Financé par
l'Union européenne

DigiSkiPasS – Passeport de compétences numériques pour les seniors

2023-1-BE01-KA210-ADU-000153530

www.digiskipass.com

Financé par
l'Union européenne

CONNAÎTRE ET APPLIQUER LA CYBERSÉCURITÉ

Financé par
l'Union européenne

SÉCURITÉ DE L'APPAREIL

MALWARE

Malware est l'abréviation de « logiciel malveillant » et de tout autre logiciel capable d'entraver le fonctionnement d'ordinateurs ou d'appareils mobiles, d'acquérir des informations sensibles, de permettre l'accès à des systèmes privés ou de forcer l'affichage de publicités indésirables. Certains d'entre eux sont inoffensifs, mais d'autres peuvent causer des dommages importants.

From: Judy Kutayiah <sale@gdayusa.com>
Subject: Package reference: 7943 1570 7625 9066
To:

Dear Client,

You have a package coming.
This message was delivered to inform you that your package is transmitted to our distribution facility. To verify the actual status of a shipment, **please click here to view an detailed invoice**.

OUR COMPANY IS RIGHT HERE FOR YOU
Thanks for choosing DHL Express. We look forward to providing you best possible service and very fast delivery at the very best price. If you have any questions? Please contact our Customer support:
For Customer support, **please click right here**.

DHL© 2018. DHL . DHLBrandmark, and the orange tones are art logos of DHL Express, Inc. All rights reserved. Trademarks,names that appear in connection with DHL services are the property of their respective owners.

Don't respond directly to this letter.

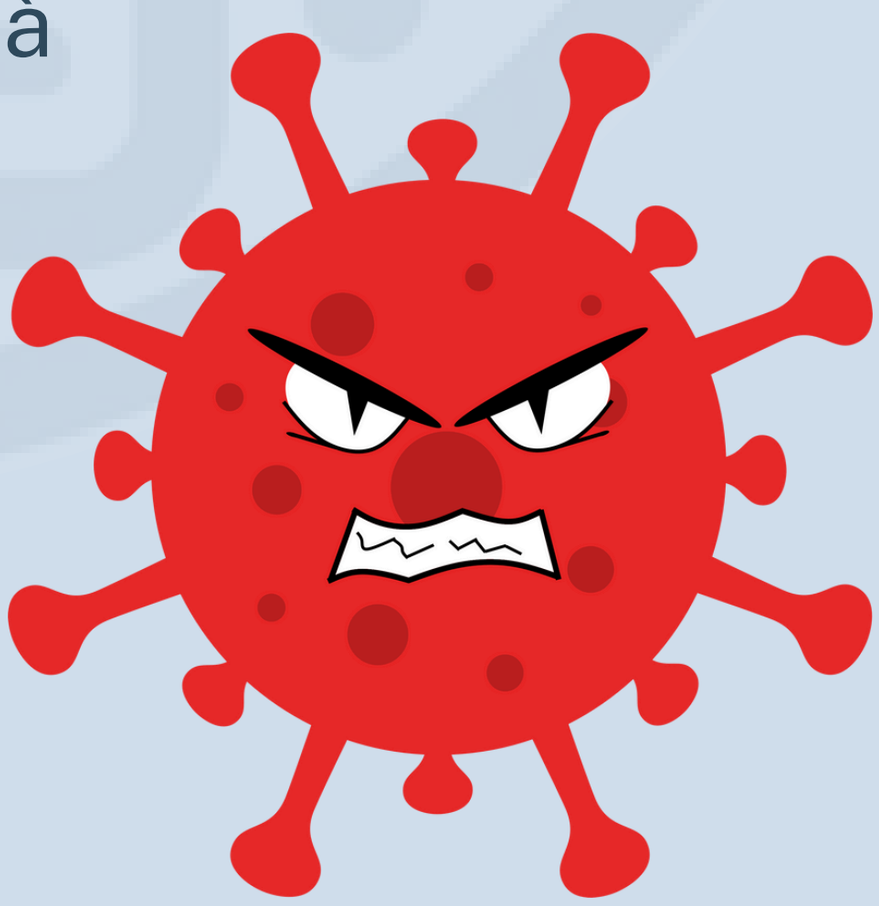
This notification keeps personal information. If you're not the expected receiver, the duplicating disclosure or other use of the material of this letter is strictly forbidden and you are recommended to erase this information promptly.

Financé par
l'Union européenne

Examinons de plus près les logiciels malveillants les plus courants

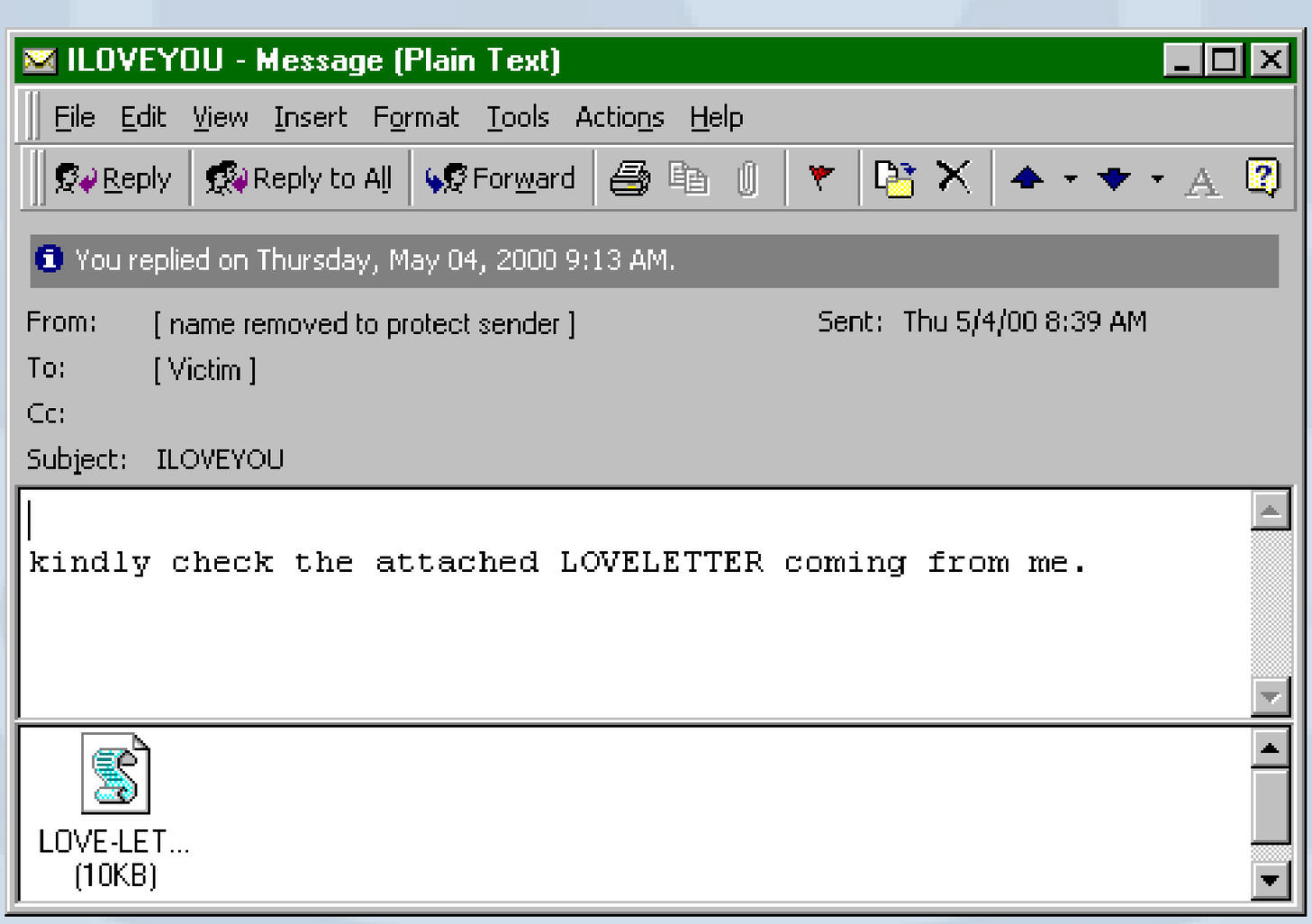
Le cheval de Troie - comme le cheval de Troie de la mythologie grecque, ce type de logiciel malveillant se distingue des autres en ce qu'il s'agit d'un programme conçu pour inciter les utilisateurs à l'installer. Le cheval de Troie peut être utilisé pour voler des informations personnelles. Pour ce faire, vous devez créer une porte dérobée dans votre système qui permet aux pirates de le contrôler. Habituellement, les ordinateurs sont infectés par des chevaux de Troie par le biais de pièces jointes à des e-mails.

VIRUS - comme le virus qui peut infecter une personne, le virus informatique est également très contagieux. Il s'agit d'un morceau de code qui infecte le logiciel hôte et propage ensuite la contagion à travers les fichiers du système. Si les fichiers sont partagés via un système, le virus peut également être transmis à d'autres appareils.



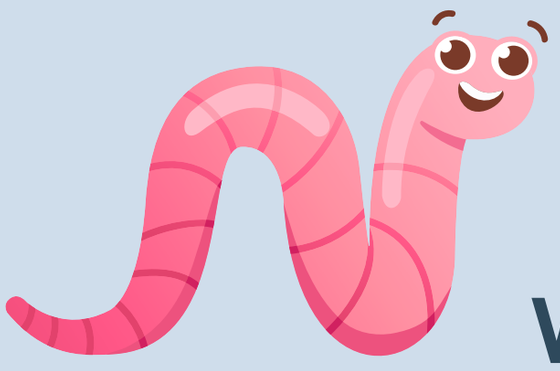
Financé par
l'Union européenne

Les virus peuvent se propager par le biais de pièces jointes à des e-mails, de clés USB, de stockage en nuage et autres. C'est une bonne idée de toujours vérifier les fichiers que vous recevez. Par exemple, si l'on vous envoie une vidéo, sachez que si le nom comprend « **.exe** », comme dans le nom « **.mov.exe** », cela aura presque certainement quelque chose à voir avec un virus.



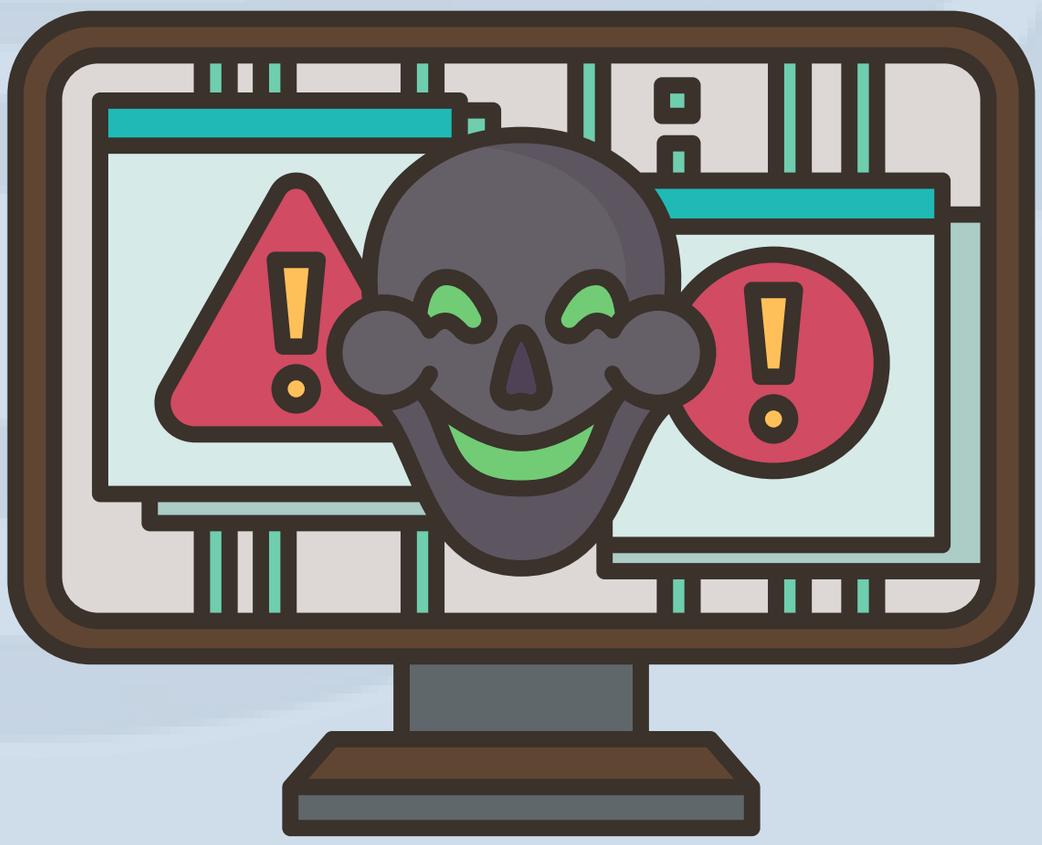
Par exemple, ***le virus ILOVEYOU*** a été l'un des premiers virus à se propager par e-mail. Dès que des utilisateurs suspects cliquent sur la pièce jointe, celle-ci se propage et infecte l'audio, l'image et tous les autres fichiers de l'ordinateur.

Financé par
l'Union européenne



WORM est le type de logiciel malveillant le plus courant. Il provoque des dommages similaires à ceux causés par les virus. La différence réside dans le fait que les vers informatiques ont la capacité de se répéter, de se multiplier et de se propager indépendamment, alors que les virus dépendent de l'activité humaine pour se propager (par exemple, exécuter un programme, ouvrir un fichier).

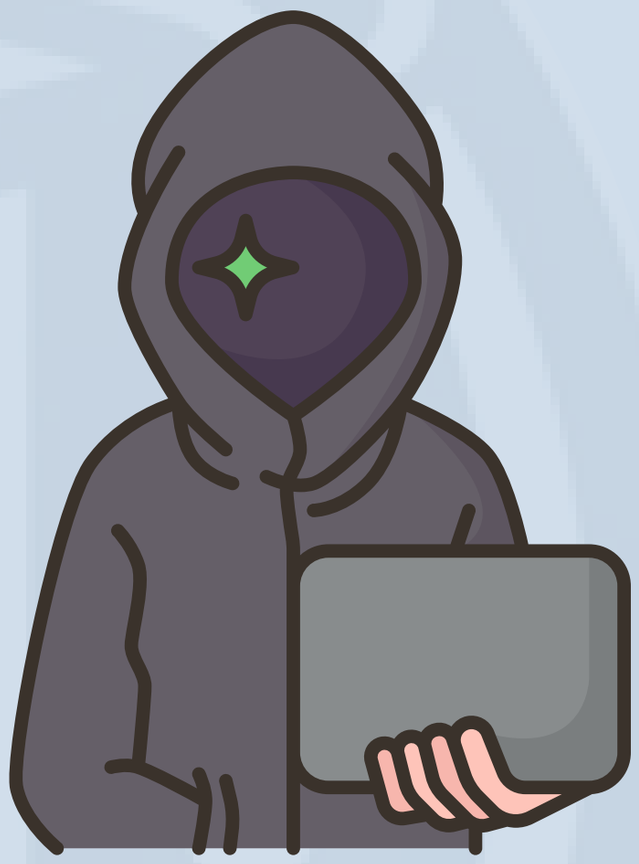
Les vers se propagent le plus souvent par l'envoi d'e-mails contenant des pièces jointes infectées aux contacts des utilisateurs dans le carnet d'adresses.



Financé par
l'Union européenne

Un logiciel espion est un type de logiciel malveillant qui fonctionne en espionnant l'activité de l'utilisateur à son insu. Les logiciels espions peuvent collecter des informations sur les utilisateurs (mots de passe, données financières, etc.) et surveiller l'activité des utilisateurs (activité sur Internet, frappes au clavier, etc.).

Un RANSOMWARE est un logiciel malveillant qui s'installe furtivement sur l'appareil de la victime et retient ses données en otage jusqu'à ce qu'une rançon soit payée.



L'attaque qui s'est produite avec le ransomware WannaCry en mai 2017 aurait infecté plus de
230 000 ordinateurs dans plus de 150 pays en une journée. Le logiciel malveillant a crypté les fichiers avec une rançon de 300 $ pour 600 $ à payer en bitcoins.

Financé par
l'Union européenne

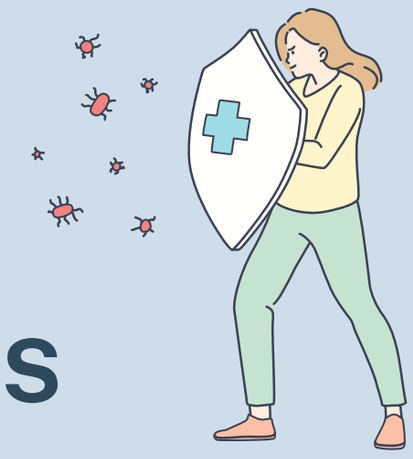
Le SCAREWARE est une forme de logiciel malveillant qui utilise l'ingénierie sociale pour provoquer un choc, de l'anxiété ou la perception d'une menace afin de manipuler les utilisateurs pour qu'ils achètent des logiciels indésirables. Il suggère généralement aux utilisateurs de télécharger et de payer pour un faux logiciel antivirus afin de le supprimer.

THE SYSTEM INFECTION PROCESS

Quels sont les moyens les plus courants d'infecter votre appareil avec des logiciels malveillants ? Cela peut se produire dans les cas suivants :

- vous ouvrez un email (infecté) à partir d'adresses inconnues,
- vous naviguez sur des sites dangereux,
- vous ne mettez pas à jour votre système d'exploitation,
- vous n'exécutez pas l'analyseur de logiciels espions,
- vous téléchargez des logiciels infectés,
- Vous téléchargez des logiciels, de la musique ou des films piratés et non autorisés.

Financé par
l'Union européenne



PRÉVENTION DES INFECTIONS

Bien qu'il n'existe pas d'utilisation sûre des ordinateurs et d'Internet de nos jours, il y a beaucoup de choses que nous pouvons faire pour minimiser les risques. Avez-vous installé un programme antivirus commercial sur votre ordinateur et votre téléphone portable ou votre tablette ? Le mettez-vous à jour régulièrement ? Avez-vous le même code d'accès (mot de passe) pour chacun de vos comptes réseau ? Utilisez-vous vos comptes en réseau sur tous les appareils ?

Voici ce que vous pouvez faire pour protéger votre ordinateur ou votre appareil mobile contre les virus et autres logiciels malveillants :

- Installez un programme antivirus autorisé et mettez-le à jour régulièrement (par exemple, AVG, Avast, Kaspersky, McAfee). Il existe également quelques options gratuites.
- Il installe régulièrement des mises à jour de sécurité pour son système d'exploitation. Certains systèmes peuvent être configurés pour se mettre à jour automatiquement à une certaine heure de la journée, de la semaine ou du mois.

Financé par
l'Union européenne

Les mises à jour prennent beaucoup de bande passante et beaucoup de temps à traiter, c'est donc une bonne idée de les configurer pour un moment où vous ne travaillez pas sur votre appareil. Pourquoi ne pas définir l 'attribut. Des mises à jour automatiques pendant le déjeuner du dimanche ou peut-être pendant la nuit ?

- Utilisez un pare-feu.
- Utilisez le bloqueur de fenêtres contextuelles de votre navigateur.
- Définissez des mots de passe forts pour vos comptes.
- Lorsque vous avez fini de travailler, déconnectez-vous toujours de votre compte réseau sur tous vos appareils.

Financé par
l'Union européenne

PROGRAMMES ANTIVIRUS

Pour lutter efficacement contre les virus, il est toujours bon d'installer un programme antivirus sur votre système. Même si vous en avez déjà un, assurez-vous qu'il n'a pas expiré et qu'il est configuré pour recevoir des mises à jour automatiques. Vous pouvez choisir parmi un certain nombre de programmes antivirus disponibles, dont beaucoup sont également gratuits.

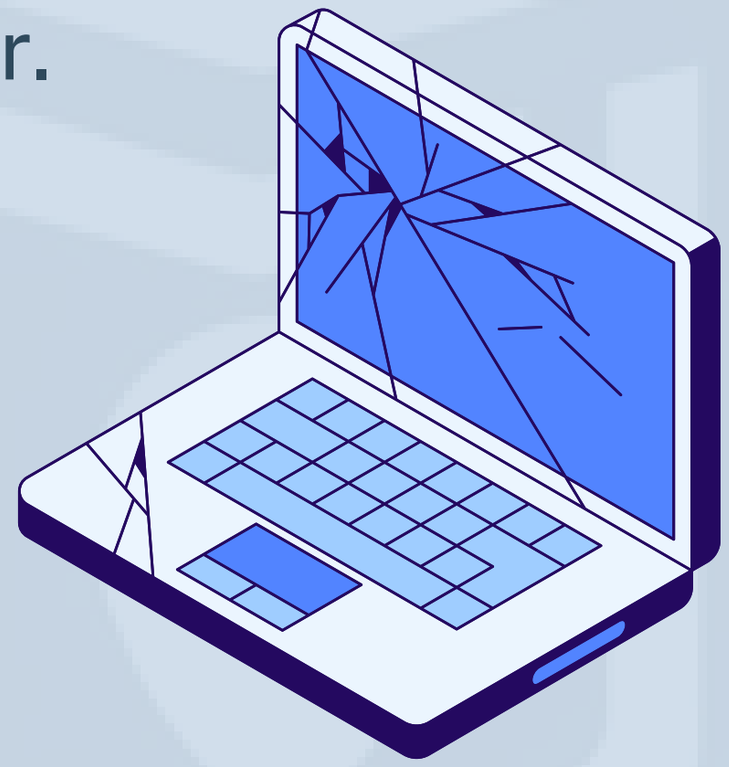
Le programme antivirus que vous choisissez doit avoir deux modes:

1. **Interactif :** Dans ce mode, le programme se cache en arrière-plan et surveille l'activité de l'ordinateur, toujours à la recherche d'un virus provenant d'un e-mail, www, USB, etc. Si un virus est détecté, un message clignote sur leécran.
2. **Analyse :** Dans ce mode, le programme antivirus analyse et vérifie toutes les parties de la mémoire et du système de stockage de votre ordinateur, à la recherche de signes d'infection. Juste au cas où, il est recommandé de configurer votre logiciel antivirus pour qu'il analyse automatiquement.

Financé par
l'Union européenne

PROTÉGEZ VOTRE APPAREIL CONTRE LES DOMMAGES PHYSIQUES

Bien que cela semble évident, il peut être utile de ne pas oublier de garder vos appareils hors de portée des enfants et des animaux domestiques. De plus, ne pas manger ou boire pendant l'utilisation de votre ordinateur peut éviter le risque de renverser de la nourriture ou des boissons sur le clavier ou d'autres composants. Cela est particulièrement vrai lors de l'utilisation d'un ordinateur portable, car les composants sont tous placés à l'intérieur.



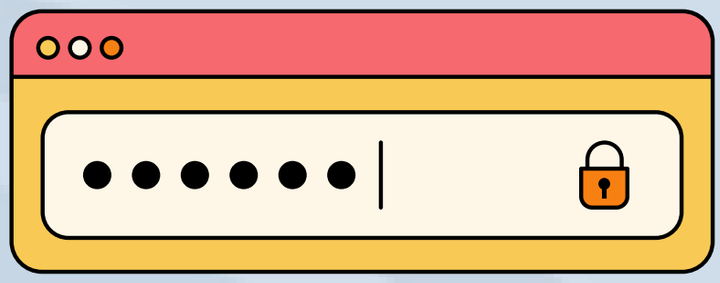
Il est très important de connecter votre ordinateur, votre écran et votre routeur à un ***parasurtenseur*** et d'éviter qu'il ne soit endommagé pendant les orages. Dans de tels cas, si vous n'avez pas de parasurtenseur, vous devez au moins déconnecter les appareils du système électrique.

Il serait également utile d'envisager de souscrire une ***assurance prolongée*** pour les appareils. Bien qu'elle ne couvre pas les accidents tels que la chute de votre ordinateur ou le déversement de liquides sur votre clavier, elle pourrait vous faire économiser des coûts de réparation élevés.

Financé par
l'Union européenne

Mot de passe

Le mot de passe ou le mot de passe est la première ligne de défense en matière de cybersécurité



À l'heure actuelle, tout le monde devrait savoir que les mots de passe comme « 123456 » et « password123 » ne sont pas assez forts, c'est-à-dire sécurisés. Cependant, il y a encore des millions de personnes qui n'utilisent pas de mots de passe sécurisés.

Selon la société de gestion de mots de passe Keeper Security, la liste des mots de passe les plus courants est tout simplement choquante. Voici la liste des mots de passe les plus utilisés en 2016.

1. Qwerty
2. 12345678
3. 111111
4. 1234567890
5. 1234567
6. password
7. 123123
8. 987654321
9. qwertyuiop
10. Mynoob
11. 123321
12. 666666
13. 18ATCSKD2W

Financé par
l'Union européenne

Vous êtes-vous rendu compte que vous avez utilisé des mots de passe comme celui-ci ??

Voyons maintenant comment créer un mot de passe sécurisé.

- Mélangez des lettres majuscules et minuscules, des chiffres et des symboles (par exemple, @, #, $,%) si vous y êtes autorisé.
- Utilisez au moins huit caractères (plus vous utilisez de caractères, plus votre mot de passe est fort).
- Utilisez les lettres initiales d'une phrase que vous aimez, surtout si un chiffre ou un caractère spécial est inclus.
- Prenez deux choses familières, puis combinez-les avec un nombre ou un caractère particulier.
- Il est recommandé de changer votre mot de passe tous les 3 mois.
- N'utilisez pas le même mot de passe pour tous les comptes que vous utilisez.
- Enfin, le meilleur mot de passe est un mot de passe facile à RETENIR.

Financé par
l'Union européenne

Gestionnaire de mots de passe

Vous avez au moins cinq comptes en ligne tels que Google, Facebook, Twitter, LinkedIn et Instagram, ainsi que des services bancaires à domicile, un portail gouvernemental, etc. Maintenant que vous savez comment créer un mot de passe sécurisé, il est temps de découvrir un logiciel de gestion de mots de passe. Comment pourrez-vous utiliser des mots de passe forts et uniques pour tous les sites Web auxquels vous avez accès ou auxquels vous souhaitez accéder ?

La réponse est un logiciel de gestion des mots de passe. Les gestionnaires de mots de passe comme KeePass stockent vos informations de connexion pour tous les sites Web que vous utilisez et vous aident à vous y connecter automatiquement en cryptant votre base de données de mots de passe à l'aide d'un mot de passe principal. Le mot de passe principal reste alors **le seul mot de passe** dont vous devez vous souvenir.

SÉCURITÉ DES DONNÉES PERSONNELLES

Définir la confidentialité des services en réseau

Avez-vous déjà consulté ou modifié les paramètres de **confidentialité** des services en ligne que vous utilisez, tels que eBay, Gmail, InstaeBay, Gmail, Instagram, Facebook, Google, YouTube, etc. ?

Financé par
l'Union européenne

Pour atteindre un certain niveau de sécurité sur Internet, vous devez être en mesure de comprendre le bon paramètre de confidentialité dans les services réseau que vous utilisez et comment le gérer au mieux.

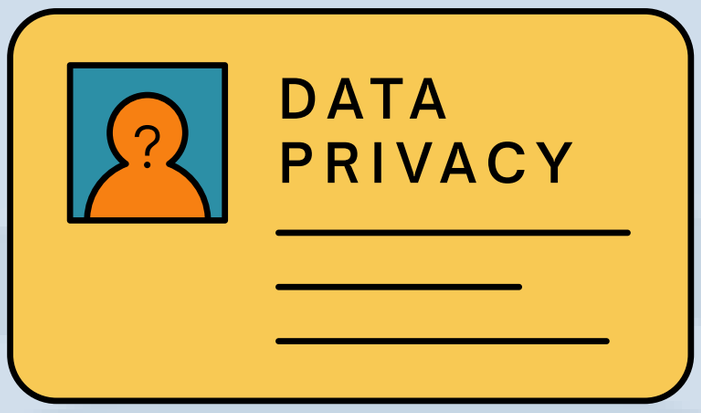
Rendre la navigation plus sûre

Voici quelques conseils pour rendre votre navigation plus sûre :

- Activez les mises à jour automatiques de votre moteur de recherche (navigateur).
- Bloquez les pop-ups, les plug-ins et les sites d'hameçonnage.
- Configurez votre navigateur de manière à ce qu'il ne stocke pas votre mot de passe.
- Désactivez les cookies tiers.
- En fonction du navigateur que vous utilisez, vous devrez ajuster ses paramètres pour une sécurité maximale.

Financé par
l'Union européenne

Définir la confidentialité des réseaux sociaux



Les réseaux sociaux permettent aux gens de se connecter, mais ils sont également une plate-forme populaire pour lancer des menaces en ligne et de la cyberintimidation. Sans le vouloir, les gens, en particulier les enfants, partagent souvent plus d'informations en ligne qu'ils ne le devraient. Cela les rend particulièrement vulnérables.

Des études récentes ont montré que 9 adolescents sur 10 publient des photos d'eux-mêmes en ligne ou utilisent leur vrai nom sur leur profil ; 8 sur 10 révèlent leur date de naissance et leurs centres d'intérêt ; et 7 sur 10 affichent le nom de l'école et de la ville où ils vivent. Ces actions peuvent faire des enfants des cibles faciles pour les « prédateurs » en ligne.

Financé par
l'Union européenne

Les **paramètres de confidentialité** sont des contrôles disponibles sur divers réseaux sociaux (par exemple, Facebook) et d'autres sites Web qui permettent aux utilisateurs de restreindre l'accès à leur profil et aux informations que les visiteurs peuvent voir.

Alors que les solutions de filtrage de contenu peuvent être utilisées pour empêcher les élèves d'accéder aux médias sociaux lorsqu'ils utilisent les ordinateurs de l'école, de nos jours, la plupart des élèves apportent des smartphones à l'école et une fois qu'ils se connectent à Internet sur ces appareils, ils sont hors de toute possibilité de contrôle par l'école. C'est pourquoi il est crucial de promouvoir une citoyenneté numérique responsable dans les programmes scolaires.

Le protocole https et les sites web sécurisés

Un site web sécurisé ne contient aucun programme malveillant, il crypte toutes les données qui y transitent afin d'assurer un échange sécurisé de données personnelles ou de transactions financières contre toute compromission.

Financé par
l'Union européenne

Comment savoir si un site web est sûr ?

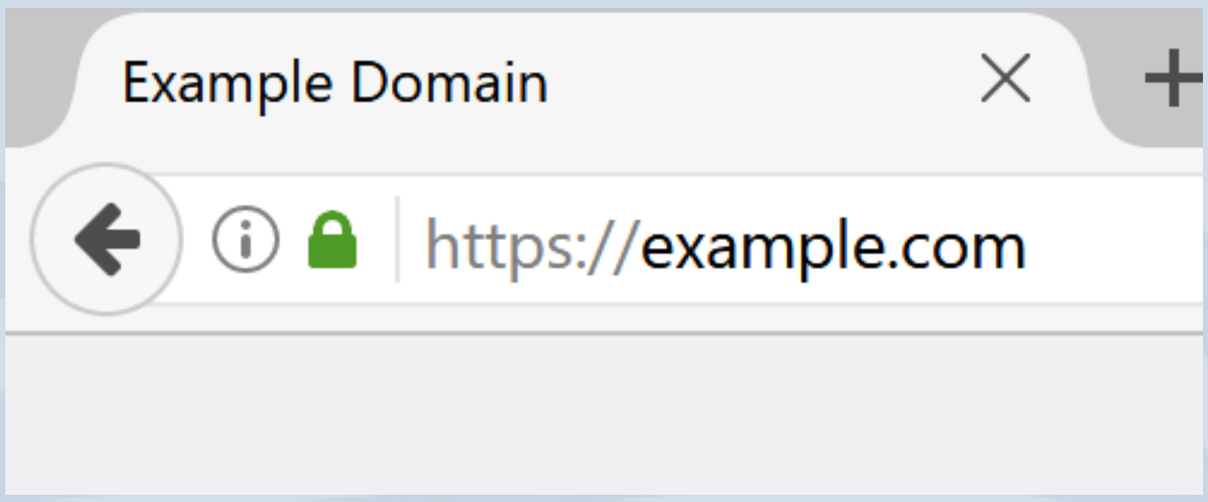
Si le site web utilise HTTPS (un protocole de communication pour **des communications sécurisées** sur un réseau informatique), le mot HTTPS apparaîtra avant l'adresse du site web.

Apprenez à connaître votre navigateur et ses fonctionnalités. En plus de https, une icône peut apparaître. Par exemple, si vous utilisez **Google Chrome** pour vérifier la sécurité d'un site, consultez l'état de sécurité sur le côté gauche de l'adresse Web.

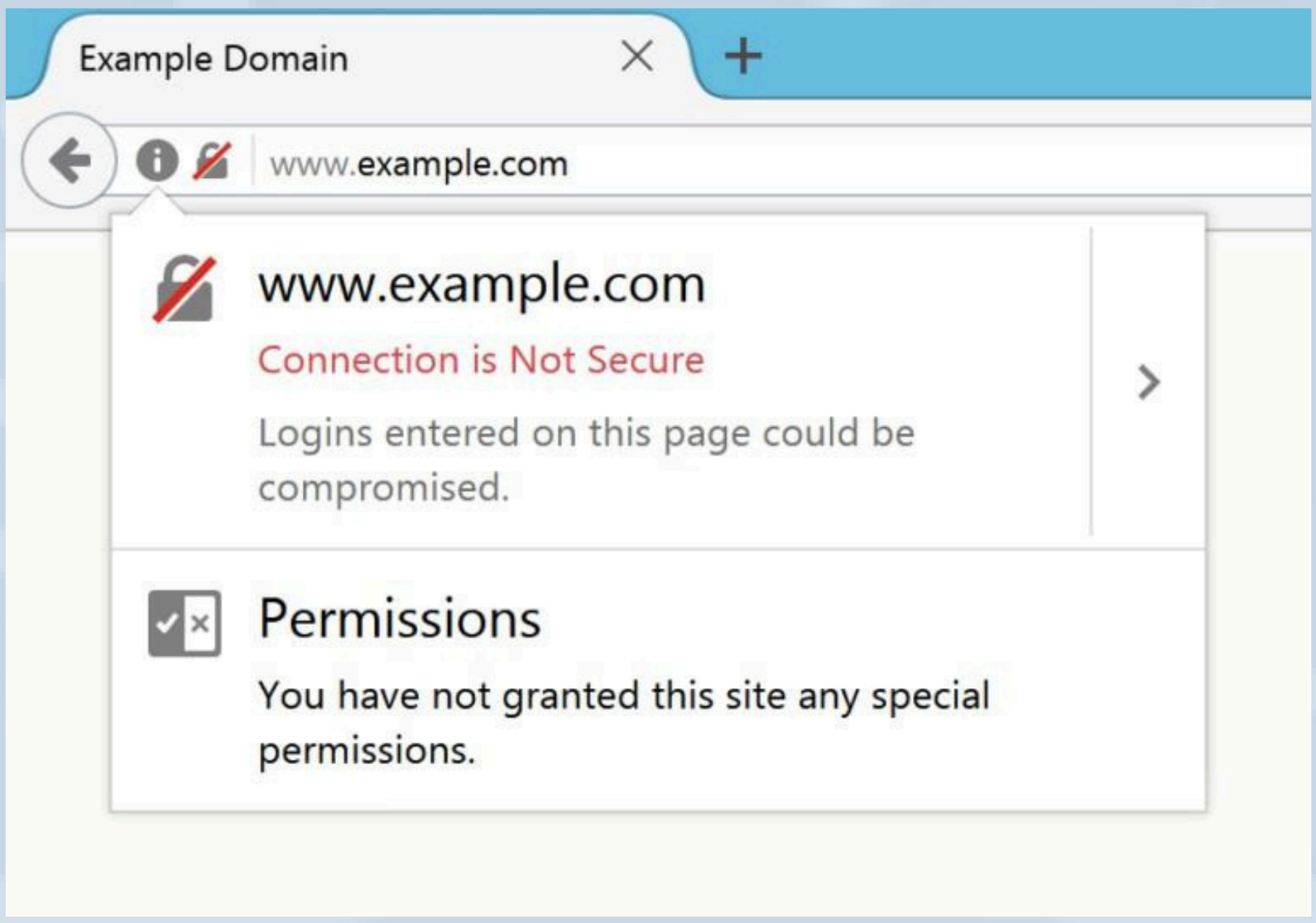
Financé par
l'Union européenne

Si vous utilisez Firefox, l'état de sécurité se trouve également sur le côté gauche de l'adresse Web :

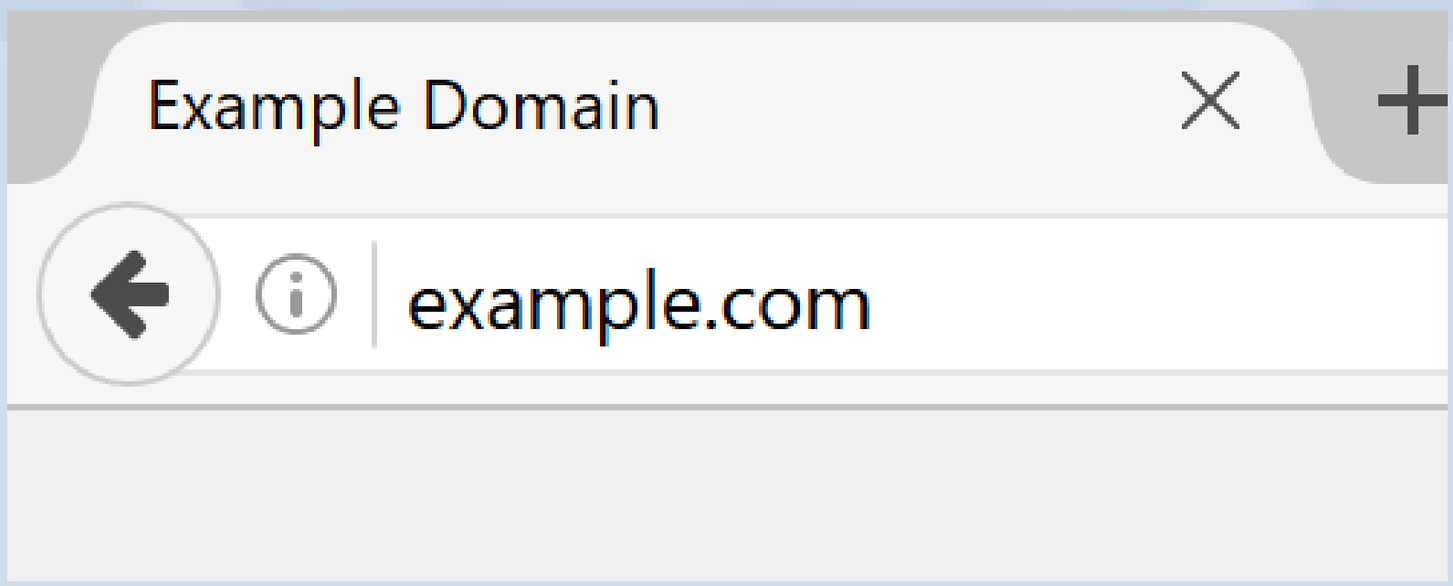
- Sûr



- Avertissement

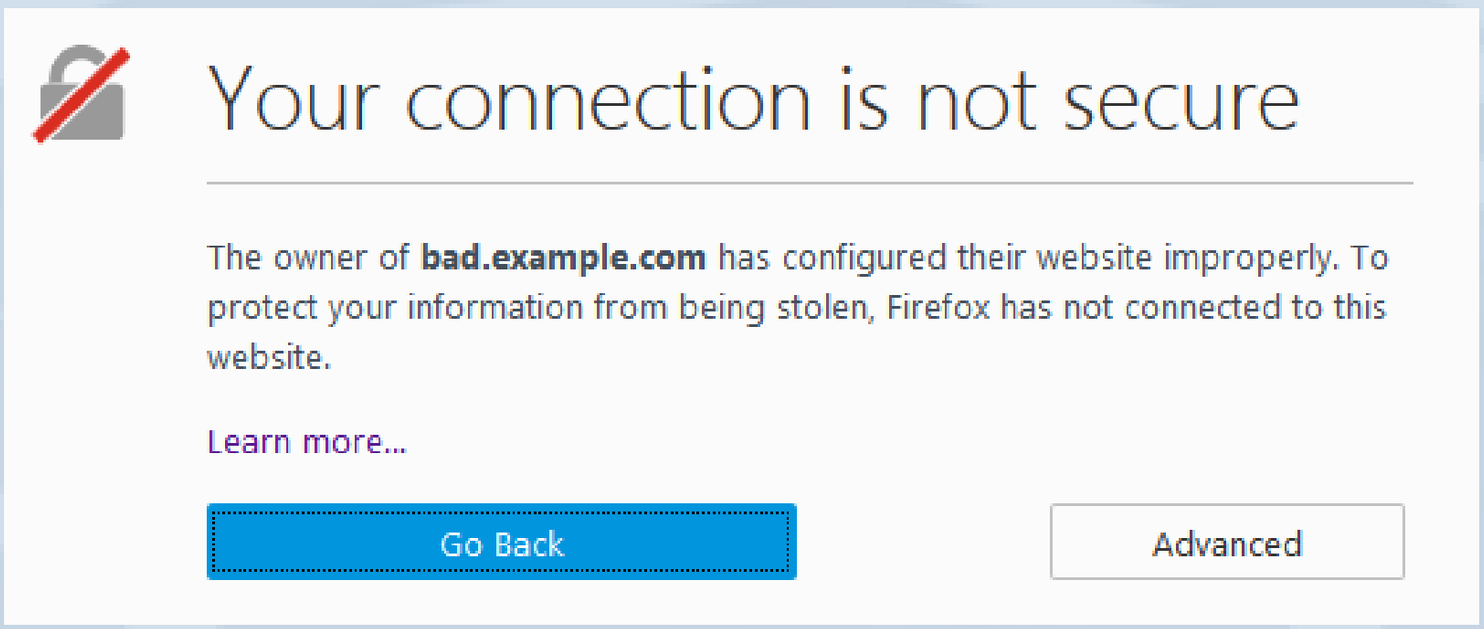


- Pas sûr ou dangereux

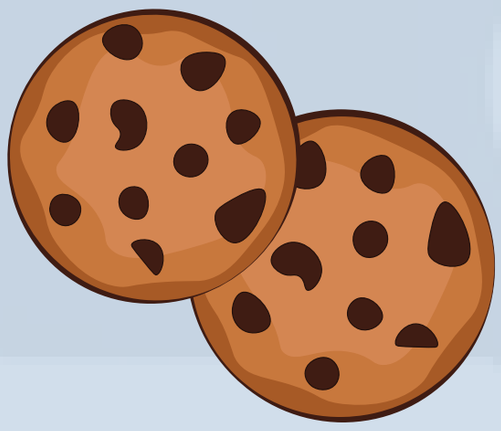


Financé par
l'Union européenne

Des précautions particulières doivent être prises lors du transfert d'informations sensibles et hautement personnelles sur le réseau. Certains sites Web peuvent ne pas être mis à jour selon les dernières normes SSL, ce qui peut être dangereux pour le transfert de données, mais suffisamment sécurisé pour naviguer et rechercher des informations.



Cookies



Les cookies Internet sont de petits fichiers qui sont stockés sur votre ordinateur. L'objectif principal d'un cookie est d'identifier les utilisateurs et éventuellement de préparer des pages Web personnalisées ou de stocker des informations de connexion au site. Les cookies ne contiennent généralement pas d'informations sensibles ou très personnelles ou quoi que ce soit de dangereux. Dans la plupart des cas, cela signifie que le site Web se souvient de votre nom d'utilisateur. Si vous supprimez vos cookies après avoir visité un site Web particulier, vous ne serez pas traité comme un visiteur récurrent. (Par exemple, vous devrez saisir à nouveau son nom d'utilisateur.)

Financé par
l'Union européenne

Surfer sur un ordinateur à usage public

Lorsque vous utilisez des ordinateurs publics, comme dans les bibliothèques, les cybercafés, les aéroports, les hôtels, etc., vous devez être très prudent. Pour préserver la confidentialité de vos informations professionnelles, personnelles ou financières, nous vous recommandons de suivre quelques règles simples :

- Ne demandez pas à un ordinateur public de se souvenir de votre mot de passe.
- Vérifiez si le pare-feu Windows est activé et si un programme antivirus a été installé.
- Ne téléchargez pas de documents confidentiels sur un ordinateur public
- Supprimez tout contenu téléchargé des e-mails.
- Déconnectez-vous après avoir utilisé un site Web qui vous oblige à vous connecter (par exemple, Gmail, Facebook, LinkedIn, etc.).

Financé par
l'Union européenne

- Lorsque vous entrez votre mot de passe et vos informations financières sur une page Web, assurez-vous toujours de faire ce qui suit :

- Vérifiez si l'URL contient « https » et un bloc dans la barre d'adresse.
- Utilisez le mode de navigation privée (par exemple, si vous utilisez Google Chrome, dans le coin supérieur droit de la fenêtre de votre navigateur, cliquez sur le menu Chrome, puis sélectionnez « Nouvelle fenêtre de navigation privée »).

La navigation privée vous permettra de naviguer sur Internet sans enregistrer d'informations sur les sites et les pages que vous avez visités, mais elle ne vous rendra pas anonyme sur Internet. Cela signifie que votre fournisseur d'accès à Internet (à la maison), votre employeur (au travail) ou les sites eux-mêmes peuvent toujours garder une trace des pages que vous avez visitées. La navigation privée ne vous protégera pas contre les logiciels malveillants qui peuvent être installés sur votre ordinateur.

Financé par
l'Union européenne

Surfer sur un réseau public

Nous avons tous vu des panneaux comme celui-ci dans un bar, un restaurant, des bâtiments publics, etc.

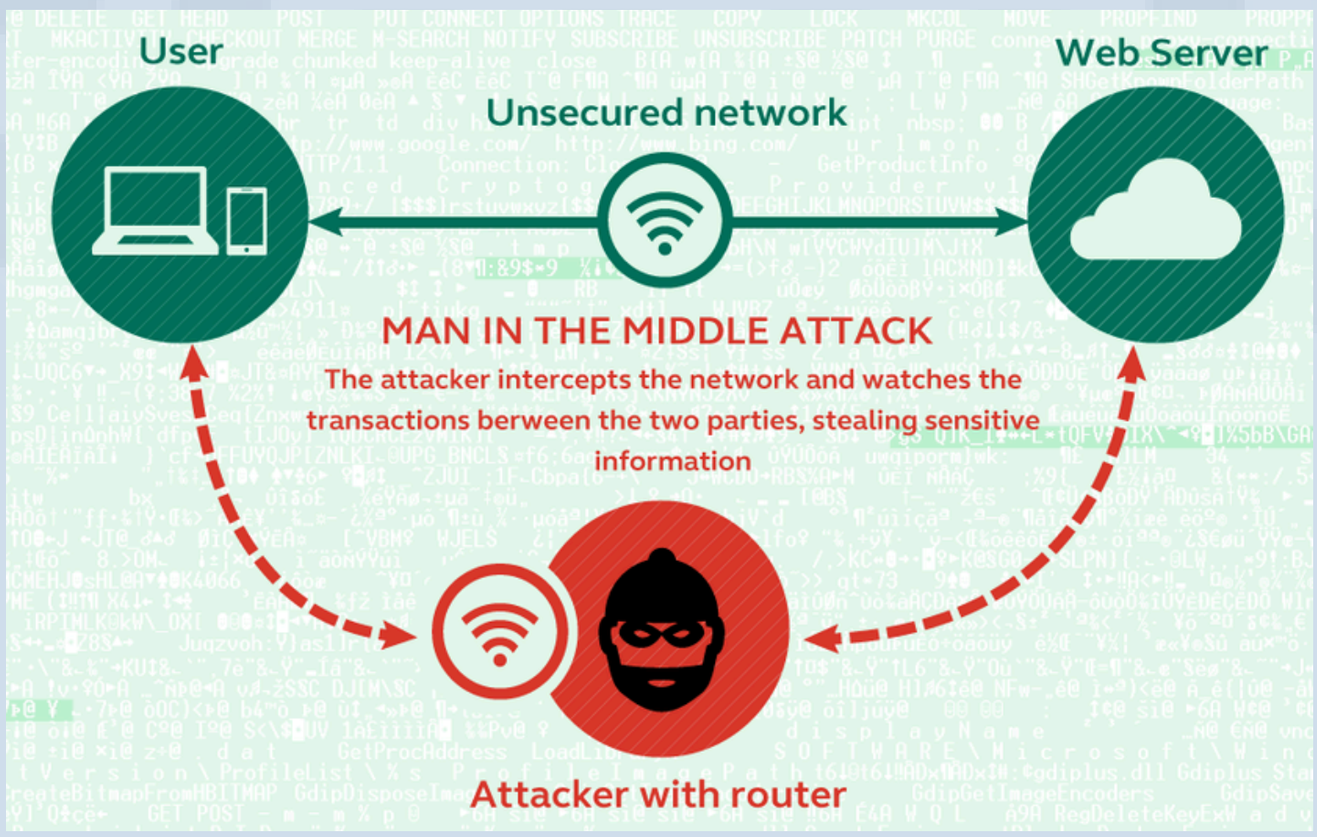
Vous êtes-vous déjà connecté à un réseau comme celui-ci en utilisant votre ordinateur portable, votre tablette ou votre smartphone ? Avez-vous pu vous connecter sans mot de passe ? Vous n'avez pas pu vérifier si l'adresse commençait par https:// ? Si vous avez répondu **OUI** à ces questions, vous avez potentiellement mis vos renseignements personnels en danger.

Financé par
l'Union européenne

Tous ces panneaux dans les lieux devraient en fait être remplacés par ceci :

Qu'est-ce qui rend une connexion sans fil plus vulnérable à l'exploitation ?

Lorsque vous vous connectez à un réseau public, c'est presque comme si vous invitiez un étranger chez vous : vous lui faites confiance en fonction des informations dont vous disposez. Toute personne accédant au même réseau (non sécurisé) peut intercepter tout passage d'informations entre votre appareil et les serveurs Web.



Financé par
l'Union européenne

Comment rester en sécurité ?

Bien qu'il n'y ait aucune garantie, vous pouvez suivre quelques étapes pour minimiser vos risques :

- **Ne vous connectez pas** à des réseaux qui ne nécessitent pas de mot de passe. Un réseau Wi-Fi officiel doit établir un mot de passe. Par exemple, si vous êtes dans un café, demandez au personnel de vérifier quel est son réseau. Il peut y avoir un faux filet spécialement mis en place sous le même nom que le bar.
- **Ne vous connectez pas** à des sites Web qui n'utilisent pas le protocole HTTPS.
- **Ne vous connectez pas** aux réseaux publics pour utiliser votre carte de crédit, consulter votre compte bancaire, payer des factures, etc.

- Lorsque vous avez fini de naviguer en utilisant leur Wi-Fi, **assurez-vous de vous déconnecter** et de supprimer le réseau afin qu'il ne vous connecte pas automatiquement la prochaine fois que vous reviendrez dans la salle.
- **N'activez le Wi-Fi que lorsque vous en avez vraiment besoin.** Cela empêchera votre appareil de se connecter automatiquement à des réseaux aléatoires.

Financé par
l'Union européenne

Utilisation sécurisée du stockage dans le cloud

Le stockage de vos fichiers (par exemple, images, vidéos, musique, documents, etc.) dans un stockage en nuage (par exemple, Google Drive, Dropbox, iCloud, Box, etc.) présente de nombreux avantages, par exemple, il y a moins de risque de perte de données. Les fichiers stockés dans le cloud peuvent être facilement consultés à partir de votre ordinateur et d'un appareil mobile connecté à Internet.

Bien que les entreprises de stockage prennent normalement les mesures de sécurité nécessaires, il n'y a aucune garantie. Cependant, les pirates sont très susceptibles d'acquérir vos données en raison d'une erreur humaine ou d'une négligence, simplement en déchiffrant votre mot de passe. Vous devez donc toujours vous assurer de :

- utiliser un mot de passe fort et sécurisé,
- Changez votre mot de passe régulièrement,
- Ne stockez pas d'informations personnelles dans le cloud
- Si possible, créez une copie de sauvegarde sur un autre périphérique (par exemple, un disque dur externe).

Financé par
l'Union européenne

Empreinte numérique : surveillance de l'identité sur le réseau

Une identité numérique (empreinte numérique) est la représentation en ligne d'un individu dans un monde virtuel tel qu'un salon de discussion, un forum, un jeu vidéo ou un espace communautaire virtuel. Toutes les activités en ligne (navigation, blogs, publications sur les réseaux sociaux et les forums, signature de pétitions en ligne, etc.) laissent une trace, ce que l'on appelle l'empreinte.

Lignes directrices pour la protection de votre identité en ligne

Avez-vous déjà cherché votre nom sur Google ? Avez-vous déjà trouvé quelque chose que vous ne voudriez pas que les autres voient ? Vous devez protéger votre « marque sur le net » et suivre les règles suivantes :

- *Utilisez des outils en réseau pour créer une empreinte positive.*
- *Ne publiez jamais quoi que ce soit que vous pourriez regretter à l'avenir.*
- *Soyez respectueux de vous-même et des autres.*
- *Choisissez des noms d'utilisateur et des avatars appropriés.*

Financé par
l'Union européenne

- Imaginez ce que votre famille et vos amis pourraient penser s'ils voyaient ce que vous faites en ligne.
- Bloquez les utilisateurs qui ont peu d'impact sur leur réputation.
- Tracez des informations sur vous-même.
- Assurez-vous que vos amis n'utilisent votre image qu'avec votre permission, et vice versa.
- Réfléchissez avant de cliquer.
- Surveillez votre identité numérique et vos empreintes digitales pour vous protéger contre la fraude en ligne et le vol d'identité. Pensez à la façon dont il aimerait être vu.

Gérer plusieurs identités sur le réseau

Nous venons d'évoquer qu'une identité numérique est la représentation en réseau d'un individu au sein d'un monde virtuel tel qu'un salon de discussion, un forum, un jeu vidéo ou un espace commun virtuel. Les gens construisent des identités numériques comme des représentations virtuelles d'eux-mêmes à des fins diverses (anonymes, professionnelles, éducatives, personnelles).

Financé par
l'Union européenne

Voici quelques avantages **de l'utilisation de plusieurs identités numériques :**

- Une identité numérique vous permet de créer des profils anonymes et de bloguer ou de discuter de manière anonyme.
- Vous pouvez rester privé tout en explorant diverses opportunités.
- Vous pouvez créer une identité numérique positive pour les opportunités professionnelles (par exemple, LinkedIn).
- Vous pouvez créer une identité numérique à des fins éducatives.

Combien d'identités numériques avez-vous ? Comment les gérez-vous ? Avez-vous déjà entendu parler d'un logiciel de gestion des mots de passe ? (par exemple, KeePass).

Protégez-vous contre la fraude en ligne et le vol d'identité

Vous avez déjà découvert diverses méthodes qui peuvent vous aider à protéger vos données personnelles sur Internet, telles que la reconnaissance d'un site Web sécurisé, l'utilisation d'Internet sur un ordinateur public, l'utilisation en toute sécurité du stockage en nuage et le suivi de l'identité et des empreintes digitales. Vous allez maintenant apprendre à vous protéger contre la fraude en ligne et le vol d'identité.

Financé par
l’Union européenne

Voici quelques règles simples que vous devez suivre, dont beaucoup vous ont déjà été apprises dans les rubriques précédentes :

- Protégez votre ordinateur et votre appareil mobile à l'aide d'un logiciel anti-malware puissant et à jour.
- Utilisez des mots de passe forts.
- Ayez des mots de passe différents pour chaque compte.
- Traquer des informations sur vous-même – examiner quelles informations privées peuvent être consultées par d'autres.
- Surveillez les communications bancaires et les communications par carte de crédit.
- Utilisez HTTPS dans la mesure du possible.
- Identifiez les e-mails et les pièces jointes suspects.
- Réfléchissez bien chaque fois que vous entrez vos renseignements personnels en ligne.

Financé par
l'Union européenne

Hameçonnage

L'hameçonnage est défini comme une tentative d'obtenir des informations sensibles telles que des noms d'utilisateur, des mots de passe et des détails de carte de crédit, souvent à des fins malveillantes, en se faisant passer pour une entité de confiance dans une communication électronique.

L'hameçonnage se fait généralement par le biais de l'usurpation d'identité ou de la messagerie instantanée de messages électroniques, et dirige souvent les utilisateurs vers la saisie d'informations personnelles sur un faux site Web, dont l'apparence et le format sont presque identiques à ceux des sites légitimes. Les communications censées provenir de sites de réseaux sociaux, de sites d'enchères, de banques, de processeurs de paiement en réseau ou d'administrateurs informatiques sont souvent utilisées pour attirer les victimes. Les e-mails d'hameçonnage peuvent contenir des liens vers des sites Web infectés par des logiciels malveillants.

Voici un exemple de tentative d'hameçonnage qui tente d'obtenir les informations de messagerie des utilisateurs.

Financé par
l'Union européenne

Comment identifier les escroqueries par hameçonnage

Voici quelques conseils sur la façon d'identifier les escroqueries par hameçonnage par e-mail :

- Ne faites pas confiance au nom affiché à l'écran.
- Regardez mais ne cliquez pas.
- Vérifiez qu'il n'y a pas de fautes d'orthographe.
- Analysez la forme de la salutation.
- Le message demande des informations personnelles.
- Méfiez-vous du langage urgent ou menaçant dans l'objet du message.
- Vérifiez la signature.
- Ne cliquez pas sur les pièces jointes.
- Ne pensez pas que l'adresse d'envoi est celle indiquée dans l'en-tête.
- L'offre semble trop belle pour être vraie.
- Le message semble provenir d'une agence gouvernementale.

Financé par
l'Union européenne

Cyberintimidation

Internet a ouvert de nouvelles possibilités pour nous tous. Le revers de la médaille, cependant, est représenté par les risques liés à une mauvaise utilisation de cet outil : parmi ceux-ci, il y a la **cyberintimidation**.

La cyberintimidation peut être définie comme l'utilisation de nouvelles technologies pour ***intimider, harceler, embarrasser, mettre les autres mal à l'aise ou les exclure.***

Pour les jeunes qui grandissent au contact des nouvelles technologies, la distinction entre la vie en ligne et la vie hors ligne est très minime. Les activités que les enfants réalisent en ligne ou par le biais de médias technologiques ont donc souvent des conséquences dans leur vie réelle. De la même manière, la vie en ligne influence également la façon dont les enfants se comportent hors ligne, et cet élément a plusieurs répercussions qui doivent être prises en compte afin de bien comprendre le cyberharcèlement.

Financé par
l'Union européenne

Tout cela peut se faire en utilisant différentes modalités offertes par les nouveaux médias. Certains d'entre eux sont :

- Appels téléphoniques
- Messages (avec ou sans images)
- Chats synchrones
- Réseaux sociaux (p. ex., Facebook)
- Sites de questions-réponses
- Sites de jeux en ligne
- Forums en ligne

Il existe de nombreuses façons spécifiques pour les enfants de se livrer à la cyberintimidation. En voici quelques exemples :

- les **ragots** se propagent par le biais de messages sur les téléphones portables, les e-mails, les réseaux sociaux ;
- publier ou transmettre des **informations, des images ou des vidéos embarrassantes** (y compris de fausses informations) ;
- **usurper l'identité et le profil d'autrui, ou en fabriquer de faux**, afin d'embarrasser ou de nuire à la réputation de la victime ;
- **insulter ou se moquer** de la victime par le biais de messages sur son téléphone portable, son courrier électronique, ses réseaux sociaux, ses blogs ou d'autres médias ;
- proférer des **menaces physiques** à l'endroit de la victime par l'entremise de quelque média que ce soit.

Ces agressions peuvent faire suite à des épisodes de harcèlement (à l'école ou plus généralement dans des lieux où les enfants se rassemblent) ou être des comportements uniquement en ligne.

Financé par
l'Union européenne

La cyberintimidation peut sembler inoffensive, mais si elle n'est pas traitée de manière appropriée, elle peut avoir de graves conséquences émotionnelles pour les enfants et les adolescents.

Voici quelques étapes à suivre pour éviter la cyberintimidation :

- Apprenez aux enfants à ne pas publier d'informations personnelles ou quoi que ce soit de très privé.
- Expliquez-leur de ne pas répondre par la colère et le ressentiment à un message qui, à son tour, exprime également de la colère.
- Expliquez aux enfants pourquoi ils ne doivent pas ouvrir les messages envoyés par des inconnus.
- Rappelez-leur de changer régulièrement et d'utiliser des codes d'accès (mots de passe) différents.
- Étant donné que ces paramètres ont tendance à changer, il est toujours judicieux de mettre à jour de temps à autre vos paramètres de confidentialité pour les services en réseau

HEALTH & GREEN IT

Know the potential health risks when working at the computer

Lorsqu'ils sont utilisés correctement et avec modération, les ordinateurs ne devraient pas avoir d'impact sur la santé de la plupart des gens. Cependant, l'utilisation intensive de l'ordinateur peut causer des problèmes de santé occasionnels et à long terme.

Financé par
l'Union européenne

Les problèmes et plaintes les plus courants sont les suivants :

- affections des membres supérieurs (pouvant toucher les doigts, les mains, les bras ou les épaules),
- douleurs dorsales et cervicales,
- problèmes oculaires,
- le stress causé par les maux de tête ou la fatigue.

Taper pendant des heures chaque jour est plus susceptible de causer des microtraumatismes répétés (TMS). Ces types de problèmes peuvent être causés par :

- une posture non naturelle ou malsaine lors de l'utilisation de l'ordinateur (en particulier les ordinateurs portables en raison des petits écrans, des claviers et des dispositifs de pointage intégrés (tels qu'une petite souris ou un pavé tactile portable),
- soutien lombaire inadéquat,
- rester assis dans la même position pendant une longue période de temps
- Poste de travail ergonomique médiocre.

Étant donné que les ordinateurs sont un outil essentiel dans notre vie quotidienne et qu'ils peuvent causer des problèmes de santé, vous devez apprendre à réduire les risques pour la santé liés à une utilisation prolongée de l'ordinateur.

Financé par
l'Union européenne

Utiliser l'ordinateur de manière saine

Diverses mesures doivent être appliquées pour réduire les risques pour la santé résultant d'une utilisation prolongée de l'ordinateur. Voici quelques exemples :

- L'image à l'écran doit être claire, fixe et exempte d'éblouissement et/ou de reflets.
- Le clavier doit être positionné correctement pour soutenir vos poignets.
- Pour prévenir les conséquences d'une utilisation prolongée de la souris, il est recommandé de faire des pauses pendant l'activité de la souris.
- La chaise de travail doit offrir une position de travail confortable et doit être entièrement réglable. Il doit être ajusté de manière à ce que les avant-bras des utilisateurs soient positionnés horizontalement et que le haut de l'écran soit au niveau des yeux. Un repose-pieds peut également être utilisé.
- Parallèlement à ces aménagements physiques, des changements réguliers de positions de travail ainsi que des périodes régulières de repos après avoir regardé l'écran sont essentiels pour éviter les problèmes de santé induits par l'ordinateur.

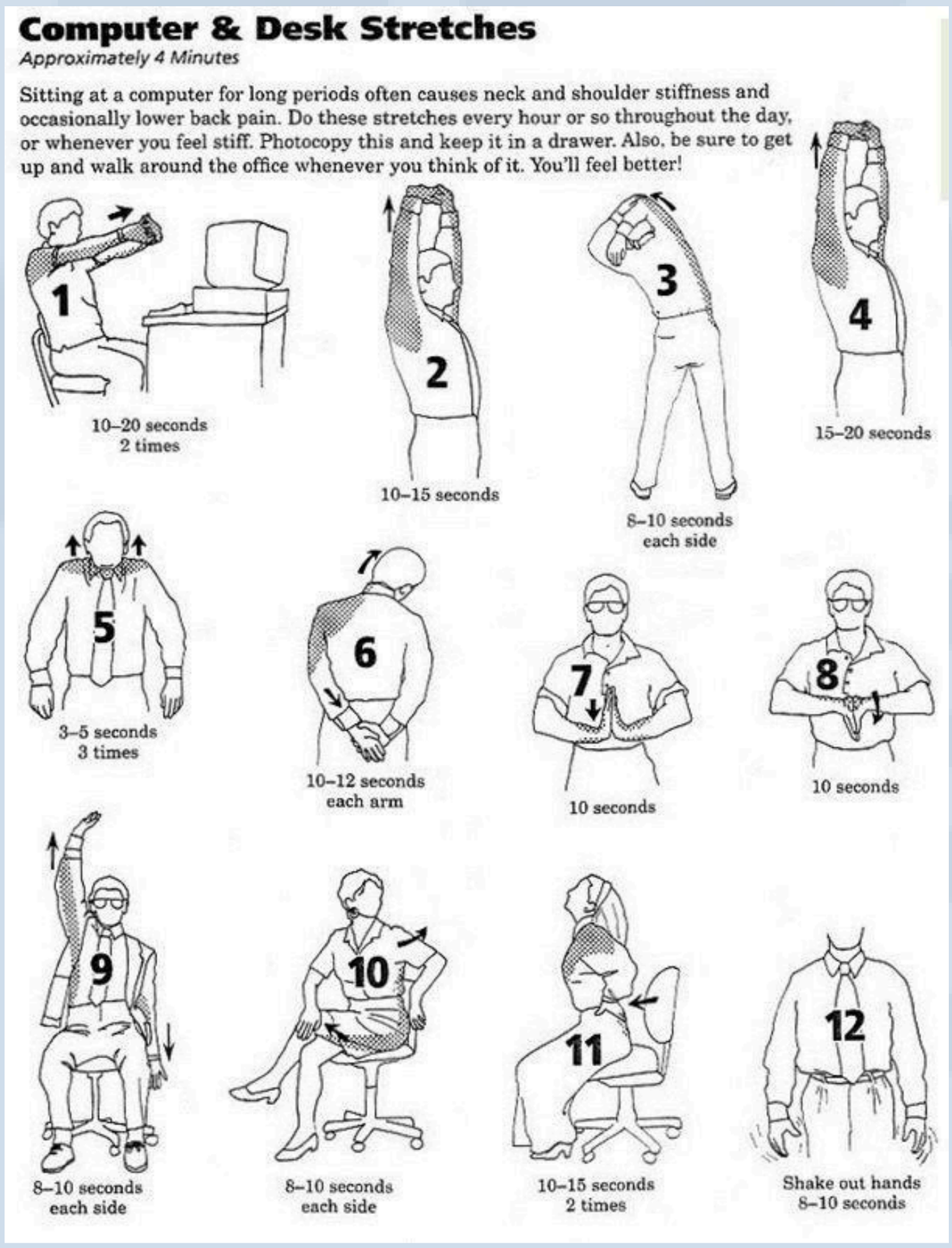
Les directives de l'Agence européenne pour la sécurité et la santé au travail (AEFA) Directive 90/270/CEE sur la manière d'utiliser les ordinateurs de manière saine peuvent être trouvées dans des indications claires sur la façon d'utiliser les ordinateurs de manière saine

Financé par
l'Union européenne

Comment détendre vos muscles tout en travaillant sur l'ordinateur

Vous avez déjà appris que l'utilisation de l'ordinateur peut causer des problèmes de santé et des moyens de réduire les problèmes de santé grâce à l'utilisation d'un équipement approprié, à la conception ergonomique du lieu de travail et au respect de pratiques de travail spécifiques (changements réguliers de position de travail et périodes régulières de repos sur écran).

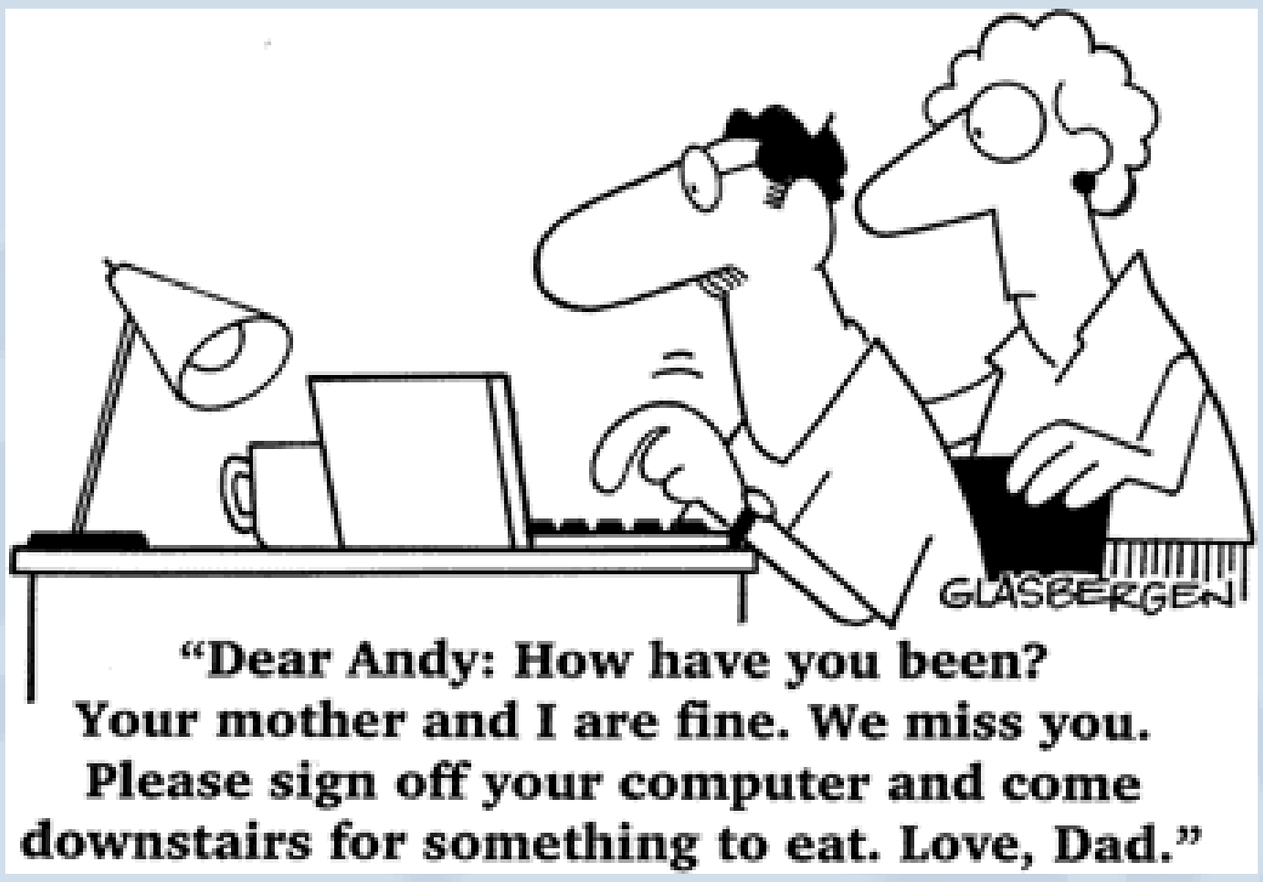
Afin d'améliorer votre posture et de garder votre santé sous contrôle, vous allez maintenant explorer comment détendre vos muscles lorsque vous travaillez toute la journée sur l'ordinateur.



Les National Institutes of Health (NIH) américains fournissent une liste complète de divers exercices et traits tels que les exercices oculaires et musculo-squelettiques, l'échauffement pour le travail, les exercices pour le dos, les exercices aérobiques et des recommandations pour le repos des muscles du dos.

Financé par
l'Union européenne

Trouver l'équilibre entre la vie en ligne et la vie hors ligne



Nous sommes entourés de technologie. Internet a changé la façon dont les gens interagissent. De nos jours, pour communiquer, nous préférons utiliser le courrier électronique, la messagerie instantanée (IM) et les sites de réseaux sociaux. Bien que les collaborations professionnelles n'aient jamais été aussi faciles, il semble que la plupart des gens aient remplacé leur vie sociale hors ligne par une vie en ligne. Les interactions en réseau peuvent difficilement remplacer les interactions en face à face, et plus nous passons de temps à socialiser en ligne, moins nous avons de temps pour socialiser hors ligne, c'est-à-dire hors réseau, dans le monde réel. Bien qu'il soit plus pratique de rester connecté en ligne, efforcez-vous de trouver un équilibre entre les mondes en ligne et hors ligne, et ne laissez pas les interactions en ligne remplacer le temps passé hors ligne avec vos amis ou votre famille.

Financé par
l'Union européenne

Appareils TIC - le nouveau pour l'ancien

La technologie utilisée dans les appareils TIC tels que les téléphones portables, les smartphones, les tablettes, les ordinateurs portables, les téléviseurs, les écrans d'ordinateur, les stations de jeu et les périphériques de stockage change très souvent.

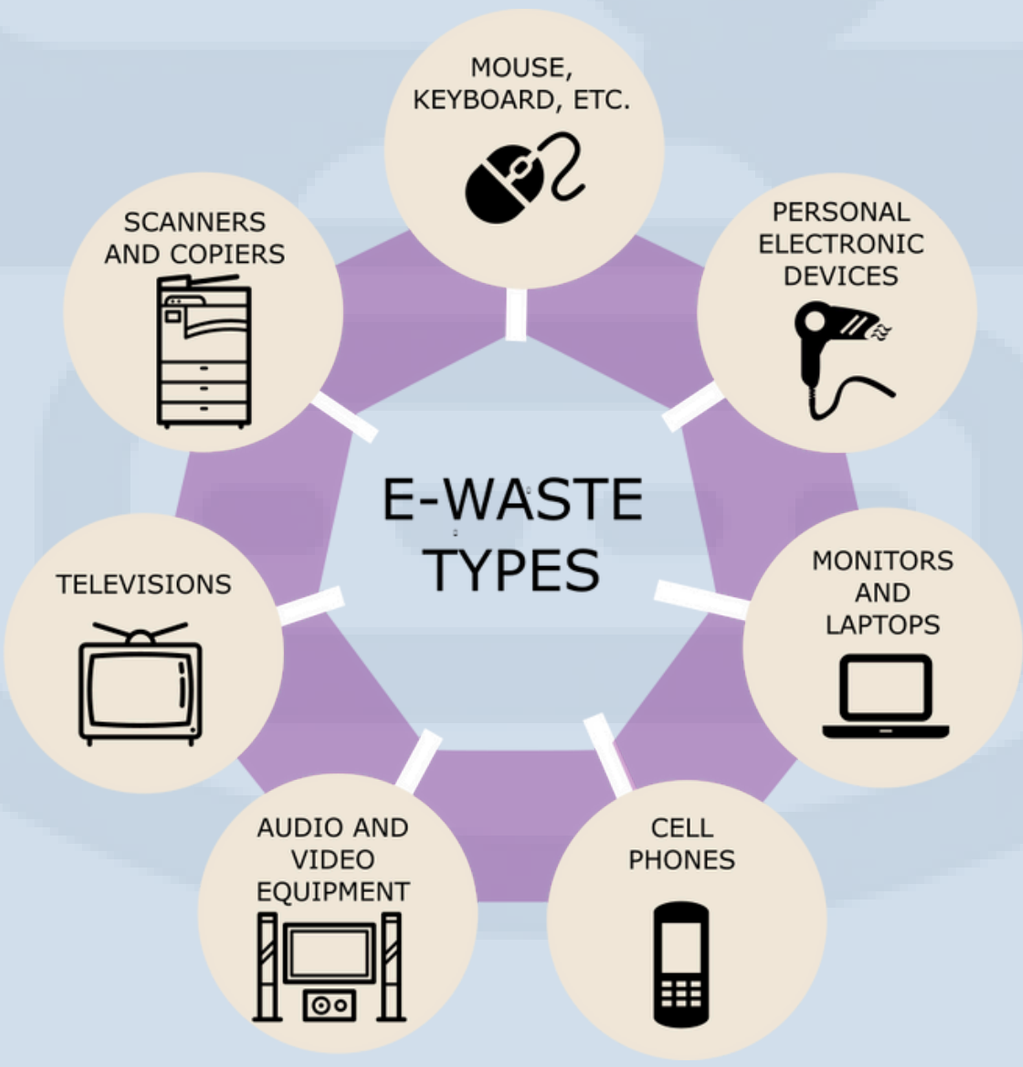
Les appareils électroniques qui étaient très utilisés par les utilisateurs il y a un an sont maintenant devenus vieux et obsolètes. Même si les « anciens » appareils fonctionnent toujours bien, les gens les jettent et les remplacent par de nouveaux.

Notre obsession de n'avoir que les appareils électroniques les plus récents et de jeter les versions obsolètes même si elles fonctionnent encore est un exemple de notre société « *jetable* ».

Financé par
l'Union européenne

Déchets électroniques

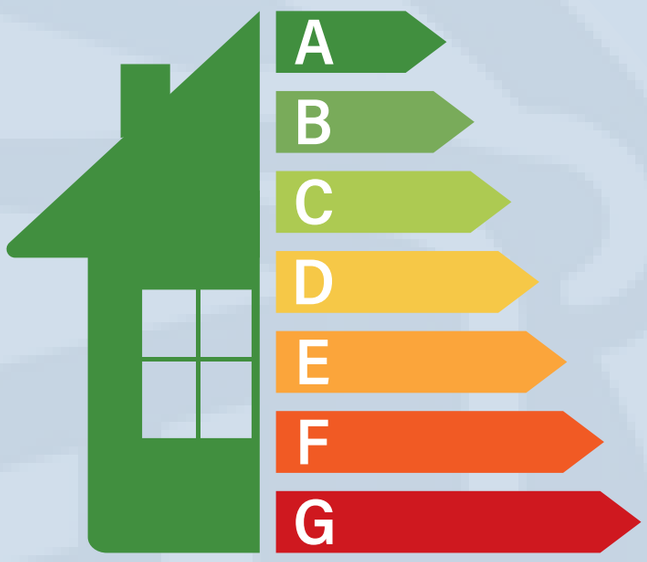
Les déchets électroniques deviennent un énorme problème dans le monde entier, car même aujourd'hui, de nombreux appareils électroniques finissent dans des décharges inadéquates. Lorsque les déchets électroniques ne sont pas éliminés correctement, les métaux toxiques, tels que le plomb (présent dans les écrans cathodiques, les batteries), le cadmium (piles rechargeables NiCd, couches fluorescentes d'écrans CRT, encres et toners d'imprimante), le mercure (lampes fluorescentes qui fournissent un rétroéclairage dans les écrans LCD, certaines piles alcalines et interrupteurs en contact avec le mercure), l'arsenic (à l'intérieur des diodes électroluminescentes) et le béryllium (boîtiers d'alimentation qui contiennent des redresseurs et des lentilles à rayons X contrôlées par silicium) sont absorbés par le sol et peuvent contaminer l'eau potable.



Financé par
l'Union européenne

C'est pourquoi la plupart des pays ont mis en place des réglementations très strictes pour éviter que les déchets électroniques ne soient déversés dans des décharges inappropriées. Bien qu'il existe des réglementations strictes, certains pays ont envoyé leurs déchets électroniques dans des endroits comme l'Asie, où ces lois ne sont pas aussi strictes.

Green IT et efficacité énergétique



Les déchets électroniques sont remplis de matériaux précieux tels que l'or, le nickel, l'acier, le plomb, le cuivre et le plastique. Chacun de ces matériaux peut être réutilisé. Par exemple, le zinc contenu dans les téléphones portables pourrait être utilisé dans la construction navale ou pour galvaniser les garde-corps métalliques et les lampadaires. L'or contenu dans les consoles de jeux vidéo peut être transformé en bijoux. Le plastique peut être réutilisé pour fabriquer des instruments de musique.

Il y a trois facteurs clés lorsque l'on pense au recyclage, à savoir **les 3 R :**

1. **réduire** la quantité de déchets produits,
2. **réutiliser** des objets du quotidien,
3. **recycler.**

Financé par
l'Union européenne

Nous avons besoin d'une grande quantité d'électricité pour alimenter des millions d'appareils TIC dans le monde. En raison de la façon dont l'électricité est produite, l'utilisation d'appareils électroniques contribue aux émissions mondiales de gaz à effet de serre (GES), mais les appareils TIC peuvent également être utilisés pour réduire la consommation d'énergie.

Par exemple, de nombreux bâtiments modernes disposent de systèmes numérisés pour le contrôle de l'environnement. En fait, il s'agit souvent d'un ordinateur qui contrôle le système de climatisation, d'ouvre-portes automatiques et de filtres solaires pour contrôler l'effet de la lumière du soleil et refroidir le bâtiment, de panneaux solaires pour réduire la consommation d'électricité, d'écrans de surveillance de l'énergie, de commandes d'éclairage LED économes en énergie et de systèmes de réutilisation de l'eau, en particulier dans les usines.