

SÉCURITÉ DE L'INFORMATION : TRUCS ET ASTUCES

TABLE DES MATIÈRES

Avant-propos	4
Comment estimer un risque	5
Analogie avec les systèmes d'information	6
LES VULNÉRABILITÉS	7
Vulnérabilités humaines	7
Vulnérabilités techniques	7
LES MENACES	8
Logiciels malveillants	8
INTERNET	11
Utilisation d'Internet	11
La fraude sur Internet	11
LE MESSAGE ÉLECTRONIQUE INDÉSIRABLE	12
Spam	12
Phishing	12
Spearphishing	14
Le saviez-vous ...	14
LA SÉCURITÉ PHYSIQUE	15
Interception à l'imprimante	15
Dumpster diving	15
L'INGÉNIERIE SOCIALE	16
LES MÉTADONNÉES	18
L'AUTHENTIFICATION	18
Se faire reconnaître par l'ordinateur	18
Le bon mot de passe	19
Le chiffrement	21
Sauvegarde et accès aux informations	21
LA MISE AU REBUT	22
SITES UTILES	23

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 paillason de votre maison afin de permettre à une connaissance d'accéder à votre domicile en votre absence :

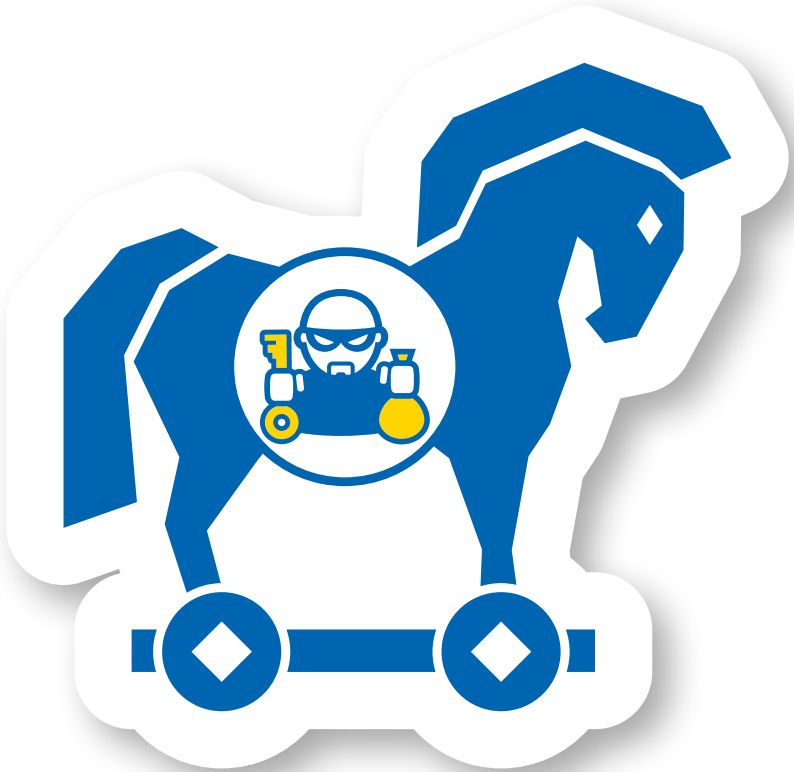
Ceci constitue une « vulnérabilité » pour les objets de valeur de votre maison / pour votre propre sécurité. Elle pourrait être mise à profit par un inconnu qui s'approprie la clef (« menace »), cambriole votre maison (« impact tangible ») et provoque chez vous un sentiment d'insécurité (« impact intangible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

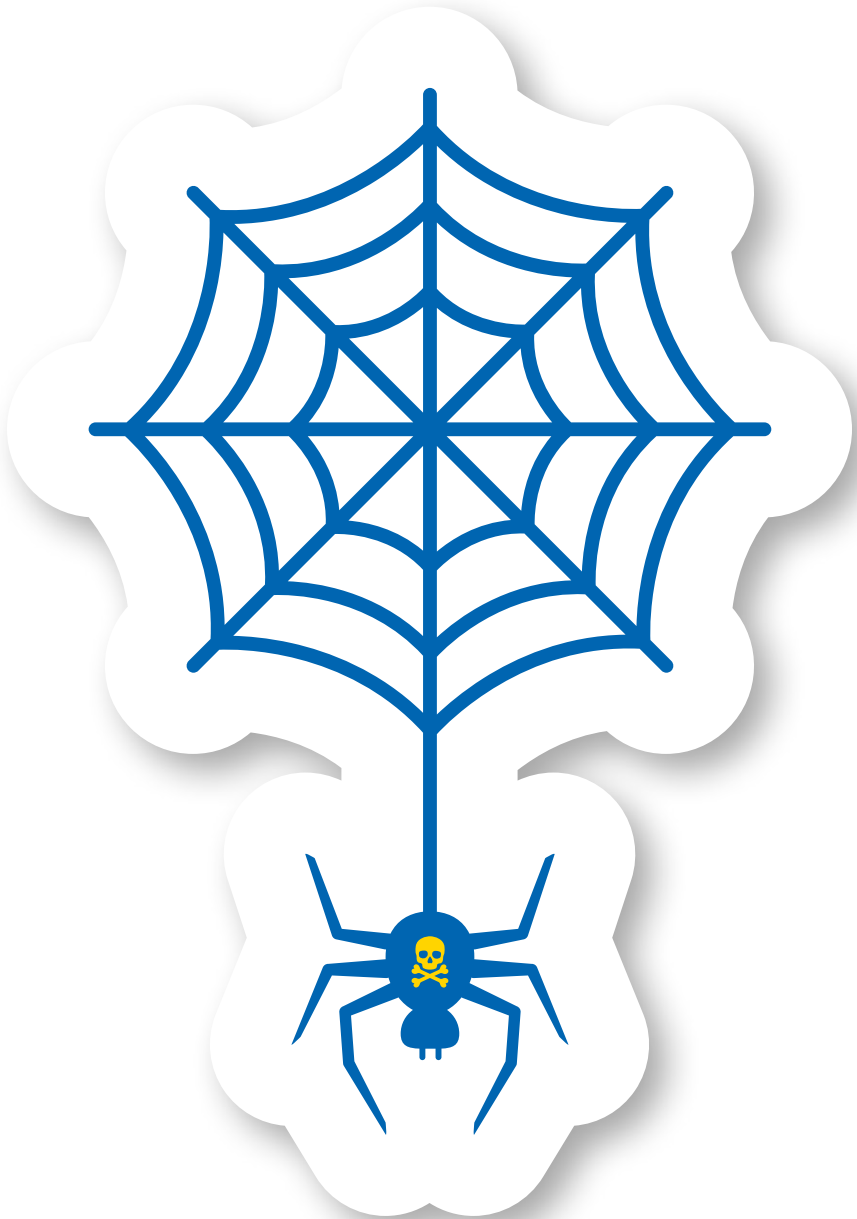
ANALOGIE AVEC LES SYSTEMES D'INFORMATION :

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.







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.

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 traînent 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.

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.cases.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.

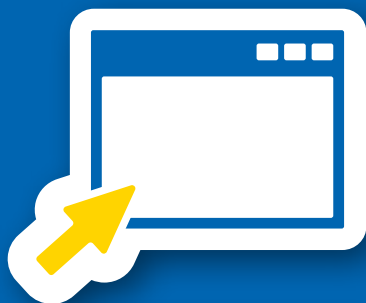
Un bon mot de passe doit être facile à retenir mais difficile à deviner. La complexité du mot de passe peut être accrue en augmentant sa longueur ; il est recommandé d'utiliser au moins 12 caractères, de préférence une quinzaine. Si le système utilisé vous impose une taille maximale vous pouvez augmenter 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 année comporte 4 saisons et 12 mois !)

SITES UTILES



cybersec.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.

→



Le site **MS&P** 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.



email : **LR@BOX**



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

