SECURITE DES SYSTEMES D'INFORMATION

GUIDE DES BONNES PRATIQUES

Je protège mes données

CRef CONSEIL DES RECTEURS

fnrs LA LIBERTÉ DE CHERCHER

ULB UNIVERSITÉ LIBRE DE BRUXELLES

UMONS Université de Mons

UNIVERSITÉ SAINT-LOUIS BRUXELLES

UCLouvain SAINT-LOUIS BRUXELLES

UCLouvain

LIÈGE université

UNIVERSITÉ DE NAMUR

SOMMAIRE

ÉDITO P03

#1
BYOD P05

#2
AUTHENTIFICATION..... P19

#3
HACKING SOCIAL P23

#4
LOGICIEL
ET MATERIEL P29

#5
SÉCURISER
SES DONNÉES P33

ÉDITO

Smartphones et ordinateurs sont devenus incontournables dans nos vies, mais ils sont également devenus une source importante pour la dispersion d'informations qui nous concernent.
En grande partie parce que le numérique a modifié notre comportement quotidien. Dans notre nouvelle société virtuelle, le besoin d'exister aux yeux des autres va nous pousser à une activité intense. Et plutôt que de privilégier le tête-à-tête de la vie réelle, nous sommes nombreux à préférer le tête-à-tête à l'écran de notre smartphone.
C'est d'ailleurs avec lui que nous partageons d'abord nos photos, nos émotions et notre vie privée.
Quand vous vous baladez dans un espace public, il vous suffit de lever la tête et de regarder autour de vous. Vous découvrirez tous ces gens qui glissent le doigt sur leur écran pour faire défiler des contenus afin de voir comment les autres ont pu réagir à leurs publications. Ce pouce levé qui va agir sur notre mental comme une récompense que nous espérions.
Mais, cette dépendance va aussi permettre de nous cibler à la fois en termes de contenu, mais aussi en nous faisant rapidement réagir, afin de permettre des intrusions dans nos environnements numériques personnels et professionnels.
En plus de cet usage permanent, il est donc extrêmement important de veiller à votre sécurité numérique.

Olivier BOGAERT
Commissaire de la Computer Crime Unit - Police fédérale

#1

BYOD

BYOD, avec quelques précautions

BYOD est l'abréviation de 'Bring Your Own Device' (pour « Prenez vos appareils personnels »), désigne la pratique qui consiste à utiliser son matériel personnel afin d'accéder aux réseaux/services mis à disposition par les universités. BYOD se rapporte aux scénarios d'usages dans lesquels le Service IT de l'université n'a aucun contrôle sur l'appareil qui est utilisé. Le manque de contrôle est précisément ce que les informaticiens n'aiment pas.

La sécurité de tous

Prenons un exemple. Quand nous allons faire un bowling, soit nous avons des chaussures dont la conformité est vérifiée par le personnel, soit nous utilisons celles qui sont mises à notre disposition. Nous ne pouvons pas utiliser nos chaussures de ville ou nos baskets sur la piste au risque de la détériorer. Si vous accédez à une application ou un service interne depuis un appareil complètement inconnu du service IT de l'université, il est légitime de se préoccuper de son état et de sa configuration. Le but est de s'assurer que son utilisation ne fait courir de risque à l'utilisateur, ni à ses données, ni à ses collègues, bref, à tout l'espace de services informatiques qui est à disposition.

Lorsque nous utilisons un ordinateur de l'entreprise, il est « géré » et applique toute une série de paramètres qui, ensemble, présentent certaines garanties. Si nous utilisons un appareil personnel, c'est la grande inconnue. Cela n'implique pas que la situation soit problématique, mais s'en préoccuper est légitime.
Au-delà des aspects relatifs à sa configuration, l'appareil personnel (l'ordinateur portable ou encore la clé USB) est souvent partagé avec toute la famille, ce qui peut engendrer l'exposition de vos données personnelles, professionnelles et également celles de l'université à des risques particuliers, principalement en matière de confidentialité. Vous n'avez rien à cacher, admettons, mais le RGPD (Règlement Général sur la Protection des Données) n'est pas d'accord avec ça.

Le BYOD à l'Université

En entreprise, l'utilisation d'un appareil personnel est relativement nouvelle alors qu'à l'Université, l'accès aux services informatiques depuis des appareils complètement inconnus ne date pas d'hier. Toutefois, la multiplicité des appareils et la connexion permanente donnent une autre dimension à cette question qui mérite la formulation de recommandations spécifiques.

J'ai un ordinateur de l'Université, le BYOD me concerne-t-il ?

L'utilisateur est concerné dès qu'il prend lui-même en charge le paramétrage d'un appareil : ordinateur, smartphone, tablette. Même s'il possède un ordinateur de l'Université, ce n'est pas sa seule manière d'accéder aux services informatiques : le courrier électronique sur son smartphone, une application de gestion depuis son ordinateur à la maison, etc. Dès lors, les dispositions particulières dont il est important de tenir compte dans un contexte **BYOD s'appliquent à tout le monde**.

De quelles dispositions particulières parle-t-on ?

Tout d'abord, l'appareil utilisé doit être bien tenu en matière de configuration et de mesures de protection. Ensuite, certaines pratiques doivent être évitées ou adaptées. Envisageons plusieurs aspects…

L'importance des mises à jour

Un système d'exploitation représente plusieurs dizaines de millions de lignes de code et un navigateur web en compte entre 5 et 10 millions. La complexité est telle qu'il est impossible que ces développements soient exempts d'erreurs et certaines d'entre-elles entraînent des failles de sécurité. De cela, nous pouvons déduire deux choses :

1. les mises à jour représentent la seule manière de corriger les erreurs et failles de sécurité des programmes et du système ;
2. lorsque vous ajoutez une application sur votre appareil, vous ajoutez des erreurs et donc des failles de sécurité.

Mettez à jour votre appareil dès qu'il vous le propose et n'installez que les applications qui sont strictement nécessaires. Evitez par exemple de multiplier les programmes qui font la même chose (navigateur, courrier électronique, etc). Veillez de plus à **utiliser les applications recommandées** par votre service informatique, ce sont celles qui vous offriront la meilleure solution dans le contexte spécifique de votre institution. Enfin, et ceci concerne principalement vos smartphones, **réduisez l'accès des applications à ce qui est strictement nécessaire** (Messenger ou WhatsApp ont-ils vraiment besoin d'accéder à votre géolocalisation ?). En cela nous appliquons un principe primordial de protection des systèmes d'information, celui de « moindres privilèges ».

« Mais, je n'ai pas besoin de la dernière version de Word, je ne fais que taper du texte ! »

On ne parle plus ici de correctif de sécurité, mais d'évolution globale des versions de logiciels et de systèmes d'exploitation. Le monde informatique évolue très rapidement et les menaces avec lui. Une application ou un système trop ancien peuvent devenir tout à fait inadaptés. Même si ce n'est peut-être pas justifié du point de vue fonctionnel, même si cela peut sembler abusif du point de vue économique, mettez à jour vos systèmes et logiciels à une version récente, c'est nécessaire du point de vue de la sécurité.

Un antivirus sur tous les appareils ?

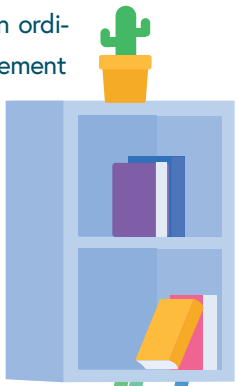
Oui, et un pare-feu aussi ! De manière générale, le virus est un programme qui s'exécute sur votre appareil au profit de quelqu'un qui n'est pas vous et toujours à vos dépends. L'antivirus veille, autant que possible à empêcher les exécutions de programmes malveillants. De la même manière que des failles et des erreurs sont présentes sur tous les systèmes, des virus existent pour tous les systèmes. Même si vous avez un mac, même si vous utilisez linux, **utilisez un antivirus.** Ça ne résout pas tous les problèmes, mais c'est un minimum.

L'antivirus est un garde qui veille au niveau de l'exécution des programmes, le pare-feu est un garde qui veille au niveau du réseau. Son rôle est tout à fait nécessaire lui aussi. Heureusement ici, votre appareil en est généralement muni d'origine, veillez simplement à ne pas le désactiver.

La sécurité physique

En matière de protection de systèmes informatiques, on entendait souvent ceci : « s'il n'y a pas de sécurité physique, il n'y a pas de sécurité du tout ». Cette expression reposait sur le fait que si une personne malveillante dispose d'un accès physique à un appareil, il ne lui faudra pas longtemps pour accéder à tout son contenu. Une petite recherche sur « mot de passe oublié » suivi de votre système « Mac », « Linux », « Windows » devrait pouvoir vous en convaincre. Aujourd'hui, on peut recourir à des systèmes de chiffrement qui permettent de s'affranchir en partie des risques liés à un accès physique à un matériel. Toutefois, dans le respect du principe de base de « défense en profondeur », la sécurité physique ne doit pas être négligée.

Ne laissez pas trainer votre portable, votre téléphone ou votre tablette, d'autant plus s'il n'est pas chiffré, mais nous reviendrons là-dessus.
Quand on imagine le risque lié à l'accès physique, on visualise souvent un hacker qui démonte l'appareil, agit sur son clavier, le connecte à un ordinateur, y branche une clé USB ou un autre dispositif. On se voit rarement soi-même intervenir, et pourtant, ce risque est bien réel. Gardez à l'esprit qu'**une clé USB ou tout périphérique branché à votre appareil peut être un vecteur pour un contenu malveillant**. Une bonne idée à ce niveau est de **désactiver l'exécution automatique / la lecture automatique**, cette fonctionnalité qui lance une action automatiquement lors de l'insertion d'un périphérique.



Sur l'ordinateur de la maison ou sur le téléphone qui ne quitte pas ma poche, pas besoin de code alors !

Rigoureusement, si vous étiez certain de toujours contrôler l'accès physique à l'appareil, en effet, vous pourriez vous passer d'autres mesures de protection. Toutefois, citons ce principe de base : attachons-nous à l'importance du contenu de cet appareil et de la raison pour laquelle il est préférable de mettre en œuvre plusieurs mesures pour le protéger.

Votre ordinateur à la maison, votre téléphone, votre portable, bref, « Your Own Device » ne contient probablement pas de données qui ne soient sauvegardées par ailleurs sur un service Cloud ou sur les serveurs de l'Université. Cela pourrait conduire à en négliger l'importance car si vous le perdez, vous ne perdez rien en termes de données, mais, outre la question de la divulgation de son contenu qui peut entrainer un problème de confidentialité plus ou moins grave, il est aussi le point d'entrée à tous vos services informatiques. Cet appareil détient potentiellement les clés de toutes les portes, les mots de passe de tous vos services, et il a donc valeur de coffre-fort. Il peut s'agir de l'enregistrement de mots de passe du navigateur ou encore d'un outil de gestion de mot de passe. Donc, même si intrinsèquement, il ne représente pas de valeur ou de risque, traitons cet appareil personnel

avec les égards qu'il mérite et utilisons un code pour en protéger l'accès. Ce code peut prendre diverses formes, allant du traditionnel mot de passe, à la biométrie, en passant par le code d'identification « PIN », des points à relier, etc. Veillez à utiliser un code qui soit « fort ». Ne négligez pas la complexité du mot de passe de votre ordinateur personnel et s'il est partagé, définissez plusieurs utilisateurs avec des espaces de travail disjoints. Cette précaution permet d'éviter le risque d'une indiscrétion sur vos données professionnelles si, par exemple, votre mot de passe est enregistré dans le navigateur d'une session partagée.

Lorsque vous utilisez votre code, veillez bien à ce qu'on ne puisse le voir par indiscrétion par-dessus votre épaule.

Si votre appareil dispose d'une solution biométrique, utilisez là, c'est la meilleure solution alliant protection et facilité d'utilisation. S'agissant de biométrie, il peut être utile de pouvoir la désactiver rapidement, ce qui est réalisé en maintenant « power » et « vol+ » ou par 5 appuis rapides sur « power » sur un iPhone par exemple.

Quand le code d'accès est-il demandé ? Quand l'appareil est verrouillé ! Configurez un verrouillage automatique après un délai d'inactivité sur votre smartphone comme sur votre ordinateur.
Utilisez un mot de passe ou un code fort sur tous les appareils, une solution biométrique si possible, avec dans tous les cas un verrouillage automatique.

Le chiffrement

Comme nous l'avons vu, seule une solution de chiffrement peut compenser un défaut de sécurité physique comme la perte ou le vol de votre appareil. Outre les questions relatives à la sécurité déjà évoquées, il ne faut pas négliger les questions relatives à la conformité, envers le Règlement Général sur la Protection des Données à caractère Personnel (RGPD) au premier chef.

Si votre appareil recèle une quelconque donnée à caractère personnel et qu'il est perdu ou volé, en l'absence d'une solution de chiffrement, il s'agit d'une fuite de données au sens du RGPD, qui doit faire l'objet d'une déclaration à l'organe de contrôle.

Si vous utilisez un iPhone ou un téléphone Android récent, son stockage est chiffré, pas de soucis, pour peu qu'il soit verrouillé avec un code suffisamment fort lors de sa perte.

S'il s'agit d'un ordinateur, il est important d'y **activer le chiffrement du disque dur**. Chaque système d'exploitation propose des outils intégrés et simples pour assurer cette fonction, mais il existe également des solutions portables entre systèmes et de qualité, y compris dans le monde Open Source. Dans tous les cas, les progrès récents, tant au niveau du matériel que des logiciels, permettent que l'utilisation du chiffrement se fasse de façon (presque) transparente pour l'utilisateur.

Attention aux services que vous utilisez

En matière de conformité et au-delà de l'appareil que vous utilisez, se pose la question des services que vous consommez. Ne perdez pas de vue que votre responsabilité peut être impliquée dans un traitement de données, notamment personnelles, qui serait réalisé par un service que vous utilisez et qui ne serait

pas conforme aux règlements en vigueur. **Prenez connaissance des termes contractuels des services que vous utilisez** en dehors de ce qui serait préconisé (supporté, validé et encadré) par votre service informatique, principalement en matière de confidentialité. Le recours à une solution en dehors de tout cadrage de votre service informatique, c'est ce que les professionnels appellent le « ShadowIT » et ce n'est en effet pas sans risques.

BDNY ou quand « you Bring a Device which is Not Yours »

Dans le paragraphe relatif à la sécurité physique, il est dit en d'autres termes que « dès que quelqu'un a un accès physique à votre ordinateur, ce n'est plus votre ordinateur ». Et si, dès le départ, ce n'est pas votre ordinateur, comme un pc public dans un bibliothèque ou un centre de congrès, est-il prudent de l'utiliser ?
Et bien tout dépend de ce que vous voulez en faire. Si vous avez besoin de rechercher un horaire de bus, pas de soucis, mais utilisez néanmoins le mode « privé » du navigateur afin d'éviter tout enregistrement local de votre activité.

Si vous voulez vous connecter à votre service de courrier électronique, ne le faites pas ! Vous ne pouvez pas avoir la moindre confiance en un appareil inconnu, tant au niveau de ce qui y est installé comme logiciel que comme matériel. Il existe par exemple des programmes d'espionnage, ou même de petits appareils qui peuvent se connecter en USB, qui enregistrent tout ce qui est tapé au clavier. De quoi récupérer facilement votre mot de passe, le cas échéant.

Ne laissez rien, en termes de données ou fichiers, et ne donnez rien, en termes de code d'accès, d'information personnelle ou confidentielle lorsque vous êtes connecté à un ordinateur public !

Je ne me connecte jamais à un réseau non sécurisé !

Le caractère sécurisé ou non d'un réseau sans fil n'a pas d'incidence directe pour celui ou celle qui l'utilise. En effet, le côté sécurisé du réseau porte principalement sur la manière de s'y connecter. Un réseau non sécurisé est accessible à tout le monde ; un réseau sécurisé nécessite un code pour s'y connecter. Au-delà de la connexion, le risque lié à l'utilisation d'un réseau sans fil dépend surtout de ce que vous en faites car la sécurité des données n'est pas assurée par le réseau, mais par l'application qui est utilisée (*).

Pratiquement tous les échanges sur internet passent par un espace sur lequel tant l'expéditeur que le destinataire ne savent rien et n'ont aucun contrôle. L'échange est sécurisé malgré tout au niveau des applications qui assurent un chiffrement des échanges de données et non au niveau du « transport ».

Il est donc préférable d'utiliser une application sécurisée sur un réseau non sécurisé que le contraire. Pour prendre une illustration classique, si vous accédez à une application de votre institution avec une adresse https validée dans votre navigateur, peu importe que vous soyez sur un réseau non sécurisé, les échanges sont chiffrés et donc illisibles pour les autres utilisateurs de ce réseau, tout va bien de ce point de vue.

Une réserve sur le caractère ouvert du réseau doit toutefois être émise. Puisque n'importe qui peut s'y connecter, on peut potentiellement y trouver n'importe quoi comme comportement, ce qui en fait un environnement potentiellement agressif et contre lequel votre appareil doit être protégé. Les protections mentionnées plus tôt, notamment les mises à jour, le pare-feu et l'antivirus, prennent ici toute leur importance. En toutes circonstances, votre appareil doit être « bien tenu ».

Dans tous les cas, réfléchissez toujours à 2 fois avant de vous connecter à un réseau ouvert que vous ne connaissez pas : ils sont l'un des moyens les plus directs pour récupérer l'information sur vous, voire de compromettre votre machine. D'une part, il y a de fortes chances qu'une bonne partie de votre activité sur le réseau ne puisse pas être chiffrée et même lorsqu'elle l'est, le fait que l'opérateur du réseau puisse l'analyser lui donne déjà de précieuses informations sur vous, même sans avoir accès aux données chiffrées. Enfin, et sans entrer dans les détails, il existe également des techniques qui permettent aussi de compromettre le chiffrement applicatif lorsqu'on contrôle un point de passage obligé du traffic réseau (comme c'est le cas de l'opérateur d'un réseau d'accès, wifi ou autre), cela vaut donc bien la peine d'y penser à deux fois lorsqu'on envisage de se connecter à un réseau ouvert inconnu.

(*) Un raccourci est pris ici, car en toute rigueur, la sécurité d'un réseau sans fil porte sur deux aspects : son accès et un chiffrement des échanges qui y sont réalisés. Le réseau assure donc un rôle dans la sécurité des données, mais ce rôle demeure local au réseau sans fil concerné. Si on considère un usage classique à travers internet, c'est au niveau des applications que la sécurité des données doit être envisagée. Dans ce cas, peu importe donc que le réseau sans fil utilisé soit sécurisé ou non puisque l'enveloppe de protection est fournie à un autre niveau et couvre l'échange de données de bout en bout.

VPN : sécurité de l'accès réseau

Commençons par le début. VPN, c'est un réseau privé virtuel (Virtual Private Network) qui trouve son origine dans la situation suivante : vous travaillez dans une entreprise qui dispose de son réseau propre et de serveurs internes qui y sont connectés. L'entreprise est connectée à Internet, mais tous les serveurs ou services ne sont pas accessibles depuis l'extérieur pour différentes raisons.

Afin de permettre un accès à un service interne depuis une connexion externe, un utilisateur peut recourir à une connexion VPN. Le VPN établira une sorte de tuyau dans lequel passeront les connexions jusqu'au réseau

de l'entreprise. Partant de là, tout se passe comme si l'ordinateur distant se trouvait, d'un point de vue logique, dans l'entreprise. Il peut donc accéder à toutes les ressources locales qui ne sont pas « publiées » sur internet.

Pour nos universités, c'est souvent le cas des ressources bibliographiques par exemple. Par ailleurs, comme le VPN permet de faire croire qu'un ordinateur est ailleurs, il a d'autres utilités moins glorieuses, comme le contournement des restrictions de marchés sur les catalogues de vidéo à la demande, ...

En résumé

- Mises à jour
- Applications minimales / applications supportées
- Antivirus & pare-feu
- Sécurité physique
- Code d'accès & verrouillage automatique
- Chiffrement des données locales
- Termes de confidentialité des services
- Attention à l'utilisation d'un réseau et d'un ordinateur partagé
- Rester vigilant

Dans un avenir proche, il est fort probable que tout cela soit simplifié grâce à des solutions techniques de gestion des appareils mobiles (MDM, Mobile Device Management), mais en attendant, c'est votre appareil et d'une certaine manière, votre responsabilité. La mise en œuvre de ces recommandations peut être simple pour certaines comme très technique pour d'autres. N'hésitez pas à faire appel à votre service informatique pour vous aider.

Toutes ces mesures appliquent deux principes fondamentaux de la sécurité de l'information : la **« défense en profondeur »** et les **« moindres privilèges »** conduisant à une situation qui donne de très bonnes garanties. Il faut ajouter qu'il est toujours possible d'aller plus loin en matière de mesures de protection, mais ce sera au prix d'une plus grande complexité de mise en œuvre et d'utilisation au quotidien. Et surtout, après tout cela, il y a ce qu'on en fait. Il n'y a aucun système informatique sur terre qui, à un moment ou un autre, ne repose sur un être humain. C'est à ce niveau que se portent aujourd'hui la majorité des attaques. L'appareil est maintenant bien configuré, n'oublions pas de configurer l'utilisateur.

#2

AUTHENTIFICATION

Authentification

Passons à présent à un autre chapitre important qui concerne l'authentification. Mais avant tout, prenons le temps de définir quelques termes importants.

Définitions :

- **Authentification**

L'authentification est un processus par lequel un système informatique s'assure de l'identité d'un utilisateur afin d'autoriser l'accès de cet utilisateur à des ressources du système en fonction des droits qui lui ont été attribués.

- **Identifiants**

Une authentification se fait au moyen d'identifiants. Ces identifiants sont généralement composés d'un ID et d'un mot de passe. L'ID est fourni par l'Université et l'utilisateur y associe un mot de passe secret de son choix.

- **Authentification Multi-Facteurs (AMF)**

L'Authentification Multi-Facteur est une authentification qui met en œuvre, de façon concomitante, des procédés de vérification faisant appel à au moins deux facteurs d'authentification différents. Parmi les principaux facteurs d'authentification, on trouve : « ce que l'on sait » (par exemple, un mot de passe), « ce que l'on possède » (par exemple, un appareil mobile), « ce que l'on est » (par exemple, l'empreinte digitale). C'est ce l'on peut qualifier de méthode d'authentification forte.

L'authentification permet d'éviter de vivre des situations particulièrement délicates.

Pour prendre la mesure de l'importance de l'authentification, prenons un exemple : « Alice est la responsable des travaux de recherche pour son département, à l'Université. Elle doit donc régulièrement accéder aux documents partagés et stockés sur le système en ligne de l'Université. Mais Alice utilise, par facilité, un mot de passe simple (123Soleil). Ce mot de passe a pu, lors d'une cyberattaque être rapidement deviné par les pirates informatiques. Ces derniers ont pu chiffrer tous les travaux du département d'Alice et exigent maintenant le paiement d'une rançon de 100.000€ pour déchiffrer ces documents sans lesquels tout le département est paralysé ! »

Que faire pour éviter d'être en difficulté ? Voici les règles élémentaires à respecter impérativement :

- **Choisissez un mot de passe composé d'un maximum de caractères**
- **Mélangez des lettres, majuscules et minuscules, des chiffres et des caractères spéciaux pour composer ce mot de passe**
- **Ne communiquez jamais vos identifiants à qui que ce soit**
- **Utilisez des mots de passe différents pour chaque application est l'idéal, mais, au moins utilisez un mot de passe différent en fonction des niveaux de sécurité recquis (Banque vs site de bricolage)**
- **Changez régulièrement votre mot de passe**
- **Utilisez un système à plusieurs facteurs si il est disponible**

Bon à savoir :

Un mot de passe complexe peut être simple à retenir s'il est composé d'une phrase personnelle. Le « password » est mort, vive la « passphrase ». N'utilisez pas un mot, mais utilisez une phrase. La phrase aura un sens pour vous, contrairement à un mot complexe, et sera facile à retenir. Elle sera un peu longue à taper au début, mais le mot de passe ainsi constitué est tellement robuste que vous n'aurez pas à le changer et vous aurez donc largement le temps de vous y habituer.
Et pour que ce soit vraiment très « fort », ajouter votre propre « clé de cryptage » personnelle dans votre phrase : vous remplacez par exemple les « i » par des « 1 », les « e » par des « 3 » (ne faites pas ça strictement, c'est un exemple). L'idée est ici de conserver le principe de la phrase en faisant en sorte que ses éléments ne soient plus vraiment des mots au sens de leur existence dans le dictionnaire.
La résultante est un excellent mot de passe, facile à retenir et qui deviendra vite facile à taper à l'usage.

L'authentification multi-facteur est disponible en Belgique à travers le FAS (Federal Anthentication Service), soit grâce à la carte d'identité électronique, soit via des applications comme « ITSME ». Il existe aussi des systèmes d'AMF basés sur des systèmes de certification internationaux tels que « Memority », « Microsoft Authenticator » ou « Google Authenticator ».

Par ailleurs, des **applications de gestion de mots** de passe comme Keypass ou OnePasword sont également disponibles. Attention, ce gestionnaire de mots de passe contiendra TOUS vos mots de passe et donc en le perdant, il vous faudra les changer TOUS !

#3

HACKING SOCIAL

Hacking social

« Ce n'est pas la technologie qui nous piège mais trop souvent nos émotions »

Beaucoup de solutions existent en termes de sécurité informatique, mais notre comportement demeure le meilleur bouclier contre les risques en matière de cybersécurité. Nous le savons, nos cerveaux sont régis par nos émotions et des pensées rationnelles, ce qui nous rend vulnérables face à ceux qui sont mal intentionnés et fait de nous des victimes potentielles du piratage.

Les modes opératoires des cybercriminels peuvent inspirer la peur ou la curiosité, mais l'objectif est de vous amener à réaliser des actions que vous n'auriez probablement pas exécutées dans un autre environnement. En effet, plutôt que de pirater nos équipements informatiques, il est plus simple d'obtenir nos mots de passe en nous les demandant. Au travers d'une communication anodine, nous fournissons généralement beaucoup d'informations sensibles sur nous.

Cette technique relève de l'ingénierie sociale.
Cela peut arriver dans le cadre d'une conversation insignifiante, lors d'un échange sur les réseaux sociaux. Souvent les questions de sécurité sont déduites de ces informations sensibles que nous divulguons (date importante, sport préféré, etc.).

Bien se protéger en vaut la peine. Dotés des bonnes informations, nous pouvons tous le faire. La sécurité sur Internet peut nous sembler complexe et donc, il nous arrive souvent de l'ignorer. En adoptant un mode de pensée axé sur la sécurité nous pourrons mieux la gérer. La prudence se situe entre la pratique et la sécurité.

L'ingénierie sociale, ou « social engineering », est une technique qui vise à accéder à des informations confidentielles ou à des équipements informatiques grâce à la **manipulation** directe ou indirecte des personnes.

Nombre de ces arnaques commencent par le courrier électronique. Il est le moyen le plus courant d'envoyer de la correspondance par Internet. Il est facile de concevoir un courrier électronique qui semble provenir d'une organisation connue. Cependant, la véracité du nom et des renseignements associés à une adresse n'est jamais garantie.

La messagerie électronique est dépourvue de système de sécurité.
Cela se traduit de la manière suivante :

- **il n'existe aucun moyen de vérifier l'identité de l'expéditeur ou la nature du courrier électronique;**
- **tous les éléments d'un courrier électronique sont falsifiables et manipulables;**
- **les courriers électroniques envoyés ne sont par défaut pas sécurisés et peuvent être lus ou modifiés au cours de sa livraison;**
- **les courriers électroniques peuvent contenir des logiciels malveillants.**

Avec les courriers électroniques, soyez calme et lucide, prenez votre temps et surtout examinez les points suivants :

Connaissez-vous l'expéditeur ?

Le nom de domaine de l'expéditeur est-il suspect ?

Ce courrier est-il attendu ?

Le sujet est-il en lien avec vos activités ?

Il est indispensable de systématiquement se poser ces questions. En cas de doute, prévenez un référent informatique.

D'autres éléments de manipulation doivent être aussi pris en considération : facture ou pièce jointe anormale, appel à un sentiment d'urgence, lien web étrange ou caché, fautes d'orthographe, annonce d'héritage, etc.

Même si le message vous semble authentique, la prudence et un peu de jugement réduisent votre risque de préjudice :

- **réfléchissez avant de cliquer et résistez à la pression que les pirates exercent pour vous soutirer de l'information ;**
- **méfiez-vous des courriers électroniques. Ils ne sont pas dignes de confiance. Faites preuve d'esprit critique ;**
- **ne craignez pas de communiquer avec une organisation pour faire des vérifications.**

Les réseaux sociaux permettent d'échanger de l'information. C'est aussi un facteur de socialisation, mais ils présentent de nouveaux risques. Les grands noms des logiciels de réseaux sociaux (Facebook, LinkedIn, …) offrent plusieurs paramètres pour contrôler la confidentialité de votre profil et de vos interactions. Prenez le temps de vous informer sur ces possibilités. La configuration de ces options peut être longue mais il est essentiel de le faire pour augmenter la sécurité de votre compte. Ainsi seuls vos amis ou des listes spécifiques pourront voir vos propos et informations privées. Reprenez le contrôle et ne laissez jamais les paramètres par défaut.

Une autre menace qui combine l'usage du courrier électronique et de votre parcours sur Internet, est l'extorsion par le chantage. Les pirates peuvent vous menacer de rendre publiques des informations confidentielles vous concernant si vous ne réalisez pas **une action** pour eux. Il est

important de se rappeler que la confidentialité et l'anonymat n'existent pas sur Internet. Peu importe la technologie ou la plateforme utilisées, l'usage des technologies de l'information laisse toujours des traces.

En général, vous recevez un courrier électronique qui vous menace de rendre publiques certaines informations confidentielles vous concernant si vous ne les payez pas. Ils affirment aussi qu'ils ont réussi à infecter votre ordinateur et ont pu accéder à des informations compromettantes (par exemple sur le fait que vous visiteriez des sites pour adultes).

Ces maîtres-chanteurs ne détiennent généralement aucune donnée compromettante sur vous. Il est possible qu'ils possèdent comme information sur vous un mot de passe que vous utilisez ou avez utilisé. Sachez que ce genre d'information est malheureusement disponible sur Internet suite à des fuites de données depuis certains sites internet que vous utilisez. Ils n'ont pas eu besoin d'entrer dans votre ordinateur pour obtenir cette information.

Que dois-je faire ?

Ne paniquez pas

Ne payez pas

Modifiez vos mots de passe si vous avez un doute

Rappelez-vous un mode de pensée axé sur la sécurité sera votre meilleur allié sur Internet : **votre bon sens est votre meilleur système de défense.**

#4

LOGICIEL ET MATERIEL

Logiciel et matériel

« Mon ordinateur a été piraté ! »

Alain vient de recevoir la visite de son support informatique, qui a détecté un comportement anormal de son ordinateur. Après vérification, il s'avère que plusieurs logiciels malveillants (malwares, en anglais) ont été installés à son insu. Cela aurait pu être pire : tous ses fichiers auraient pu être monnayés contre rançon, effacés, voire volés et revendus…

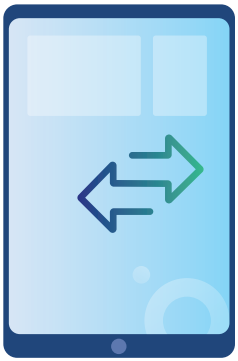
Comment est-ce possible ?

Comme expliqué brièvement au chapitre précédent, si le phishing (hameçonnage, technique utilisée pour obtenir des renseignements personnels dans le but de perpétrer une usurpation d'identité) et le social engineering représentent l'immense majorité des cyberattaques réussies, les cybercriminels peuvent également exploiter les faiblesses de nos ordinateurs, plutôt que de tromper les utilisateurs eux-mêmes.

Nos ordinateurs peuvent être vulnérables. Les logiciels sont devenus des monstres de complexité, et de cette complexité découlent inévitablement des erreurs et des failles. Ces dernières sont analysées et exploitées à distance pour commander à nos ordinateurs de réaliser des actions à notre insu, visant la plupart du temps à installer des virus et autres malwares. Une fois cela fait, le pirate pourra soit contacter sa victime pour monnayer la restauration de la santé de l'ordinateur, soit utiliser l'ordinateur en toute discrétion pour en attaquer d'autres par exemple.

Comment se protéger de ces vulnérabilités ?

Comme nous l'avons vu, des moyens le permettent. On a cité le fait d'effectuer les **mises à jour** régulières (du système d'exploitation, des applications...), d'utiliser un **antivirus** moderne (attention de n'en installer qu'un seul, sinon ils peuvent se neutraliser), ou encore d'autres mesures de protection comme un **pare-feu**, un antimalware ou le **chiffrement** de votre disque dur à confier à votre support informatique local.



Malgré toutes ces précautions, mon ordinateur est infecté… que faire ?

1. Une bonne réaction initiale est de déconnecter votre ordinateur du réseau (câblé et WiFi), de la sorte, vous coupez l'accès du pirate à votre ordinateur, les virus ne risquent pas de se propager aux autres ordinateurs du réseau, et l'exfiltration de vos données est impossible.

2. Déconnectez également vos périphériques de stockage USB (disque dur portable…), et vérifiez en parallèle si les données de vos sauvegardes ont été affectées.

3. Dans la mesure du possible, adressez-vous à votre support informatique. Vos données professionnelles comme vos photos privées des 10 dernières années ont trop de valeur pour laisser les choses au hasard.

#5

SÉCURISER SES DONNÉES

Sécuriser ses données

Nous manipulons tous de grandes quantités de données dans notre travail quotidien. Qu'il s'agisse simplement de nos emails, de résultats de recherche de publications ou de rapports divers, elles sont variées et demandent souvent à être protégées de façon adaptée à leur nature et aux contraintes qui s'y attachent.

Choix du support

Le choix du support des données informatiques va évidemment dépendre de leur nature et de l'usage qu'il en sera fait. Dans la plupart des cas, le stockage sur un ordinateur de l'institution est suffisant pour vos emails ou vos documents personnels, mais la question devient plus épineuse lorsqu'on envisage de partager les données avec des collaborateurs.

Dans tous les cas, on notera toutefois que si le support contient des données sensibles (au sens de la vie privée ou de la propriété intellectuelle par exemple), il conviendra de chiffrer ces données par des moyens cryptographiques (voir plus bas).

Supports amovibles et/ou portables

En fonction de la taille, l'utilisation d'un disque dur externe, d'une simple clé USB ou encore d'une carte mémoire (ex. SD) peut s'avérer utile mais doit faire l'objet d'attentions particulières : par sa nature, un tel support peut être volé, perdu ou encore endommagé facilement. C'est d'ailleurs aussi plus généralement le cas des ordinateurs portables qui sont souvent utilisés comme premier moyen de stockage. Il conviendra donc d'en assurer le backup (nous y reviendrons) et la protection physique : surveillance personnelle, fermeture des portes, utilisation de cadenas de sécurité.

Supports distants

L'utilisation de supports distants nous permet non seulement de pouvoir accéder à nos données depuis plusieurs postes de travail, mais aussi de les partager avec nos collaborateurs.

En règle générale, privilégier uniquement l'utilisation des services institutionnels doit être considéré comme une règle d'Or ! Qu'il s'agisse de partages Windows ou d'outils de cloud privé (tel que Owncloud/Nextcloud) ou de cloud public professionnel (tel que Office365), l'infrastructure institutionnelle est sécurisée par des informaticiens professionnels et placée sous la responsabilité de l'institution, notamment par rapport au respect des législations en place (ex. RGPD).

Si les possibilités offertes par l'institution ne conviennent pas à votre besoin : parlez-en avec le service informatique ! On ne connait pas toujours tout ce qui est possible en termes de moyens et d'adaptations.
Si vraiment vous êtes contraints d'utiliser un service de stockage externe : prudence ! Les services gratuits (Google Drive, Dropbox, iCloud et autres)

sont généralement à proscrire : « lorsque c'est gratuit, c'est vous le produit ». Veuillez toujours faire en sorte de disposer d'un contrat en bonne et due forme avec votre prestataire et assurez-vous des clauses concernant la sécurité des données lors de la définition du marché public. La mise en application du RGPD a ajouté de très importantes contraintes par rapport à l'utilisation de ces services, l'usage du chiffrement (voir plus loin) devrait y être systématique, par simple mesure de précaution. N'hésitez-pas à consulter votre responsable de la sécurité informatique pour être conseillé à ce sujet.

Protection des données

Quel que soit le support choisi, il est toujours primordial, pour des données partagées, d'identifier qui peut y accéder (lecture/écriture) pour quels usages et pendant combien de temps.

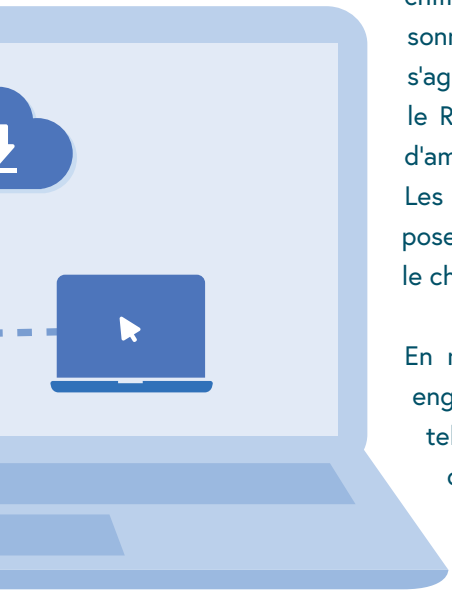
Gestion des droits d'accès

Les services de partage de fichiers ou d'édition collaborative offrent généralement la possibilité de définir finement ces droits d'accès (n'utilisez pas ceux qui ne le permettent pas). La définition précise de ces droits (où chacun peut faire ce qui lui est nécessaire mais pas plus, moindre privilège) et la gestion de ceux-ci dans le temps (par exemple lorsqu'un collaborateur quitte le projet) représentent un enjeu très important pour la gestion de

vos données et devraient faire l'objet d'une responsabilité spécifique au sein de tout projet.

Cryptographie et Chiffrement

Lorsque l'on manipule des données sensibles, par exemple au sens du RGPD pour les données à caractère personnel, ou des données précieuses, brevets ou plus généralement de Propriété intellectuelle de l'institution, l'usage du chiffrement devrait être envisagé systématiquement. Le chiffrement des données permet d'éviter qu'une personne tierce puisse les lire et les exploiter. Lorsqu'il s'agit de données sensibles à caractère personnel, le RGPD impose l'usage du chiffrement sous peine d'amendes très élevées en cas de fuite.



Les services informatiques de votre institution proposent des solutions permettant de mettre en place le chiffrement de vos données de façon sécurisée.

En règle générale, ces solutions cryptographiques engendrent quelques contraintes supplémentaires, telle que la gestion de clefs de chiffrement qui doivent être sécurisées, ou une authentification plus forte, utilisant par exemple en plus du login et mot de passe, une confirmation par SMS. En fonction des solutions choisies, ces contraintes seront plus ou moins fortes mais nécessitent votre implication personnelle pour être efficaces. Il faut se souvenir qu'en cas de perte des clés de chiffrement, il n'est tout simplement plus possible d'accéder aux données chiffrées ! L'usage de la cryptographie

dans votre institution adresse ce problème au niveau global afin de garantir que la récupération des données chiffrées reste possible.
En matière de cryptographie, comme pour toute la sécurité informatique, « la sécurité par obscurité n'existe pas ». Privilégiez toujours les logiciels utilisant des algorithmes bien connus et éprouvés. Les solutions Open-Source, dont le code peut être audité, devraient être utilisées préférentiellement.

Sauvegardes des données

Quel que soit le niveau de sécurité de vos supports ou de vos outils, la sauvegarde de vos données ou backup doit faire l'objet d'une attention particulière. Il faut pouvoir disposer de backups réguliers, automatiques et stockés de manière sécurisée.
Comme toujours, privilégiez l'utilisation des services institutionnels. Même s'il est souvent très facile d'acheter et d'installer un disque dur externe bon marché pour y faire ses backups, celui-ci constitue un support de données potentiellement très sensibles et qui doit être sécurisé comme tel (voir ci-dessus). Le backup de vos données professionnelles devrait être placé sous la gestion et la responsabilité des informaticiens de l'institution.

Cycle de vie des données

Les données que nous manipulons dans le cadre de notre travail sont souvent associées à des contraintes de conservation particulières : la durée d'un projet, le temps d'une thèse ou parfois à très long terme pour archivage. Le cycle de vie de vos données devrait être défini dès le départ : depuis l'acquisition jusqu'à l'archivage en passant par le stockage. C'est une occasion de définir les mesures de sécurisation appropriées pour chacune de ces étapes.
L'archivage ou la destruction des données en fin de projet est une étape importante qui ne doit pas être négligée.

ULB
Contact : Alex Genatzy
Email : rssi@ulb.be
Lien : https://portail.ulb.be/fr/informatique/securite-it

ULiège
Contact : Simon François
E-mail : rssi@uliege.be
Lien : https://my.segi.uliege.be/securite

Université St Louis Bruxelles
Contact : Pierre Reinbold
E-mail : rssi@usaintlouis.be
Lien : https://usaintlouis.be/securite-it

UCLouvain
Contact : Pierre Reinbold
E-mail : rssi@uclouvain.be
Lien : https://intranet.uclouvain.be/fr/myucl/services-informatiques/securite-it.html

Université de Mons
Contact: Alexandre Amorison
E-mail: rssi@umons.ac.be
Lien: https://www.umons.ac.be/cism

UNamur
Contact: Alain Foulon
E-mail: rssi@unamur.be
Lien: https://terranostra.unamur.be/pssi

Editeur responsable: Pierre Wolper, Président du CRef