nc3.lu
National Cybersecurity
Competence Center
LUXEMBOURG

LA SÉCURITÉ DE L'INFORMATION

TRUCS & ASTUCES


ERROR
STOP

SÉCURITÉ DE L'INFORMATION :
TRUCS ET ASTUCES

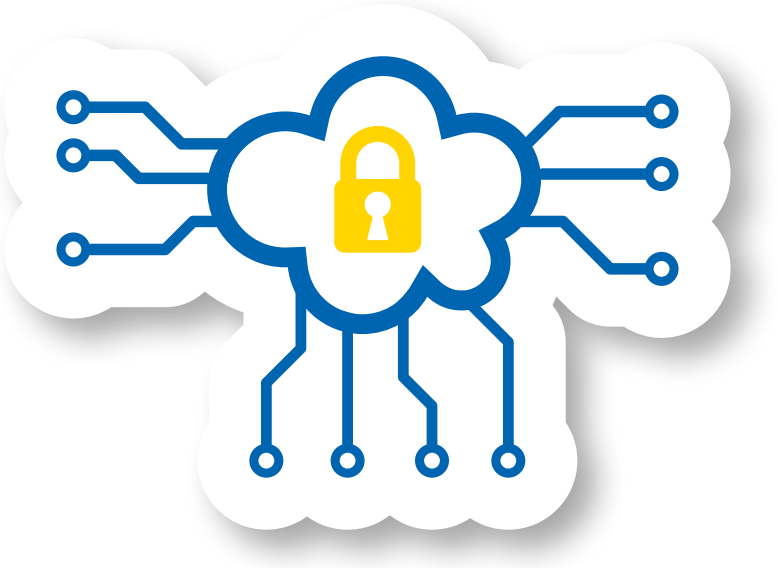
TABLE DES MATIÈRES

AVANT-PROPOS

Les technologies de l'information occupent une place essentielle dans notre société. Nous menons nos relations professionnelles et privées en grande partie à l'aide d'un ordinateur fixe ou portable, d'un Smartphone ou d'une tablette etc. Nous manipulons tous des informations sensibles, personnelles ou professionnelles dont la perte, le vol ou l'indisponibilité peuvent avoir des conséquences graves pour soi-même ou autrui.

Or, prenons-nous pour autant soin de sécuriser nos échanges lorsque nous communiquons par voie électronique et adoptons-nous des comportements sûrs lorsque nous manipulons des données ?

Cette brochure livre quelques conseils concrets pour une utilisation sécurisée des technologies de l'information.



COMMENT ESTIMER UN RISQUE

Le risque zéro n'existe pas. La sécurité n'est ni un bien ni un service que l'on peut acheter. Ceci vaut pour tous les aspects de la vie courante : nous ne pouvons pas être assurés de mener une existence sans accident. Mais nous pouvons prendre des précautions et respecter certaines mesures de sécurité. Nous pouvons également souscrire à des assurances spécialisées couvrant certains dégâts.

De la même manière, il est impossible d'éliminer tous les risques en matière de communication électronique. Il s'agit plutôt de les limiter au maximum, là où c'est possible, en partant d'une analyse précise de la situation.

Estimer un « risque » au niveau d'un système d'information revient à analyser 3 facteurs dans une situation donnée :

- le facteur « vulnérabilité » : il s'agit *d'une faiblesse ou d'un défaut* (facteur humain, technique ou organisationnel).
- le facteur « menace » : il s'agit d'un facteur externe ou interne. *Quelqu'un ou quelque chose qui pourrait exploiter la vulnérabilité*.
- le facteur « impact » : il s'agit des *conséquences* produites par la réalisation de la menace. Elles peuvent être tangibles et quantifiables sur le plan matériel, ou intangibles (retombées psychologiques, atteinte à la renommée d'une personne ou d'une structure professionnelle…).

EXEMPLE DANS LA VIE QUOTIDIENNE :

Vous laissez la clef sous le paillasson de votre maison afin de permettre à une connaissance d'accéder à votre domicile en votre absence :

Ceci constitue une « vulnérabilité » pour les objets de valeur de votre maison / pour votre propre sécurité. Elle pourrait être mise à profit par un inconnu qui s'approprie la clef (« menace »), cambriole votre maison (« impact tangible ») et provoque chez vous un sentiment d'insécurité (« impact intangible »).

ANALOGIE AVEC LES SYSTEMES D'INFORMATION :

Vous inscrivez votre mot de passe sur un papier que vous laissez à proximité de votre ordinateur dans l'intention de le transmettre à un collègue de travail pour qu'il puisse accéder à vos dossiers en votre absence. Ceci constitue une « vulnérabilité » dans le système. En effet, une personne malintentionnée pourrait trouver ce papier, se connecter à votre ordinateur et s'approprier des documents confidentiels ou envoyer des messages en votre nom, mettant ainsi en péril votre travail ou votre personne.

Les vulnérabilités humaines ne sont pas une fatalité. Avec un peu d'entraînement, d'organisation et de vigilance, nous pouvons développer nos défenses et notre résilience.

LES VULNÉRABILITÉS

VULNÉRABILITÉS HUMAINES

L'être humain n'est pas infaillible. Il peut être victime de fatigue ou de stress, ou encore être manipulé par des personnes malveillantes qui utiliseront ses penchants naturels (peur, pitié, curiosité, avidité…) afin de lui soutirer des informations critiques ou de lui faire ouvrir des portes vers ces informations.

VULNÉRABILITÉS TECHNIQUES

Un logiciel contient des instructions et données nécessaires pour que l'ordinateur puisse effectuer des traitements. Les logiciels étant des constructions humaines, ils peuvent contenir des erreurs de conception qui, sans entraver leur bon fonctionnement, peuvent représenter des *vulnérabilités* qu'une personne malveillante pourra exploiter.

Pour limiter le risque lié à ces vulnérabilités techniques :

- vos logiciels doivent être à jour ;
- votre antivirus doit être fonctionnel.

Gardez à l'esprit qu'aucune mesure n'est infaillible ; les anti-virus ne protègent pas de tous les logiciels malveillants, les filtres « anti spam » ne filtrent pas tous les courriers indésirables. En cas d'anomalies ou d'alertes logicielles, n'hésitez pas à contacter votre service technique.

LES MENACES

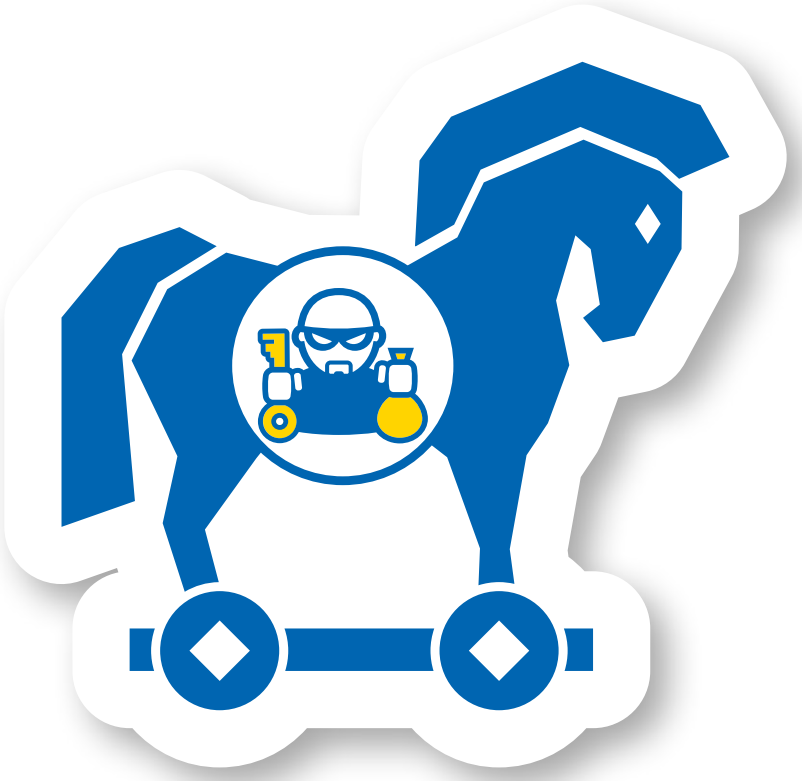
LOGICIELS MALVEILLANTS

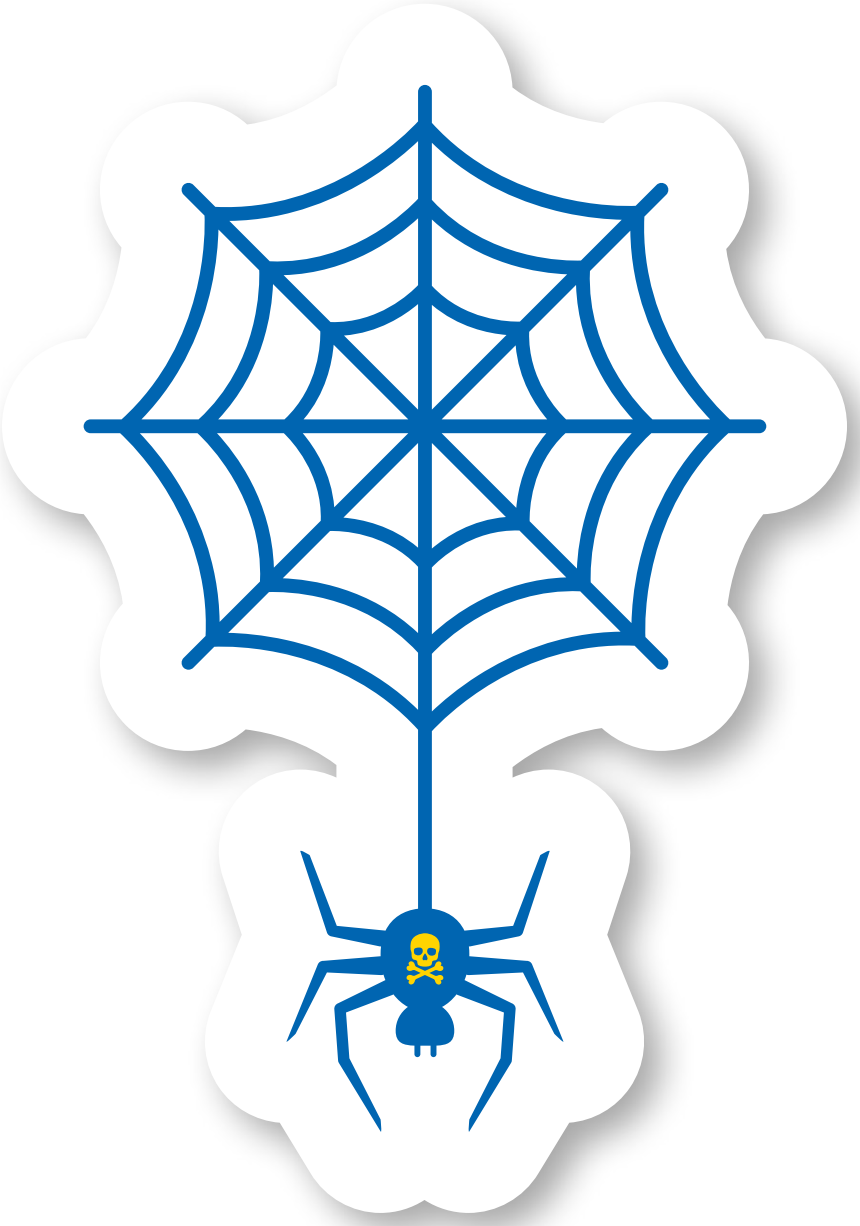
Un ordinateur ne peut pas faire la différence entre un logiciel malveillant et un logiciel légitime. En effet, la différence entre les deux réside dans « l'intention » du programmeur. De ce fait, il est impossible de concevoir une plateforme informatique protégée contre des logiciels malveillants. Actuellement, les logiciels malveillants servent principalement au vol de données.

On parle couramment, entre autres, de virus, de chevaux de Troie et de vers, de rançongiciel… Mais pour résumer, la plupart des logiciels malveillants servent à extorquer de l'argent.

RÉFLEXES SÉCURITÉ

- Demander l'accord du service informatique avant d'installer un logiciel.
- Eviter les extensions de fonctionnalités superflues, telles que les plugins ou les barres d'outils.
- Mettre à jour les logiciels installés sur la machine.
- Supprimer les logiciels inutiles.
- Surveiller les messages de l'antivirus et signaler toute anomalie aux responsables informatiques.





INTERNET

UTILISATION D'INTERNET

Internet est souvent source de logiciels malveillants. Trop nombreux sont les sites licites mal protégés qui sont compromis et ensuite utilisés pour infecter les ordinateurs des visiteurs. L'infection de ces derniers se passe alors le plus souvent via l'exploitation de vulnérabilités techniques des navigateurs.

LA FRAUDE SUR INTERNET

A l'origine, les attaques de systèmes d'information avaient une vocation ludique. Mais de nos jours, elles sont davantage motivées par un but lucratif.

Certaines données peuvent permettre d'accéder au porte-monnaie de la victime : accès au web-banking, accès à de l'argent virtuel, e-commerce (numéros de cartes de crédit).

D'autres données, par exemple les mots de passe, permettent de propager des logiciels malveillants ou des arnaques. Celui qui vole un mot de passe « Facebook », vole une identité en ligne et par là même la confiance du groupe d'amis.

LE MESSAGE ÉLECTRONIQUE INDÉSIRABLE

Il faut savoir que les messages indésirables ne sont pas limités aux courriels (« e-mails »). Un message indésirable peut parvenir entre autres des réseaux sociaux ou messageries instantanées.

SPAM

Les spams sont des mails non sollicités, souvent publicitaires voire trompeurs.

La messagerie électronique est un des moyens de communication les plus pratiques et rapides qui existent de nos jours. C'est aussi une forme de communication bon marché, mais souvent peu sécurisée (non chiffrée). Il est très simple de modifier le contenu d'un message électronique, respectivement de falsifier le nom de l'expéditeur. C'est pourquoi ces derniers sont souvent utilisés pour répandre des codes malicieux ou pour réaliser des attaques de type « ingénierie sociale » (voir : L'ingénierie sociale).

Des outils cryptographiques peuvent aider à sécuriser le contenu des messages électroniques.

PHISHING

Le phishing est une technique utilisée pour obtenir des renseignements personnels dans le but de perpétrer une usurpation d'identité. La technique consiste à faire croire à la victime qu'elle s'adresse à un tiers de confiance — banque, administration, etc. — afin de lui soutirer des renseignements personnels : mot de passe, numéro de carte de crédit, date de naissance, etc. C'est une forme d'attaque informatique reposant sur l'ingénierie sociale. Elle peut se faire par courrier électronique ou par d'autres moyens de communication électroniques.
Les cibles les plus courantes sont Apple, Paypal, Google, les services bancaires en ligne, et l'administration des contributions directes.

COMMENT RECONNAÎTRE LE PHISHING

Un phish (message électronique utilisé dans une attaque phishing) peut généralement être reconnu par les indices suivants :

- le message électronique suggère de réagir rapidement ;
- le message électronique s'adresse à vous de manière impersonnelle – souvent une formulation générique est utilisée comme « cher client » ;
- le message électronique contient un lien qu'il faut suivre. Pour se protéger, il ne faut surtout pas suivre ce lien !

Si vous recevez un message correspondant à un de ces critères, il vaut mieux l'ignorer. Si vous avez des doutes sur la véracité du message, vous pouvez également ouvrir vous-même votre navigateur et taper manuellement l'adresse du site concerné.

SPEARPHISHING

Les techniques de phishing se perfectionnent constamment, ce qui rend les messages électroniques malveillants difficilement reconnaissables. On parle également de « spearphishing » (phishing ciblé) créé sur mesure pour la victime. Ce genre d'attaque ciblée utilise des informations récoltées sur la victime pour construire un message crédible et très difficile à différencier d'un e-mail légitime. Le plus souvent, ce type d'attaque vise à infecter l'ordinateur des victimes.

REFLEXES SECURITE

- Supprimer sans les ouvrir les messages provenant d'un expéditeur inconnu ou dont le sujet paraît étrange.
- Ouvrir les fichiers joints seulement s'ils proviennent de personnes fiables. Si le message est étrange, contacter la personne par un autre canal.
- Refuser de partager des informations liées à des données sensibles, même au sein de son lieu de travail.
- Se méfier des courriels qui demandent une action précipitée.
- Ne pas cliquer sur le lien dans les messages électroniques. Naviguer manuellement sur le site en question, en introduisant soi-même l'adresse dans le navigateur.

Le saviez-vous…

Toute une économie parallèle s'est mise en place dans le monde virtuel. On considère aujourd'hui que la cybercriminalité est une des activités les plus lucratives dans le domaine du crime organisé.

Le fait de n'avoir rien à cacher en tant qu'utilisateur n'est pas une raison de se conduire de manière imprudente. A l'instar des trafiquants qui introduisent des stupéfiants dans les bagages des voyageurs, des personnes malintentionnées pourraient utiliser votre ordinateur pour envoyer du spam ou héberger de la pédopornographie.

LA SÉCURITÉ PHYSIQUE

La sécurité physique va de pair avec la sécurité de l'information. L'accès aux bureaux peut représenter une grande menace.

Verrouillez vos objets et documents de valeur dans des armoires. Sauvegardez vos données sensibles sur votre ordinateur uniquement si votre disque dur est chiffré.

Si vous rencontrez un visiteur sur votre lieu de travail, demandez-lui le but de sa visite et accompagnez-le à l'endroit souhaité.

INTERCEPTION À L'IMPRIMANTE

Un risque de vol/perte d'information existe également pour les documents qui trainent sur l'imprimante et sont à la portée de tous. Prenez soin de récupérer vos copies directement après l'impression. Il importe de s'habituer à détruire tout papier comportant des informations sensibles dans un broyeur (« shredder »). Dans la mesure du possible, verrouillez les poubelles et bennes à ordures.

DUMPSTER DIVING

Ce terme signifie littéralement « plonger dans la benne à ordures ». C'est-à-dire fouiller les déchets ! Il s'agit d'un moyen très utilisé par les fraudeurs. Qui d'entre nous ne jette pas parfois du courrier, des photos ou des documents à la poubelle, sans prendre le soin de les broyer au préalable. Les bennes à ordures quant à elles manquent souvent de cadenas et restent sans surveillance jusqu'au passage du camion de ramassage. Ces déchets peuvent livrer des tas d'informations sur une personne ou une société : nom, adresse, compte bancaire, informations professionnelles ou privées, etc.

Il importe de s'habituer à détruire tout papier comportant des informations sensibles dans un broyeur (« shredder ») – de préférence un broyeur coupe confetti. Dans la mesure du possible, verrouillez les poubelles et bennes à ordures.

RÉFLEXES SÉCURITÉ

- Ranger les documents papier dans une armoire verrouillée.
- Verrouiller, mettre en veille ou éteindre l'outil informatique lorsque l'on quitte le poste de travail, ou quand on laisse son matériel sans surveillance.
- Enregistrer les documents électroniques sur un serveur de fichiers se trouvant dans une salle verrouillée.
- Accompagner un visiteur à l'endroit de sa visite et ne pas le laisser sans surveillance.
- Récupérer ses documents dès l'impression.
- Broyer les documents sensibles avant de les jeter.

L'INGÉNIERIE SOCIALE

On parle d'ingénierie sociale lorsqu'un individu se sert d'une fausse identité ou de techniques de manipulation, pour inciter une personne à livrer des informations qu'elle n'aurait habituellement pas données, ou à accomplir une action qu'elle n'aurait pas effectuée.

RÉFLEXES SÉCURITÉ

- Vérifier l'identité du demandeur et le bien-fondé de la requête, avant de partager des informations personnelles ou professionnelles en direct, par téléphone, e-mail ou via Internet. En cas de doute, répondre ultérieurement et procéder entretemps à une vérification.
- Ne pas céder aux demandes « urgentes » ou menaçantes (par exemple d'un prétendu prestataire informatique qui doit « absolument » accéder à votre serveur) ;
- Ne pas écouter un inconnu qui prétend vouloir vous aider.

LES METADONNÉES

Saviez-vous que tout document contient des données relatives à sa création?

Ces « métadonnées » sont également disponibles pour des fichiers photos : date de création de la photo, informations sur la prise de vue et sur l'appareil utilisé, mais aussi les coordonnées exactes de la prise de vue si l'appareil contient un module GPS (courant sur les Smartphones).

Avant d'envoyer des documents de type office, nous conseillons à l'utilisateur de vérifier si des métadonnées révélatrices se trouvent encore dans le fichier. De même, les personnes publiant des images sur Internet doivent vérifier si elles ne contiennent pas des informations sensibles et si elles ont l'accord explicite de toutes les personnes représentées.

RÉFLEXES SÉCURITÉ

- Supprimer toutes les données cachées sensibles d'un document ou d'une photo avant une publication sur Internet.

→ Consultez **www.nc3.lu** pour des informations relatives à la suppression des données cachées.

L'AUTHENTIFICATION

SE FAIRE RECONNAÎTRE PAR L'ORDINATEUR

La connexion à un outil informatique se fait via un moyen d'authentification. Le plus souvent il s'agit de *quelque chose que vous connaissez*, comme le « nom d'utilisateur » et le « mot de passe ».

Il y a aussi moyen d'utiliser *une chose que vous possédez*, une « Smartcard » par exemple, contenant un code spécifique que la machine saura reconnaître.

Vous pouvez aussi vous identifier par *ce que vous êtes* : il s'agit le plus souvent de vous faire reconnaître par votre empreinte digitale.

L'utilisation de deux méthodes conjointes augmente naturellement la sécurité au niveau de l'identification. Malheureusement la méthode la plus utilisée reste actuellement le mot de passe.

Il est donc primordial d'être vigilant quant au choix de celui-ci.

LE BON MOT DE PASSE

Votre « nom d'utilisateur » et votre « mot de passe » sont des données d'accès personnelles. Elles doivent rester secrètes et individuelles.

Un bon mot de passe doit être facile à retenir mais difficile à deviner. La complexité du mot de passe peut être accrue en augmentant sa longueur ; il est recommandé d'utiliser au moins 12 caractères, de préférence une quinzaine. Si le système utilisé vous impose une taille maximale vous pouvez augmenter la complexité en variant les jeux de caractères. Utilisez par exemple des lettres minuscules, des majuscules, des symboles et des chiffres. Evitez de choisir des mots qui apparaissent dans un dictionnaire ou qui font référence à des informations personnelles (noms de vos proches; dates personnelles; etc.).

Utilisez des mots de passe différents pour chaque outil informatique, compte ou service.

Pour définir votre mot de passe, choisissez de préférence un moyen mnémotechnique. Se servir d'une « phrase » de passe au lieu d'un « mot » de passe peut représenter un avantage, quand le logiciel vous permet de choisir librement la longueur du secret. Exemple : « les 3 anacondas d'Amazonie » pour votre code d'accès à amazon.com. Si vous êtes limité par le logiciel, composez votre mot de passe à partir des premières lettres d'une phrase.

Exemple : **1ac4se12m!** (**1 a**nnée **c**omporte **4 s**aisons **e**t **12 m**ois **!**)

Si vous disposez de plus d'une dizaine de comptes qui nécessitent des mots de passe, il est avantageux d'utiliser une application de stockage de mots de passe sûre. Ces gestionnaires contiennent alors tous vos mots de passe qui seront protégés par 1 seul mot de passe maître. Ce dernier devra être d'une grande solidité.

RÉFLEXES SÉCURITÉ

- Choisir un mot de passe complexe, facile à retenir. Le garder secret et le changer régulièrement.
- Utiliser des mots de passe différents pour chaque application ou appareil.
- Utiliser une application de stockage de mots de passe sûre.

LE CHIFFREMENT

Le chiffrement (algorithmes mathématiques pour rendre le contenu illisible) de la communication est le seul moyen de vous assurer que vos messages atteignent leur destination sans être interceptés au passage. Le message passe via Internet et donc via des serveurs etc. qui ne sont pas forcément tous dignes de confiance.

Des techniques simples de chiffrement existent pour les pages web. Elles se signalent dans l'URL du site visité qui commence par les lettres « https » au lieu de « http ».

D'autres méthodes de chiffrement existent pour d'autres moyens de communication, mais peuvent être plus difficiles à utiliser. Le chiffrement du message électronique est par exemple une technique difficile à mettre en place.

Un moyen facile pour transmettre des documents sensibles de manière sûre par courrier électronique consiste à les archiver (format de fichiers : zip, rar,...) et à protéger l'archive par un mot de passe. Ensuite il suffit d'envoyer l'archive en pièce jointe à son destinataire et de lui communiquer le mot de passe par téléphone ou sms (ou bien par tout autre canal sécurisé – mais il ne faut surtout pas l'envoyer par le même canal de communication).

Le chiffrement peut aussi vous aider à protéger les données sensibles sur les PC, tablettes ou smartphones, ou encore sur les backups.

SAUVEGARDE ET ACCÈS AUX INFORMATIONS

Il est vital de faire des sauvegardes régulières sur un support qui n'est pas connecté tout le temps à la machine. Cela vous permettra d'être mieux protégé contre le disfonctionnement du disque dur ou les « Ransomwares ». Dans la plupart des cas, lors d'une infection de ce type, la sauvegarde est le seul moyen de récupérer vos données, comme vos photos de vacances ou vos documents personnels.

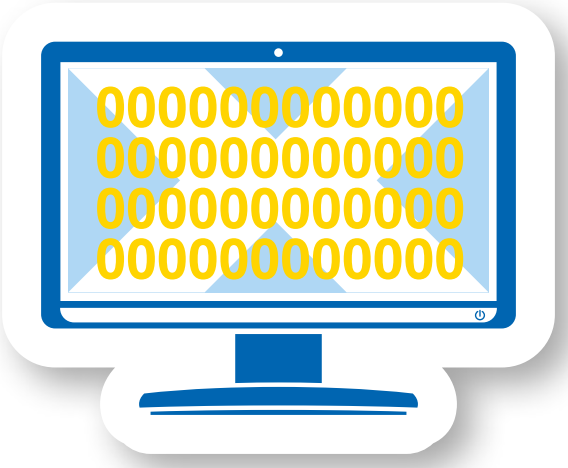
LA MISE AU REBUT

En utilisant un ordinateur, de nombreuses données sensibles s'accumulent. Si l'ordinateur, voire le disque dur, est mis au rebut, vendu, donné en cadeau ou envoyé en réparation, ces données sensibles sont rarement effacées correctement.

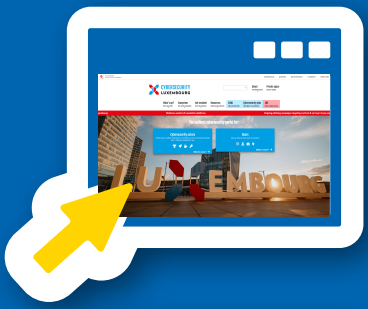
Si l'on supprime des fichiers sur l'ordinateur, ils sont d'abord envoyés dans la corbeille (« recycle bin ») d'où ils restent accessibles et peuvent être récupérés facilement.

De même, lorsque l'on vide la corbeille, les données ne sont pas véritablement supprimées du disque dur. Ce qui est effacé, c'est leur référence dans l'index des fichiers, libérant l'espace préalablement occupé pour d'autres fichiers. Tant que de nouveaux fichiers ne viennent pas écraser l'espace ainsi libéré, les données restent intactes sur le disque dur et peuvent être reconstituées avec l'aide d'outils informatiques spécifiques.

Pour effacer de façon efficace les données de son disque dur, il est nécessaire d'écrire sur toute la surface du disque. Certains logiciels spécialisés permettent de le faire, mais l'opération peut être longue. Il est plus rapide de détruire le disque physiquement.



SITES UTILES



CYBERSECURITY.LU est le portail luxembourgeois de la cybersécurité. Il rassemble les outils, les actualités, les événements et les acteurs de la cybersécurité au Grand-Duché de Luxembourg.
→ **www.cybersecurity.lu**

Le site **NC3** propose des méthodes et des services aux entreprises et aux administrations qui désirent renforcer la sécurité de leurs informations au niveau organisationnel. Il lance également des alertes sur les menaces qui surgissent régulièrement et offre une Helpline pour répondre aux questions et aux problèmes liés à la cybersécurité.
→ **www.nc3.lu**
email : **info@nc3.lu**

Le site **CERT / CSIRT** rassemble les équipes d'intervention d'urgence (Emergency and Response Teams) privées et publiques.
→ **www.cert.lu**

Le site **BEE SECURE** promeut la cybersécurité et l'utilisation responsable des nouveaux médias auprès du grand public. Il s'adresse notamment aux jeunes et au secteur éducatif luxembourgeois.
→ **www.bee-secure.lu**

www.nc3.lu

info@nc3.lu

nc3.lu
National Cybersecurity
Competence Center
LUXEMBOURG

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère de l'Économie

Luxembourg House
of Cybersecurity