans cesse me justifier



Maliciel



Spam



Surcharge
du système



Scripts



Recherche de Hameçonnage
métadonnées



Spoofing



Comment un hacker gagne-t-il de l'argent avec des images nues ?

Ruse sociale : **fraude à l'amitié**

Un hacker se sert **d'un profil faux ou usurpé pour contacter quelqu'un en ligne**. Au bout d'un moment, quand on fait confiance à ce profil, ce hacker propose d'échanger des photos ou des vidéos nues. Dès qu'il les a en sa possession, il menace de les envoyer à ta famille et tes amis, à moins qu'on le paie. Il exploite donc nos émotions pour nous soutirer de l'argent.



Maliciel



Spam



Surcharge
du système



Scripts



Recherche de Hameçonnage
métadonnées



Spoofing



Fraude à
l'amitié

Résumé

Les hackers se servent des **astuces techniques** et **ruses sociales** suivantes :

Astuces techniques



Maliciel



Spam



Surcharge
du système



Scripts



Recherche de
métadonnées

Ruses sociales



Hameçonnage



Spoofing

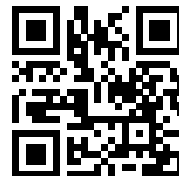


Fraude à
l'amitié

À faire

Un puzzle ! Essaie de relier les **exemples de piratage** avec les astuces correspondantes.

- ☐ **Ouvre le plateau** sur un ordinateur portable.
- ☐ Indique **une astuce et un exemple** de piratage selon toi.
- ☐ Si la réponse est correcte, ils disparaissent du plateau.
- ☐ Continue le puzzle **jusqu'à ce que le plateau soit vide.**



nws.vrt.be/3Pq3l4m

03

Au travail

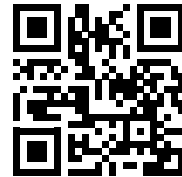
1. Cherche les lacunes dans le système

A toi de jouer !

Vidéo

Regarde la vidéo suivante.

Notre hacker éthique Inti a une mission à te confier.



À faire

La police a besoin de ton aide. Sais-tu comment les cybercriminels s'y sont pris ?



- ☐ **Ouvre le simulateur** en scannant le code QR.
- ☐ Parcoure le simulateur **étape par étape**.
- ☐ **Il est possible de faire des allers-retours !** Certaines données sont peut-être très bien cachées.

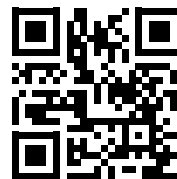
Le simulateur a été développé par Tree company, un bureau qui se propose d'informer et d'impliquer les gens dans des thèmes de société à l'aide d'outils en ligne.





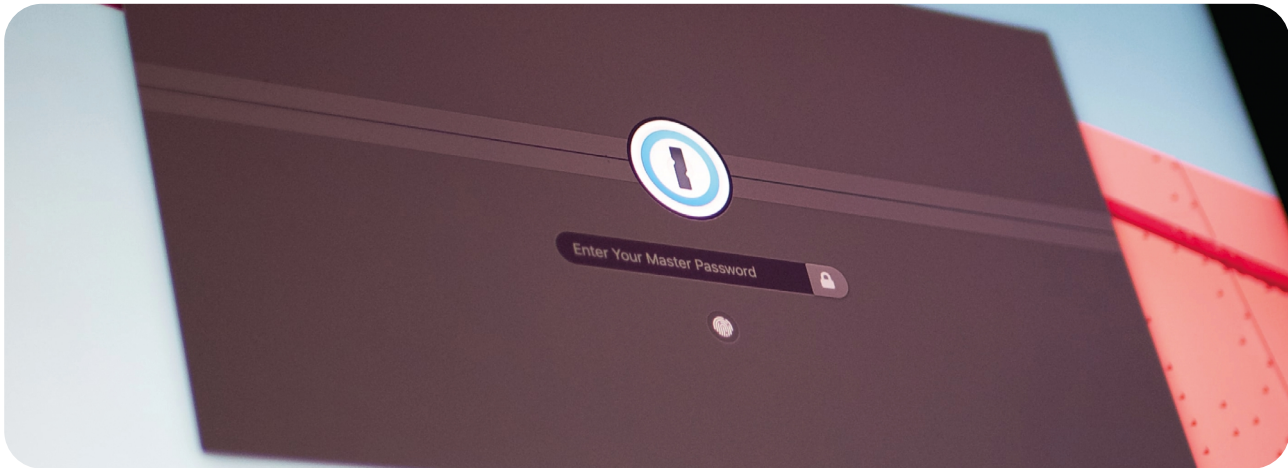
Vidéo

Regarde la vidéo suivante.
Notre hacker éthique Inti résume
ce que tu as fait.



2. Deviens un(e) expert(e)

Voici encore quelques exercices **pour renforcer tes aptitudes**. Non seulement, elles feront de toi un(e) expert(e) en piratage éthique, mais tu reconnaîtras aussi toujours mieux les astuces utilisées par les hackers !



Mission n° 1 : Détecte l'hameçonnage

Lequel des e-mails ci-dessous est de l'hameçonnage ? Comment le savoir ?

De : Bpost bc55f@bokiers.pt
Sujet : Problème de livraison avec votre colis !!!
Date : Octobre 1, 2022 à 12:47
À : quinten@gmail.com



Problème de livraison avec votre colis B-Post.

Cher client,

Votre colis portant le numéro 155019624022227 ne peut être livré le 01-10-2022 en raison de frais de douanes impayés.

Une nouvelle date de livraison est prévue entre le 03-10-2022 et le 04-10-2022.

Un montant de 4,26 EUR reste impayé.

Confirmation d'expédition

Vous recevrez un e-mail et un sms de confirmation après la confirmation de votre paiement.

- **IMPORTANT** : Si votre paiement n'a pas été effectué dans les 24 heures, votre colis restera bloqué à la douane et sera automatiquement renvoyé à l'expéditeur.

Le service client de Bpost.

N noreply@ing.be
À : Gwenaelle DEKEGELEER

① En cas de problème lié à l'affichage de ce message, cliquez ici pour l'afficher dans un navigateur web.

14-0

Chère Madame DEKEGELEER,

Merci d'avoir activé l'**app ING Banking** sur votre appareil mobile !

Dès à présent, vous pouvez :

- explorer ses **nombreuses possibilités**
- découvrir d'autres **produits ING**
- vérifier vos **comptes** et effectuer des **virements en euros (SEPA)**
- appeler ING **directement** via votre **app ING Banking**
- accéder à une multitude de **services**.

Vous avez réactivé l'app suite au blocage de votre accès ? Utilisez-la comme avant !

Vous n'êtes pas à l'origine cette activation ?

Bloquez immédiatement votre carte de débit ING en appelant **CARD STOP au +32 70 344 344 et le numéro ING qui se trouve au dos de votre carte.**

Plus d'info

Allez sur ing.be/fraude pour consulter les recommandations de nos experts en matière de lutte contre la fraude.

Des questions ?

Cet e-mail est généré automatiquement. Pour toute question, appelez le **Service Client au +32 2 464 60 02**. Nos collaborateurs vous répondront avec plaisir du lundi au vendredi de 8 à 20h et le samedi de 9 à 17h.

Cordialement,

Frank Plehiers
Directeur Klientendienst

Mission n° 1 : la solution

Check l'expéditeur

Tout le monde connaît Bpost. Mais regardez bien **l'adresse e-mail de l'expéditeur** : l'e-mail vient d'une adresse portugaise (@boksters.pt). C'est très étrange.

Question bizarre

Des frais de douane concernent un colis venant de l'étranger. As-tu commandé quelque chose à l'étranger ? Tu attends un colis ? Ou cela ne te dit rien ? Si **le message est inattendu**, il s'agit probablement d'hameçonnage.

On met la pression

Méfie-toi si on te demande **de réagir vite**. Dans cet e-mail, il est 'IMPORTANT' de payer 'dans les 24 heures'. Les escrocs essaient ainsi de ne pas te laisser le temps de réfléchir.

De: Bpost bc59f@boksters.pt
Sujet: Problème de livraison avec votre colis !!!
Date : Octobre 1, 2022 à 12:47
A : quinten@gmail.com



Problème de livraison avec votre colis B-Post.

Cher client,

Votre colis portant le numéro **155019624022227** ne peut être livré le 01-10-2022 en raison de frais de douanes impayés.

Une nouvelle date de livraison est prévue entre le 03-10-2022 et le 04-10-2022.

Un montant de 4,26 EUR reste impayé.

Confirmation d'expédition

Vous recevrez un e-mail et un sms de confirmation après la confirmation de votre paiement.

IMPORTANT : Si votre paiement n'a pas été effectué dans les 24 heures, votre colis restera bloqué à la douane et sera automatiquement renvoyé à l'expéditeur.

Le service client de Bpost.

Pas de nom

Les escrocs envoient souvent le même message à plein de gens en même temps. C'est pourquoi ils s'adressent à un 'cher client' et jamais à toi **personnellement**.

Le lien est erroné

Les faux messages contiennent souvent un lien où il faut cliquer. Ce lien conduit alors vers un site web où il faut remplir des données. Ces sites sont souvent très bien imités. Vérifie donc si le **nom de domaine est exact**: www.bpost.be est exact, mais pas www.bpost-envois.be

Mission n° 2 : le meilleur mot de passe

Recherche en ligne quels sont les mots de passe les plus utilisés. Cela t'indique lesquels il vaut mieux éviter.

Mais qu'est-ce qu'il faut alors pour composer un bon mot de passe ?

Réfléchis en groupe pour imaginer quelques règles. Ensuite, chacun(e) compose un solide mot de passe.

Astuces pour composer des mots de passe solides

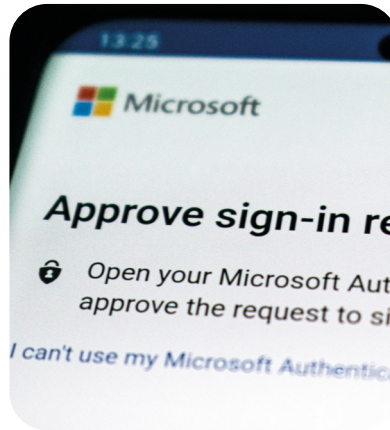
- ✓ **Utilise pour chaque compte un mot de passe différent.**
- ✓ Imagine **une phrase secrète** au lieu d'un mot de passe et change les lettres en symboles et chiffres. Par ex. "Ceci = mon mot de passe pour ma sécurité sur internet!" ou "Ch@ngeL3sL3ttr3s3n\$Ymb0l3s3tCh1ffr3e\$C0mm3C3c1"
- ✓ Plus il y a de caractères, mieux c'est : **un minimum de 12 est conseillé.**
- ✓ Utilise des minuscules, majuscules, chiffres, caractères spéciaux et espaces.
- ✓ N'utilise jamais **des infos personnelles**, comme un nom de famille ou celui du chien, une date de naissance, un numéro de téléphone, etc.
- ✓ Ne jamais choisir **des mots typiques** comme 'motdepasse' et 'admin' ou des séries comme '12345' et 'azerty'.

3. Comment me protéger ?

Pour ne laisser aucune chance aux pirates, il est important de bien protéger toutes ses données. Voici les **3 règles de base** pour se protéger :



1. Un gestionnaire de mots de passe



2. Une authentification à deux facteurs

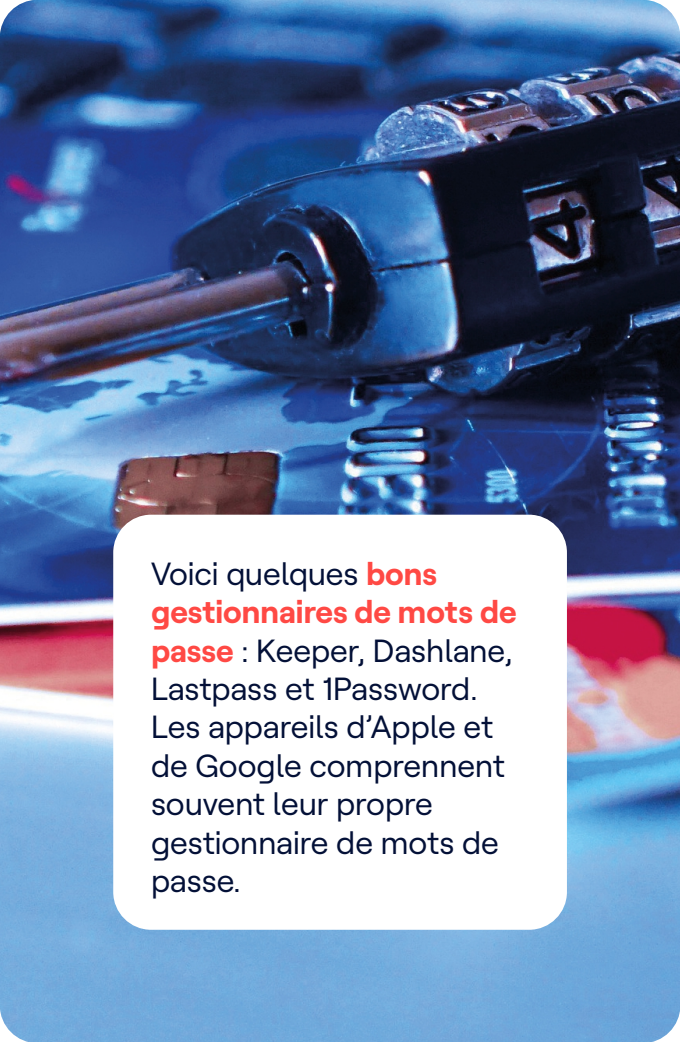


3. Reconnaître les faux messages

Gestionnaire de mots de passe

Compose toujours **un mot de passe le plus long possible**, et différent pour chaque compte.

Rassemble tous ces mots de passe dans un **gestionnaire de mots de passe**. On y enregistre tous les mots de passe et il suffit dès lors de retenir le mot de passe (très solide !) du gestionnaire. En plus, ce gestionnaire génère lui-même des mots de passe hyper longs et aléatoires qu'il remplit automatiquement quand on veut se connecter. C'est super pratique !



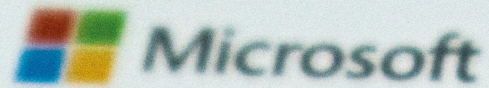
Voici quelques **bons gestionnaires de mots de passe** : Keeper, Dashlane, Lastpass et 1Password. Les appareils d'Apple et de Google comprennent souvent leur propre gestionnaire de mots de passe.

Authentification à deux facteurs

Une authentification à deux facteurs (2FA) vaut encore mieux qu'un bon mot de passe. Celle-ci **combine deux étapes** pour accéder à un compte.

La 2FA utilise le plus souvent une chose qu'on sait (p. ex. un mot de passe) et une chose qu'on a (p. ex. un téléphone portable) ou qu'on "est" (par ex. une empreinte digitale). La **première étape** consiste à se connecter avec un mot de passe. A la **deuxième étape**, ce compte envoie un code à notre téléphone portable, qu'il faut remplir pour avoir accès.

Choisis toujours la 2FA si cette option existe !



Approve sign-



Open your Microsoft
approve the request

can't use my Microsoft Au



Reconnaître les faux messages

Il faut toujours se méfier des messages qui demandent de **cliquer sur un lien** ou de **télécharger une pièce jointe**. Il y a de grandes chances qu'il s'agisse d'un faux message.

Pour **reconnaître** ce genre de messages, vérifiez d'abord l'expéditeur. Méfie-toi si tu ne connais pas l'entreprise ou si on demande de réagir vite. Contrôle le lien : si l'adresse web te semble suspecte, c'est probablement un faux.

04

**Comment contrer
les hackers ?**

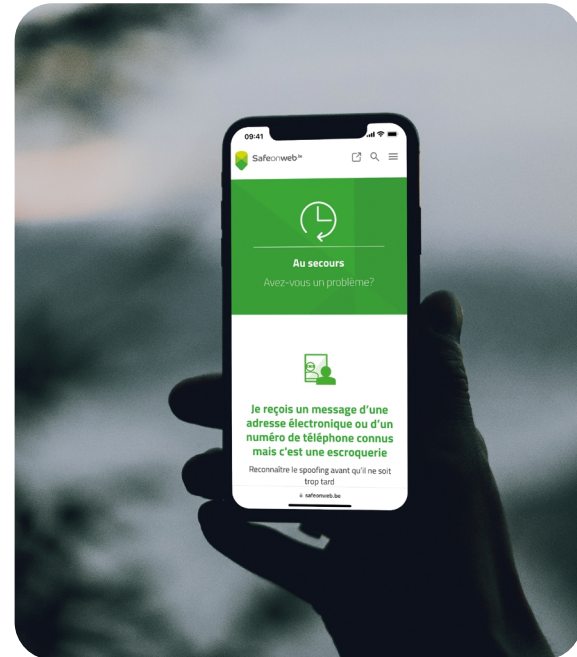
1. Check-list cybersécurité

Un autre moyen de faire obstacle aux hackers, **c'est en accordant une plus grande attention à sa propre cybersécurité**. Tout comme on veille à la fermeture des portes et des fenêtres en quittant la maison.

- ☐ Utilise **un gestionnaire de mots de passe**.
- ☐ Enregistre pour chaque compte un **mot de passe unique et solide** dans le gestionnaire.
- ☐ Sers-toi si possible d'une **authentification à deux facteurs**.
- ☐ Adapte tes **paramètres de confidentialité** sur les réseaux sociaux : tu peux définir entre autre qui peut regarder ton profil et qui peut t'envoyer des messages.
- ☐ Attention au **téléchargement d'applis, de programmes ou de pièces jointes** ne provenant pas d'une source officielle. Il y a de fortes chances qu'il s'agisse d'un virus.
- ☐ Installe **un logiciel antivirus** sur tous tes appareils et lance un scan sécurité.
- ☐ Active la **mise à jour automatique** du logiciel. Ou contrôle régulièrement toi-même si une appli, un programme ou un appareil a besoin d'une mise à jour.
- ☐ Fais régulièrement des **sauvegardes** de fichiers, de photos et de vidéos importants pour toi, soit sur le Cloud soit sur un disque dur externe.
- ☐ Réfléchis bien avant de mettre des choses en ligne. Le bouton '**supprimer**' n'existe pas sur internet !
- ☐ Sois **toujours méfiant(e)** ! Si quelque chose semble trop beau pour être vrai, c'est très probablement le cas !
- ☐ Change toujours immédiatement **le mot de passe standard de nouveaux appareils**.

2. Victime de piratage ?

Ce site web propose de l'aide en cas de problèmes de cybersécurité :
<https://www.safeonweb.be/fr/au-secours>



3. Notre responsabilité à tous

Chacun(e) est personnellement responsable de la protection de ses réseaux et appareils. Mais la société a aussi besoin de gens qui font de **la cybersécurité leur métier**. Les universités belges aussi s'engagent dans la recherche en matière de cybersécurité. Elles investissent dans de **nouvelles technologies**. C'est essentiel, car les cybercriminels aussi inventent sans cesse de meilleures manières pour attaquer nos systèmes.

Lorsque chacun(e) de nous lutte contre les pirates informatiques, individuellement et avec l'aide d'experts, nous sommes mieux armés contre toutes les formes de cybercriminalité.

Vidéo

Regarde la vidéo suivante.

Jennifer Nyembo passe en revue les moyens technologiques dont nous disposons pour améliorer notre sécurité en ligne.



05

En savoir plus



Tu veux en **savoir plus** sur la cybersécurité après avoir travaillé avec cette EDUbox ? Cette dernière partie propose toute une série de liens utiles pour en savoir plus !

As-tu un mot de passe fort ?

- ☐ www.rtbef.be/article/la-reelle-force-d-un-mot-de-passe-11004899
- ☐ www.rtbef.be/article/internet-un-nouveau-coffre-fort-pour-vos-mots-de-passe-10511677

Teste la force de ton mot de passe : campagne.safeonweb.be/fr/indice-de-sante-digitale

Les dangers des appareils connectés

Les appareils connectés à Internet ne sont pas toujours sécurisés. Découvre ici quelques conseils de base à prendre en compte. C'est de cette manière que tu réduiras la probabilité que les voleurs puissent avoir un aperçu de ton habitation.

www.besafe.be/fr/vol/appareils-connectes

Le site Je décide

www.jedecide.be/les-jeunes

Vidéo : Jeunes hackers éthiques

Les étudiants en cybersécurité de toute l'Europe s'affrontent dans le cadre du **European Cybersecurity Challenge 2021**. Dans cette vidéo tu rencontres l'équipe Belge des '**Belgian Red Daemons**'. www.youtube.com/watch?v=P2eTgRvn8Vw

Poser des questions ?

Tout le monde s'entraide dans la CyberSquad. Tu peux poser des questions (anonymement) à d'autres jeunes et toi-même aider les autres. Tu peux y **trouver toutes sortes de questions et de solutions** pour tous les problèmes que tu peux rencontrer en ligne.

☐ cybersquad.be/

☐ childfocus.be/fr-be/S%C3%A9curit%C3%A9-en-ligne/Jeunes

Témoignages : La semaine du numérique

Sur le site de **la semaine du numérique** tu trouves de nombreux témoignages intéressants. www.lasemaine numerique.be/-Actualites-.html

Articles d'actualité : le site RTBF.be

- ☐ www.rtbef.be/article/sur-quel-reseau-social-trouve-t-on-le-plus-d-arnaques-11118798
- ☐ www.rtbef.be/article/phishing-nouvelle-vague-de-sms-frauduleux-concernant-itsme-10911215
- ☐ www.rtbef.be/article/market-place-vinted-2ememain-de-faux-acheteurs-veulent-vider-votre-compte-bancaire-10918788
- ☐ www.rtbef.be/article/tiktok-nouvel-outil-des-pirates-11091456

Safe on web

Un problème au niveau de ta cybersécurité ? Tu veux connaître ton niveau de sécurité en ligne ? Ou tu recherches d'autres astuces pour surfer en toute sécurité ? **Safe on web** t'explique tout ce qu'il faut savoir ! Ce site informe et conseille tous les citoyens belges d'une manière efficace et correcte sur la cybersécurité et la sécurité en ligne.
www.safeonweb.be/fr

Acheter en ligne en toute sécurité

Tu aimes acheter en ligne et tu veux t'assurer qu'une **boutique en ligne soit fiable** ? Le site web suivant t'aide à faire des achats en ligne en toute sécurité.
www.dnsbelgium.be/fr/nouvelles/acheter-en-ligne-en-toute-securite