ÉCOLE POLYTECHNIQUE
FÉDÉRALE DE LAUSANNE

Le petit guide illustré

sécurité IT

Comment se prémunir contre les cyber-attaques

LA SÉCURITÉ INFORMATIQUE

La sécurité informatique vous concerne. Que vous le vouliez ou non, elle concerne tout le monde, sceptique ou convaincu.

Vols de matériel ou de données, usurpation d'identité virtuelle, ou encore surveillance des faits et gestes numériques ne sont plus l'apanage des personnalités célèbres, mais peuvent arriver à n'importe lequel d'entre nous.

En tant qu'acteur-clé dans une école polytechnique de renom, chacun se doit de connaître les risques en termes de sécurité informatique et de savoir comment réagir face aux menaces de plus en plus présentes - qu'elles soient virtuelles ou non.

Au travers de conseils simples et d'exemples concrets, nous vous proposons de réduire au maximum les risques liés à l'utilisation de l'informatique.

Sommaire

1 **Mot de passe**
2 **Poste de travail**
3 **Utilisation nomade : clés USB et disques durs externes**
4 **Connexion à un wifi public**
5 **Copyright et téléchargements**
Attention à ma boite mail !
6 **Courriels malveillants**
7 **Phishing / Hameçonnage**
8 **Hoax / Canulars**
9 **SPAM / Pourriels**
10 **La jungle du web**
10 **Cookies**
11 **Internet sans peur et sans reproche**
11 **Sites protégés et connexion chiffrée**
12 **Classifier l'information pour se protéger**
13 **Glossaire**

Impressum :

Rédaction : Magaly Mathys, Céline Deleyrolle, Julien Robyr (Communication IT, VPSI)
Illustrations: Igor Paratte (Pigr)
Graphisme : Julien Robyr
Impression : Centre d'impression EPFL
Avec la collaboration de Patrick Saladino et Jean-François Dousson (Sécurité IT, VPSI)

EPFL
ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE

MOT DE PASSE

POURQUOI EST-CE IMPORTANT ?

Votre mot de passe est similaire à une clé de coffre-fort : personnelle, intransmissible, il n'y en a qu'une par modèle et le code qui y est apparenté doit être unique, secret et suffisamment complexe.

Il est réellement votre arme la plus efficace contre une cyber-attaque. Choisissez-le bien!

Et utilisez en plusieurs!

COMMENT CHOISIR ?

A chaque utilisation son mot de passe ; évitez d'utiliser toujours le même, même si c'est pratique pour s'en souvenir. Et surtout, changez régulièrement vos mots de passe (au moins une fois par an).

Evitez les mots courts, évidents, les prénoms et autres dates de naissance. Ne facilitez pas la tâche aux hackers!

Qu'est-ce qu'un bon mot de passe ? Il doit contenir une douzaine de caractères au minimum : combinaison de lettres majuscules, minuscules, de chiffres et caractères spéciaux. Évitez les suites numériques ou alphabétiques, et n'employez pas de mots du dictionnaire ou de noms propres.

ASTUCE BONUS

Créez des phrases. P.ex. J3b0ss34L3PFL! (= "Je bosse à l'EPFL!")

Voici une liste des pires mots de passes les plus couramment utlisés par les internautes :

12345678	BATMAN
PASSWORD	1111111
QWERTZ	ACCESS
FOOTBALL	696969
ABC123	MOTDEPASSE
LETMEIN	12345

(source: splashdata)

ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE

VOTRE POSTE DE TRAVAIL

QUELQUES HABITUDES DE TRAVAIL

POUR DIMINUER FORTEMENT LE RISQUE DE PIRATAGE

- **Attachez l'écran et l'unité centrale avec un câble de sécurité. Gardez la clef dans un endroit sûr.**
- **N'utilisez votre compte administrateur que lorsque vous en avez besoin et déconnectez-vous ensuite.**
- **Activez l'écran de veille protégé par mot de passe après 15 minutes maximum.**
- **N'installez aucun logiciel piraté ou dont vous n'êtes pas sûr de la provenance.**
- **Sous Windows, installez l'antivirus officiel de l'Ecole.**
- **Activez les mises à jour automatiques.**

Un nouveau poste de direction vient de s'ouvrir à l'EPFL. Deux collaborateurs ont postulé, Robert et Aline. Ils se connaissent, mais ne s'apprécient guère en raison de vieux contentieux professionnels.

Un soir, après avoir travaillé tard, Robert passe devant le bureau d'Aline et remarque que son ordinateur fixe est allumé. Il lui suffit de quelques minutes pour trouver des informations personnelles gênantes et les envoyer à la direction avec l'identifiant d'Aline. Celle-ci démissionne une semaine plus tard et Robert décroche le poste.

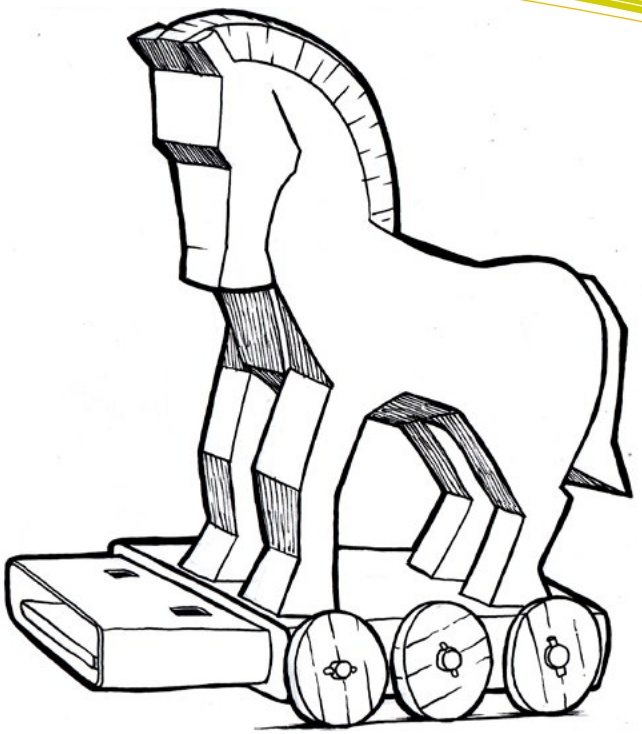
LES RISQUES

Il suffit de quelques dizaines de secondes pour qu'un poste de travail sans surveillance devienne la cible d'une personne mal intentionnée. Le vol de matériel représente le cas le plus courant car le plus visible, mais vols de données et accès non autorisés à des services web de l'Ecole engendrent des risques sérieux pour l'utilisateur et l'EPFL.

EPFL
ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE

CLÉ USB
DISQUE DUR EXTERNE UTILISATION NOMADE

Même sans ouvrir de fichier, une clé USB peut contenir un amorçage automatique (autorun) et un malware programmé pour voler tous les documents sensibles et les identifiants. De plus, une porte dérobée peut être installée sur le serveur du laboratoire.



Corine est doctorante en physique nucléaire. Lors d'une pause-café, elle trouve une clé USB sur une table. Mue par une intention louable, elle la branche à son laptop pour trouver l'identité de son propriétaire. Elle ne s'est pas rendue compte que la clef contenait un logiciel espion.

ALORS QUE FAIRE ?

- **Désactivez la fonction d'exécution automatique (autorun) de contenu stocké sur des périphériques amovibles dans votre système d'exploitation**
- **Nettoyez proprement le contenu de la clé avant de la prêter. Un formatage complet est vivement recommandé.**
- **Dans la mesure du possible, ne stockez jamais d'informations sensibles sur une clé USB.**
- **Verrouillez systématiquement le poste de travail avant de vous en éloigner afin d'éviter tout incident lié à l'insertion d'une clé USB pendant une absence.**

EPFL ECOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE

LAPTOPS, TABLETTES & TÉLÉHONES PORTABLES WIFI PUBLIC

LES RISQUES

Toutes les communications que vous établissez au travers d'un réseau non sécurisé (WiFi public ou connexion filaire dans un hôtel) peuvent être interceptées à votre insu.

QUELQUES CONSEILS

- Utilisez le service VPN de l'EPFL pour chiffrer toutes vos communications.
- Dans la mesure du possible, activez le chiffrement du téléphone ou de la tablette.
- Désactivez le partage de fichiers.
- Désactivez le réseau sans fil lorsque vous ne l'utilisez pas.

BON À SAVOIR

Les données échangées ne se limitent pas aux emails ou à la navigation web, mais également à toutes les informations techniques envoyées et reçues par un ordinateur pour son fonctionnement.

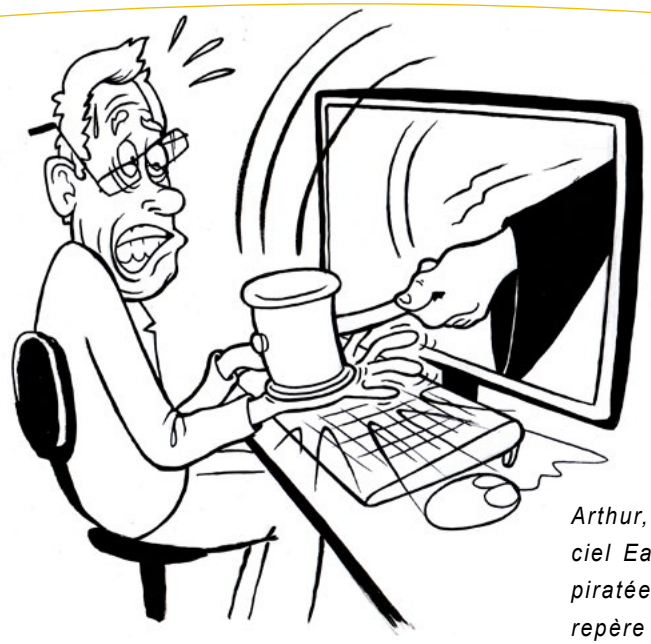
Alain est directeur d'un laboratoire de bio-ingénierie. Lors d'un déplacement professionnel, il se connecte au wifi gratuit de l'aéroport pour vérifier ses emails avec sa tablette. 6 mois plus tard, un laboratoire étranger brevète le système sur lequel il travaillait depuis 3 ans.

WIFI À DOMICILE

Lors de l'installation de votre wifi à domicile, pour plus de sécurité choisissez toujours le protocole WPA2/AES. Puis sur le routeur, ne laissez pas l'accès administrateur donné par défaut (souvent « admin » avec le mot de passe « admin ») et protégez ce compte par un mot de passe robuste de plus de 12 caractères.

EPFL ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE

COPYRIGHT & TÉLÉCHARGEMENT



Le respect de la propriété intellectuelle tient une place importante au sein des valeurs fondamentales de l'EPFL. En reconnaissant les droits de tiers, l'EPFL contribue à protéger ce qu'elle produit au travers de ses contributeurs, à savoir ses chercheurs, ses étudiants et ses employés.

Arthur, doctorant dans un laboratoire, décide d'utiliser le logiciel Easydrag&Drop pour ses recherches. Il trouve une licence piratée sur Internet et l'installe sur son poste de travail. L'éditeur repère la version illicite et décide de bloquer toutes les licences de l'EPFL tant qu'Athur n'a pas payé la version piratée.

DÉFINITION

Beaucoup considèrent la copie d'un logiciel, d'un film ou d'une œuvre musicale comme un geste innocent et sans conséquences. Il n'en est rien. Tout acte de piratage engage pleinement la responsabilité individuelle de son auteur qui peut être amené à en répondre devant la justice.

CE QUE VOUS RISQUEZ

En cas d'utilisation de l'infrastructure de l'EPFL pour des actes de piratage, les auteurs transgressent non seulement des lois suisses et/ou étrangères, mais aussi des directives internes, et portent atteinte à l'image de l'Ecole et aux droits patrimoniaux de tiers. Nous tenons à vous rappeler que l'EPFL ne tolère aucun acte de la sorte et est en droit d'engager des poursuites à l'égard des contrevenants.

ATTENTION

Sont concernés : films, images, photos, icônes, musique, logiciels, systèmes d'exploitation, livres numériques et tous contenus protégés par des droits d'auteurs.

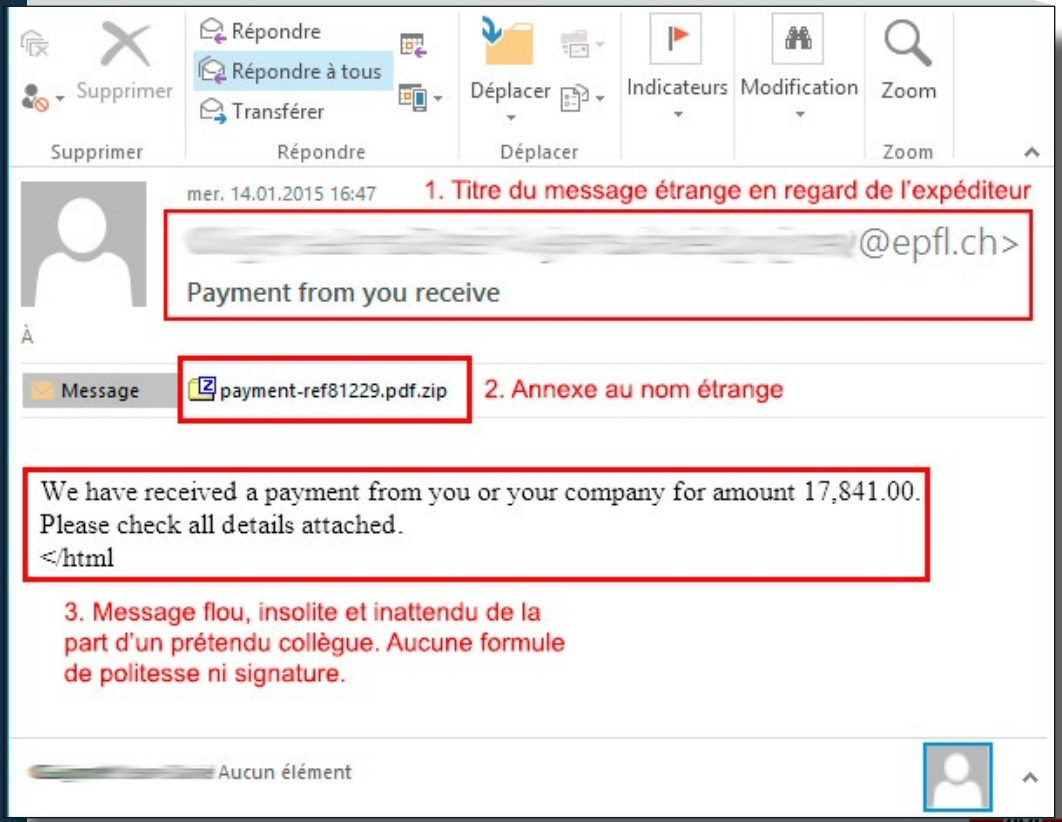
ATTENTION À MA BOITE MAIL

COURRIELS MALVEILLANTS

Il s'agit d'un message électronique dont le contenu (une annexe ou un lien dans son corps) a été pensé pour piéger le destinataire et profiter des ressources de son système d'information. On pense ici en priorité aux chevaux de Troie, dont le but est d'exploiter les ressources de la machine (connexion réseau et données qui y sont stockées) à des fins malhonnêtes et aux sites de phishing, destinés à dérober les identifiants personnels des utilisateurs par le biais d'une page qu'ils hébergent.

Des hackers se sont renseignés pendant plusieurs mois sur un ou plusieurs salariés de TV5 Monde. Ils ont simplement utilisé Google, les réseaux sociaux et d'autres moyens "artisanaux" comme le ciblage de comptes Skype afin de se renseigner sur leur cible.

Ils ont ensuite envoyé à leurs cibles un mail plus vrai que nature, les invitant à télécharger un fichier joint, en réalité un cheval de Troie. Une fois les postes infectés, par exemple celui du community manager, les pirates ont pu installer des keyloggers et des malwares. Ils ont ainsi récupéré les identifiants et mots de passe nécessaires à la prise de contrôle des réseaux sociaux de TV5 Monde.



PHISHING ATTENTION À MA BOITE MAIL

LES RISQUES

Le hacker peut utiliser votre boite email, usurper votre identité et avoir accès à toutes vos données. Il peut revendre ces informations ou les utiliser pour pénétrer le système IT de l'EPFL et y insérer un virus. L'impact financier est difficilement chiffrable en raison de l'énorme diversité des attaques.

ALORS QUE FAIRE ?

Effacez immédiatement ce genre d'email douteux et n'ouvrez surtout pas leur pièce-jointe ou lien inséré dans le corps du message.

Dans le doute, contactez le Service Desk de la VPSI au 1234 ou 1234@epfl.ch

LES SIGNES DISTINCTIFS

URGENCE DES DÉMARCHES À ENTREPRENDRE

et/ou sur risque de perdre des données ou des courriels si vous n'agissez pas rapidement.

SIGNATURE DU COURRIEL GÉNÉRIQUE ET IMPERSONNELLE

Toutes les communications officielles de la VPSI sont signées par l'un de ses collaborateurs, qui se tient à votre disposition par téléphone pour vous confirmer la légitimité du message.

COMMUNICATIONS OFFICIELLES BILINGUES

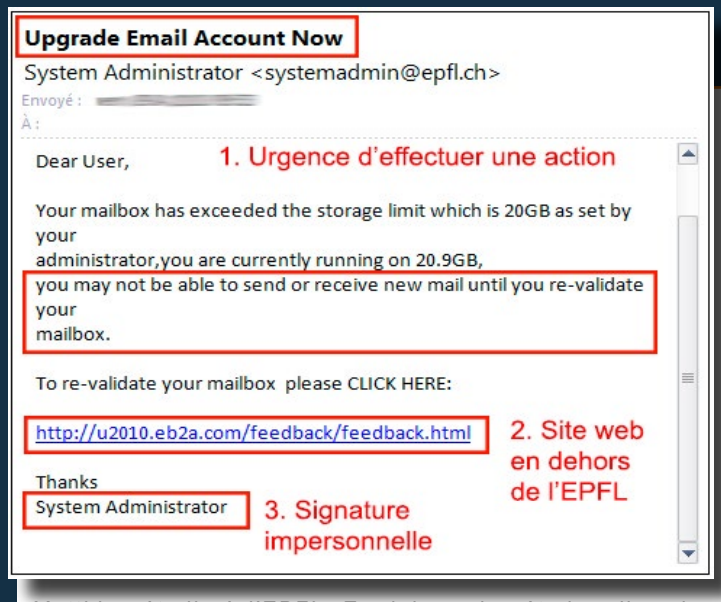
Dans la mesure du possible, tous les emails officiels sont rédigées dans les deux langues utilisées à l'école (français et anglais).

FAUTES D'ORTHOGRAPHES FRÉQUENTES

et/ou grammaire grossières et construction des phrases approximative, genre google translate.

LIEN HORS EPFL

Finalement, dans le cas où l'on vous demanderait de transmettre vos identifiants par le biais d'une page web, on constate que cette dernière n'est pas hébergée à l'EPFL (l'adresse du site ne se termine pas par .epfl.ch)



Matthieu étudie à l'EPFL. En dehors des études, il a plusieurs petits boulots, dont un dans une cafétéria de l'EPFL. Un matin, il reçoit un email d'un des restaurants de l'école qui lui annonce avoir oublié de le payer la somme de CHF 117.-. Il n'a qu'à cliquer sur un lien et se connecter pour que le transfert ait lieu. La page vers laquelle il est redirigé ressemble à s'y méprendre à la page de login de l'EPFL. Il s'identifie. Ses données personnelles sont copiées par le hacker.

HOAX CANULARS
ATTENTION À MA BOITE MAIL

Un Hoax est un courrier propageant essentiellement une information fausse et souvent invérifiable. Il peut contenir des alertes à des faux virus, une chaîne de solidarité ou une offre exceptionnelle(ment fausse). Par définition, un hoax ne représente pas un danger pour votre ordinateur, vos finances ou votre destin.
Les risques des canulars de l'Internet résident ailleurs mais sont néanmoins réels.

LES RISQUES

DÉSINFORMATION
les personnes vont y croire et donc le diffuser la rumeur qui va avec.

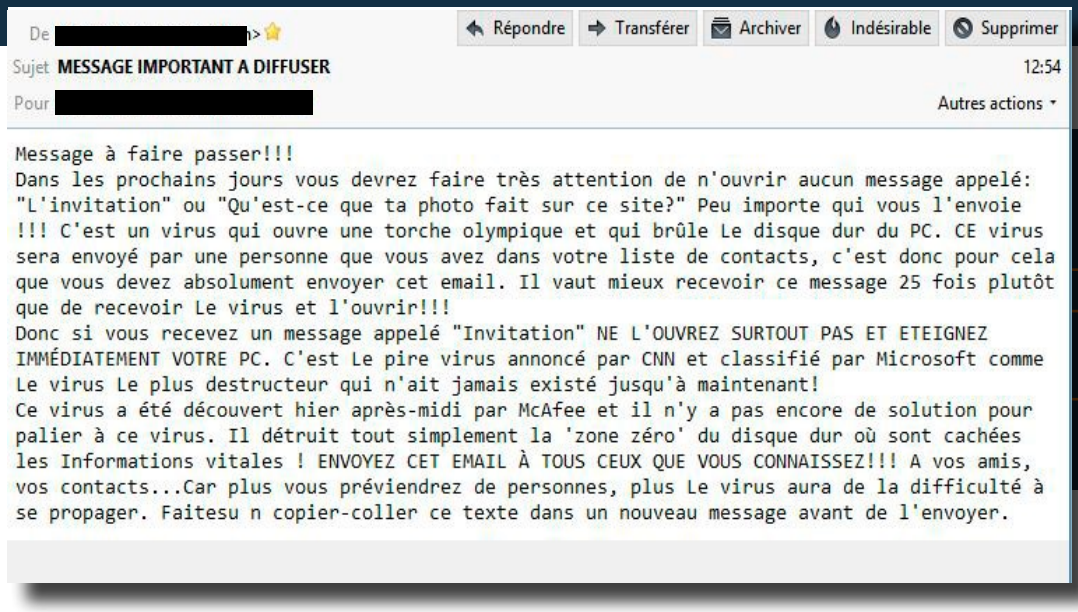
REMPLISSAGE INUTILE DES BOÎTES MAILS

ENGORGEMENT DU RÉSEAU
au même titre que le pourriel (spam) avec du trafic inutile.

ATTEINTE À L'IMAGE
Que penseriez-vous si vous étiez le sujet du hoax ?

FAUSSE ALERTE
Et à force de crier au loup…

NUIRE AUX INTERNAUTES
Faire croire qu'un fichier système contient un virus et conseiller aux internautes de le supprimer.



OÙ SE RENSEIGNER ?

1234@epfl.ch

Hoaxbuster
www.hoaxbuster.com

HoaxKiller
www.hoaxkiller.fr

POURRIELS SPAM
ATTENTION À MA BOITE MAIL

Bien que très répandus et déjà fort médiatisés, les spams deviennent toujours plus performants. Leur but ? Vous vendre tout et n'importe quoi: médicaments, diplômes, crédits, logiciels informatiques ou encore des astuces pour vous faire gagner de l'argent sans effort.

Une fois que votre adresse e-mail se balade sur le net, il n'est plus possible d'empêcher son utilisation. Par contre, voici quelques conseils pour minimiser les risques de spamming.

N'ACHETEZ JAMAIS CE QUI VOUS EST PROPOSÉ

Le simple fait qu'il y ait un infime pourcentage de personnes qui y répondent fait que c'est rentable pour les spammeurs. Si personne n'y répond, cela sera moins rentable poux eux, et ils seront moins incités à envoyer du spam.

N'ESSAYEZ JAMAIS DE VOUS DÉSINSCRIRE

La plupart du temps, cela ne fera que confirmer au spammeur que votre adresse email est valide, et qu'il y a bien un humain derrière qui lit ses mails. Votre adresse email prend alors immédiatement de la valeur à leurs yeux.

NE LAISSEZ JAMAIS VOTRE ADRESSE EMAIL SUR LES FORUMS

Il existe des robots qui parcourent automatiquement les sites web et collectent des adresses email pour les spammer.

METTEZ À JOUR VOTRE LOGICIEL D'EMAIL

Chaque logiciel qui n'est pas à jour offre une opportunité aux spammeurs, même les moins expérimentés. Ne jouez pas avec le feu!

Si vous possédez un site internet ou un blog,

N'Y LAISSEZ PAS VOTRE ADRESSE EMAIL

sous forme de texte. Mettez la uniquement sous forme d'image, cela empêchera les robots qui scannent la toile de la trouver.

NE JAMAIS RELAYER UN HOAX

invitant l'utilisateur à transmettre le courrier au maximum de contacts possible. De telles listes sont effectivement des aubaines pour les collecteurs d'adresses.

CRÉER UNE OU PLUSIEURS « ADRESSES-JETABLES »

servant uniquement à s'inscrire ou s'identifier sur les sites jugés non dignes de confiance.

COOKIES LA JUNGLE DU WEB

INTERNET SANS PEUR ET SANS REPROCHE

LES COOKIES

Comme des petites miettes, les cookies sont des petits fichiers placés dans votre navigateur par certains sites pour analyser vos pérégrinations virtuelles.

☆

RISQUES & IMPACTS

Ils peuvent être utiles (enregistrement d'adresses URL de sites déjà visités), mais également discutables car permettent de vous suivre à la trace et établir votre profil.

☆

ALORS QUE FAIRE ?

N'oubliez pas d'effacer régulièrement ces cookies (options de votre navigateur).

INTERNET SANS PEUR ET SANS REPROCHE

Voici quelques conseils de sécurité pour surfer sans se faire croquer les données :

Maintenez à jour votre système d'exploitation ainsi que toutes les applications web. En d'autres mots, faites les mises à jour lorsque le système vous l'indique.

☆

Utilisez des mots de passe sûrs et différents pour chaque site internet.

☆

Tenez compte des avertissements de votre navigateur.

☆

Méfiez-vous des sources de téléchargements douteuses. Installez l'antivirus officiel de l'Ecole et ne le désactivez pas.

EPFL ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE

LA JUNGLE DU WEB

SITES PROTÉGÉS
CONNEXION CHIFFRÉE
USURPATION D'IDENTITÉ

1 1 0 1
0 0 1 1
1 0 0 1
1 1 1 0 1 0 0

SITES PROTÉGÉS
CONNEXION CHIFFRÉE

Vérifiez les certificats des serveurs. Les certificats numériques sont généralement utilisés lors de l'établissement d'une connexion chiffrée (https) afin que le serveur puisse prouver son identité aux clients de ses services (paiement en ligne, consultation de certaines données, etc.) et ainsi attester de sa légitimité.

☆

ALORS, QUE FAIRE ?

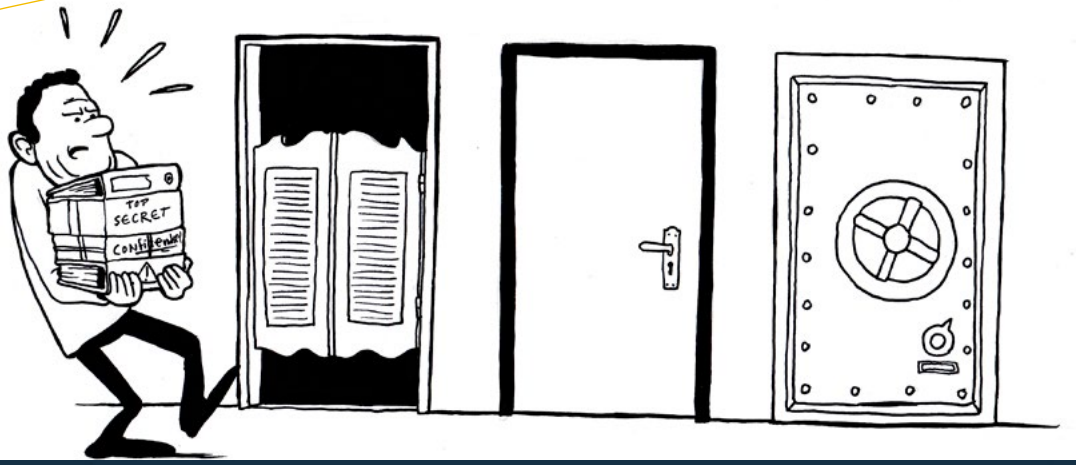
Refusez de communiquer toute donnée sensible à un site présentant un certificat erroné (vous aurez une notification de la part de votre navigateur), car il pourrait bien s'agir d'un site de phishing.

USURPATION D'IDENTITÉ

Gardez en tête que l'usurpation d'identité est une pratique courante. Il peut arriver que votre identité soit usurpée et utilisée à mauvais escient pour envoyer du SPAM, pour plaisanter ou pour nuire.

EPFL
ÉCOLE POLYTECHNIQUE
FÉDÉRALE DE LAUSANNE

CLASSER L'INFORMATION
POUR SE PROTÉGER



La classification de l'information est un procédé permettant de distribuer les informations suivant un certain nombre de degrés caractérisant leur niveau de protection souhaité. Elle permet de mettre l'accent sur la protection des informations qui ont de la valeur.

RISQUES

Une mauvaise classification de l'information facilite le travail de l'agresseur. Il y verra une porte d'entrée alléchante vers tous types d'informations sensibles et non sécurisées, comme l'état de santé d'un collaborateur, la fiche d'évaluation d'un professeur, un casier judiciaire ou des informations bancaires détaillées.

CONSEILS

- Classifier systématiquement l'information selon sa valeur.
- Adapter les mesures de sécurité de vos informations à leur classification.
- Adapter la classification au fil du temps si leur valeur a évolué.

René est étudiant en informatique. Il aide régulièrement Xavier, un ami doctorant en architecture, sur des questions informatiques.

Un soir, René est seul devant l'ordinateur de Xavier. Mû par la curiosité, il regarde les derniers documents ouverts. Ils ne sont pas protégés et font mention d'un projet de nouveau bâtiment sur le campus. Très intéressé, René envoie le tout à un ami journaliste qui s'empresse de publier l'information.

EPFL ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE

GLOSSAIRE

Cookies

Les cookies sont des petits fichiers placés dans votre navigateur par certains sites web pour éviter de devoir se reconnecter à chaque page ou pour analyser vos errances virtuelles.

Hoax (canular)

Les hoax sont de fausses annonces qui font appel au sentiment d'insécurité ou à la compassion du destinataire pour l'inciter à transmettre le message à l'ensemble de ses contacts.

Malware

Programme malveillant introduit dans un ordinateur à l'insu de son utilisateur. Cette catégorie regroupe les virus, vers, chevaux de Troie, cryptolocker, ransomware, backdoors, etc...

Phishing (hameçonnage)

Le phishing est une escroquerie où l'expéditeur se fait passer pour quelqu'un de confiance (un contact personnel, une banque, un service [at] epfl.ch) pour obtenir des données confidentielles.

SPAM (pourriels)

Les messages de type SPAM sont des messages non sollicités qui visent à arnaquer l'utilisateur, l'inciter à cliquer sur un lien publicitaire ou encore à surcharger les infrastructures informatiques.

HELP !!

En cas de doute, de problème ou de question, n'hésitez surtout pas à contacter le Service Desk de la VPSI

021 693 1234
1234@EPFL.CH

POLYLEX

Comme nul n'est sensé ignorer la loi, vous êtes vivement encouragé à consulter la Politique de sécurité des systèmes d'information en vigueur à l'EPFL (LEX 6.5.1) et la Directive pour l'utilisation de l'infrastructure électronique de l'EPFL (LEX 6.1.4) sur http://polylex.epfl.ch.

LOI SUISSE

Le Code Civil Suisse (art. 28) interdit de porter atteinte à la personnalité d'un tiers.

Le Code Pénal Suisse interdit l'atteinte à l'honneur et la diffamation (art. 173), la calomnie (art. 174), l'injure (art. 177) et la discrimination (art. 261bis).

La Loi sur la protection des données (LPD art. 12) interdit d'utiliser les données de tiers à des fins illicites ou même contre leur volonté (p.ex. s'emparer du profil d'un tiers et se faire passer pour lui).

La Loi sur les droits d'auteurs (LDA, art. 67) interdit de diffuser, de modifier et de mettre à disposition une oeuvre (p.ex. télécharger sans droit de la musique, des films, des logiciels, etc.).

La loi sur le personnel de la Confédération (LPers, art. 22) informe que le personnel est soumis au secret professionnel, au secret d'affaires et au secret de fonction.

ÉCOLE POLYTECHNIQUE
FÉDÉRALE DE LAUSANNE