Chapitre 7

Le risques sur internet

Objectifs ICT

☐	Connaître les prescriptions et normes de sécurité dans le cadre d'un comportement responsable avec les informations dans un environnement de moyens informatiques.

Au terme de ce chapitre, je suis capable …

Thème 1	
☐oui ☐non	D'expliquer aux utilisateurs les prescriptions et normes de sécurité dans le cadre d'un comportement responsable avec les informations dans un environnement de moyens informatiques.

Table des matières

1 Les Risques sur internet d'après MELANI – contremesures proposées

Quelques rares et très légères modifications ont été apportées au texte original.

1.1 Virus

[1]

Un virus se compose d'instructions programmées qui prescrivent à l'ordinateur les actions à exécuter. Afin de se propager, le virus s'installe dans un "programme hôte" qui peut être une application (p. ex. un logiciel téléchargé) ou un document (p. ex. un fichier Word ou Excel). En exécutant l'application ou en ouvrant le document, le virus est activé et exécute des actions préjudiciables. Les virus sont souvent transmis par des documents attachés aux courriels ou via des fichiers infectés téléchargés à partir d'Internet. Une fois activés, ils peuvent aussi se propager par courriel aux contacts répertoriés dans le carnet d'adresse. D'autres moyens de propagation sont des supports de données externes, p. ex. des CD-ROM, des clés mémoire USB (USB memory sticks), etc.

Conséquences et dangers

- Modification et effacement de données
- Changement affectant les contenus affichés à l'écran et apparition de messages inattendus.

Contre-mesures

- Logiciels antivirus
- Faire preuve de prudence avec le courrier électronique
- Prendre ses précautions en naviguant sur Internet

2 Vers

[1] http://www.lagedeclasse.fr/virus-informatique-a114590930

2

A l'instar des virus, les vers (worms) comportent des instructions programmées qui prescrivent à l'ordinateur les actions à exécuter. Mais à la différence des virus, les vers n'ont pas besoin d'un programme hôte pour se reproduire. Au contraire, ils utilisent les lacunes de sécurité ou des erreurs de configuration des systèmes d'exploitation ou des applications, pour se propager d'ordinateur à ordinateur. Les cibles des vers sont les ordinateurs qui présentent des lacunes de sécurité ou des erreurs de configuration et qui sont connectés d'une façon ou d'une autre (p.ex. via Internet, le réseau local, etc.) à d'autres ordinateurs.

Conséquences et dangers

- Accès non autorisé à l'ordinateur
- Effacement de données
- Espionnage de données confidentielles
- Envoi de pourriels

Contre-mesures

- Software Updates
- Logiciels antivirus
- Pare feu (Personal Firewall)
- Supprimer tout partage des espaces disques

[2] https://cosicmuhamed.wordpress.com/

2.1 Chevaux de Troie

 [3]

Les chevaux de Troie sont des programmes qui, de manière larvée, exécutent des actions préjudiciables tout en se présentant à l'utilisateur comme des applications ou des fichiers utiles. Il s'agit souvent de programmes téléchargés depuis l'Internet. Mais des chevaux de Troie peuvent aussi revêtir la forme de morceaux de musique ou de films (p. ex. dans les formats MP3 ou MPEG actuellement en vogue). Ils utilisent les lacunes de sécurité dans différents programmes de lecture (p. ex. Media Player), afin de s'installer subrepticement dans le système. Les chevaux de Troie se répandent également via les fichiers attachés aux courriels.

Conséquences et dangers

- Accès illicites aux données confidentielles (p. ex. mots de passe pour les services en ligne, codes d'accès pour l'e-banking) en enregistrant les touches activées et transmettant ces données aux assaillants (hackers).
- Accès non autorisé à l'ordinateur (p. ex. en installant ou en utilisant une porte dérobée).
- Envoi de pourriels depuis votre ordinateur.

Contre-mesures

- Logiciels antivirus
- Pare-feu (Personal Firewall)
- Faire preuve de prudence avec le courrier électronique
- Prendre ses précautions en naviguant sur l'Internet

[3] http://www.vir.us.com/removedelete-trojan-horse-dropper-generic6-aoly-from-pc-instructions

2.2 Logiciel espion et publicitaire (Spyware, adware)

[4]

Le terme de "spyware" ou logiciel espion se compose des mots anglais "spy" (espion) et "software" (logiciel). Ce programme collecte des informations, à l'insu de l'utilisateur, sur ses habitudes en matière de navigation (surf) ou sur les paramètres du système utilisé pour les transmettre à une adresse courriel prédéfinie. Le type d'informations collectées dépend du genre de logiciel espion utilisé, la palette allant des mots de passe aux habitudes de navigation.

Le terme d"adware" est issu de la contraction des mots anglais "advertising" (publicité) et "software". Il s'agit de logiciel affichant de la publicité ciblée non désirée. Il est difficile d'établir une claire séparation entre les définitions des termes spyware et adware. Les logiciels publicitaires (adware) enregistrent également souvent les habitudes de surf de l'utilisateur et les emploient pour lui offrir des produits correspondants (p. ex. via des liens). Les logiciels espions et les logiciels publicitaires sont transmis le plus souvent par des programmes téléchargés.

Conséquences et danger

- Espionnage de données confidentielles (p. ex. des mots de passe)
- Mise en danger des données privées
- Publicité non sollicitée

Contre-mesures

- Pare-feu (Personal Firewall)
- Faire preuve de prudence avec le courrier électronique
- Prendre ses précautions en naviguant sur l'Internet

[4] https://cosicmuhamed.wordpress.com/

2.3 Social Engineering

 [5]

Les attaques de social engineering (subversion psychologique) utilisent la serviabilité, la bonne foi ou l'insécurité des personnes pour accéder par exemple à des données confidentielles ou conduire la victime à exécuter certaines actions spécifiques. De tous les types d'attaques, celles-ci restent parmi les plus fructueuses. Via le social engineering, un attaquant pourra par exemple chercher à obtenir les noms d'utilisateur et les mots de passe des collaborateurs d'une entreprise, se présentant au téléphone comme l'administrateur du système ou le responsable de la sécurité. Sous prétexte de graves problèmes informatiques et en échangeant au préalable des informations sur l'entreprise (p. ex. noms des supérieurs hiérarchiques, processus, etc.) la victime est progressivement mise en confiance et enjôlée jusqu'au moment où elle livre les informations souhaitées.

Des méthodes de social engineering sont souvent utilisées pour diffuser des virus ou des chevaux de Troie, notamment lorsque le nom du document lié et contenant un virus apparaît particulièrement alléchant (p. ex. "I love you", "Anna Kournikova", etc.). Le phishing (hameçonnage) est également une forme spéciale d'attaques de social engineering.

Conséquences et danger

- Divulgation d'informations confidentielles
- Escroquerie
- Diffusion de virus et de chevaux de Troie

Contre-mesures

Attention en transmettant des informations

Ne transmettez pas, même par téléphone, des informations confidentielles (p. ex. nom d'utilisateur, mot de passe, etc.). Au cas où la personne insiste, informez votre supérieur hiérarchique, votre responsable du système ou votre fournisseur de services (p. ex. banque, fournisseur d'accès Internet, etc.). Un fournisseur de services sérieux ne vous demandera jamais votre mot de passe.

2.4 Hameçonnage (Phishing)

[5] http://www.commentcamarche.net/faq/29627-cybercriminalite-le-boom-de-l-ingenierie-sociale

[6]

Le mot phishing (hameçonnage) se compose des mots anglais "password" (mot de passe), "harvesting" (moisson) et "fishing" (pêche). Via l'hameçonnage, des pirates tentent d'accéder aux données confidentielles d'utilisateurs Internet ne se doutant de rien. Il peut s'agir p. ex. d'informations concernant les comptes pour des soumissionnaires de ventes aux enchères en ligne (p. ex. eBay) ou des données d'accès pour le e-banking. Les pirates font appel à la bonne foi, à la crédulité ou à la serviabilité de leurs victimes en leur envoyant des courriels avec des adresses d'expéditeur falsifiées. Ces courriels signalent p. ex. à la victime que les informations concernant son compte et ses données d'accès (p. ex. nom d'utilisateur et mot de passe) ne sont plus d'actualités ou ne sont plus sécurisées, les invitant à les modifier à l'aide d'un lien indiqué dans le courriel. De fait, le lien n'aboutit pas sur le site du fournisseur de services (p. ex. la banque), mais sur un site à l'identique falsifié par les pirates.

Conséquences et dangers

- Grâce aux données acquises frauduleusement, l'escroc peut effectuer des transactions bancaires au nom de l'utilisateur d'Internet, la victime, ou placer des offres dans les enchères en ligne.

Liens et téléchargements

http://www.antiphishing.org

Contre-mesures

- e-banking en toute sécurité

2.5 Lacunes de sécurité

Les programmes sont composés d'instructions qui indiquent à l'ordinateur les actions à exécuter. Il n'est pas rare que des applications comprennent des millions de lignes d'instructions. Rien d'étonnant que des erreurs puissent s'y glisser ! Presque chaque jour, des erreurs de conception ou de programmation sont découvertes et publiées. La plupart de

[6] http://hackingstuffs.com/attacks/phishing-attack/

ces erreurs n'ont pas d'influence sur la sécurité d'un système ou d'une application. Cependant, les erreurs de programmation, au niveau de la sécurité, peuvent permettre d'accéder de manière non autorisée aux données et aux systèmes. Ce sont ces erreurs que l'on appelle lacunes de sécurité ou vulnérabilités.

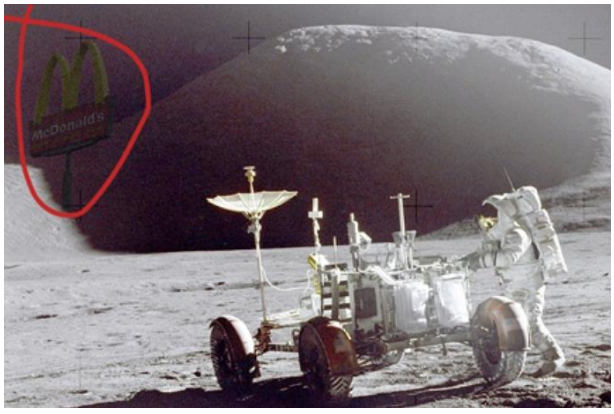
Liens et téléchargements

Informations actualisées sur les brèches de sécurité

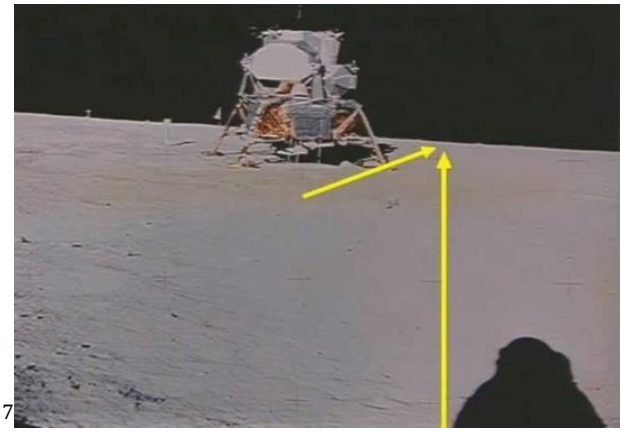
Contre-mesures

- Software Updates
- Stratégie à deux navigateurs et autres possibilités

2.6 Canulars (Hoax)



[7]


[8]

Les courriels vous annonçant de nouveaux virus particulièrement virulents sont presque toujours de fausses annonces (canulars ou hoax). Les canulars sont toujours conçus sur le même modèle. Ils signalent l'apparition d'un nouveau virus dangereux résistant même à un logiciel anti-virus récent. De plus, la source indiquée par l'annonce est une entreprise informatique renommée et il est demandé de transmettre l'annonce à autant de monde que possible.

Outre de fausses informations concernant les virus, on trouve également des annonces très diverses nous faisant compatir au triste destin de personnes malades ou proposant des offres discutables. On parle également dans ce cas de chaînes de courriels.

Conséquences et dangers

- Suivre les mesures proposées dans le canular peut entraîner la perte de données ou la mise hors usage de l'ordinateur.
- Panique potentielle et trafic de données inutile
- Surcharge de l'infrastructure nécessaire aux courriels

[7] http://www.freakingnews.com/NASA-loses-moon-landing-tape-Pictures---1115.asp
[8] http://www.dazeddigital.com/artsandculture/article/20885/1/today-marks-the-45th-anniversary-of-the-moon-landing

Liens et téléchargements

Informations sur les canulars (hoaxes)

Contre-mesures

- Consultation d'autres sources

En cas de doute, vérifiez s'il s'agit d'un canular en consultant les sites Internet des fournisseurs de logiciels anti-virus.

- Refus d'exécuter les instructions du courriel

N'exécutez en aucun cas les instructions recommandées par le canular, surtout s'il s'agit d'effacer des fichiers, d'installer un programme ou de transmettre l'information à vos connaissances.

- Expéditeur à rendre attentif au fait qu'il s'agit d'un canular

Dans le cas où vous connaîtriez l'expéditeur, signalez-lui que son courriel est un canular ou une fausse information, après avoir vérifié vous-mêmes cela.

2.7 Pourriel (spam)

9

10

La notion de pourriel (spam) englobe tous les messages électroniques indésirables et les chaînes de courriels. La personne qui envoie de tels messages est appelée polluposteur (spammer), tandis que l'on parle de pollupostage (spamming) pour l'action proprement dite. Selon plusieurs études, les pourriels représenteraient déjà plus de 60 % du courrier électronique au plan mondial et la tendance est à la hausse.

Conséquences et danger

- Perte de temps puisqu'il faut parcourir puis effacer à chaque fois ces messages.
- Très grosse charge pour l'infrastructure IT (Internet, serveur de messagerie).

[9] http://www.toonpool.com/artists/deleuran_250 http://nuriatorregrosa.blogspot.ch/2012/01/eviter-que-vos-emails-deviennent-des.html

[10] http://3.bp.blogspot.com/ selon http://nuriatorregrosa.blogspot.ch/2012/01/eviter-que-vos-emails-deviennent-des.html

Liens et téléchargements

Informations sur les pourriels (spam)

Contre-mesures

- Faire preuve de prudence avec le courrier électronique
- Pas d'adresses électroniques courtes

Les polluposteurs recourent à des programmes qui testent toutes les combinaisons possibles des adresses courtes (p. ex. xyz@yahoo.com). Le choix d'une adresse électronique plus longue garantit une certaine protection (p. ex. prénom.nom@yahoo.com).

- Filtres proposés par les programmes de messagerie

Plusieurs programmes de messagerie proposent des fonctions pour filtrer les courriels entrants.

- Filtre anti-pourriel

Pour l'usage domestique ainsi que pour les PME, des solutions ont été développées qui permettent de réduire les problèmes de pourriels. Les courriels entrants sont analysés selon certains critères (p. ex. objet, adresse de l'expéditeur, mots-clefs dans le texte du courriel, etc.) et classés soit en courriels acceptables ou soit en pourriel (mis à la poubelle). La difficulté réside dans la configuration de ces critères si bien que l'entretien d'un filtre anti-pourriel efficace peut être très fastidieux.

- Utilisation des copies aveugles lors de l'envoi d'e-mail à plusieurs destinataires

Lors de l'envoi de courriels, les adresses électroniques inscrites dans les cases "à" ("to") ou "CC" (Carbon Copy) sont accessibles à tous les destinataires. Lorsque le nombre des destinataires est important, des adresses électroniques risquent ainsi de tomber entre les mains de «spammers» (auteurs de pourriels). Quand des messages sont envoyés à de nombreux destinataires, le nom de ceux-ci devrait être inscrit dans la case correspondant aux copies aveugles "BCC" (Blind Carbon Copy). En effet, le contenu de la case BCC ne peut pas être lu par les destinataires.

2.8 Cookies

Les cookies (témoins de connexion) sont des petits fichiers texte qui s'installent sur l'ordinateur du visiteur lorsque ce dernier consulte une page Internet, ceci dans le but de lui simplifier la tâche. A titre d'exemple, il faut parfois dans certains services en ligne s'annoncer à l'aide d'un nom d'utilisateur et du mot de passe correspondant. Afin d'éviter de devoir répéter l'opération à chaque fois, ces informations sont stockées après sélection de l'option correspondante sur un témoin de connexion sur le disque dur local et réutilisées automatiquement à chaque visite du site. Les boutiques en ligne les utilisent également afin de procéder à l'enregistrement intermédiaire de la corbeille d'achat ou pour présenter des produits qui sont venus s'y ajouter depuis la dernière visite.

On différencie les témoins de connexion à durée de vie limitée (session cookies) de ceux dont cette durée est plus longue (persistent cookies). Les premiers s'effacent à la fermeture du navigateur ou au moment de quitter la page Internet correspondante. Pour les autres, la

date de péremption (du témoin) est déterminée par l'application Internet qui le crée et qui peut l'utiliser jusqu'à cette date.

Conséquences et danger

- Mise en danger de la sphère privée. Les exploitants de sites Internet peuvent à l'aide des témoins de connexion enregistrer le comportement de la personne qui visite le site pour établir son profil client.

Contre-mesures

- Restriction des témoins de connexion

Paramétrez le navigateur Internet pour faire apparaître un message lorsque des témoins de connexion s'installent ou pour laisser l'utilisateur choisir interactivement d'accepter ou de refuser le témoin de connexion. Cependant, cette manière de faire s'avère pénible dans la pratique étant donné que la plupart des sites Internet recourent aux témoins de connexion; et il devient souvent alors impossible de faire des achats en ligne.

- Acceptation de témoins de connexion uniquement pour des sites Internet spécifiés

Paramétrez le navigateur Internet de manière à n'accepter que les témoins de connexion provenant de certains sites Internet spécifiés.

- Recours à des outils

Il existe des outils qui effacent les témoins de connexion, voire les empêchent même de s'installer sur l'ordinateur.

2.9 Chat et messagerie instantanée

11

Le "chat" (bavardage en ligne) désigne un moyen de communiquer sur Internet en temps réel avec d'autres utilisateurs. Contrairement au téléphone, les discussions se font non pas

[11] http://goldstarteachers.com/live-online-chatting/

en parlant mais en écrivant. L'utilisateur peut s'entretenir simultanément avec tous les participants ou se retirer avec un seul dans un salon privé inaccessible aux autres. Différentes plates-formes de bavardage en ligne sont accessibles gratuitement sur Internet.

Un mode de communication analogue est offert par les services de messagerie instantanée (instant messaging) (p. ex. AOL, MSN, ICQ et Yahoo), auprès desquels des millions d'internautes sont enregistrés.

Conséquences et danger

- Les services de bavardage en ligne sont utilisés en raison de leur apparent anonymat également pour agir de manière illégale, p. ex. par des pédophiles à la recherche de leurs semblables ou de victimes.
- Introduction de virus, vers et chevaux de Troie sur votre propre ordinateur.
- Les participants au bavardage en ligne sont régulièrement enjoints à cliquer sur des liens ou à entrer des commandes inconnues.

Contre-mesures

- Software Updates
- Supprimer tout partage des espaces disques
- Précautions à prendre en "chattant"

De manière générale, faites particulièrement attention en utilisant le bavardage en ligne et notamment s'il faut ouvrir des fichiers ou des liens.

- Désactivation de la réception automatique des fichiers
- Aucune confidence lors du chat

Aucune donnée confidentielle (p. ex. les mots de passe) n'a sa place dans le bavardage en ligne!

2.10 Bluetooth, Handy, PDA

[12]

Les temps sont révolus où les téléphones portables ne servaient qu'à téléphoner! Actuellement, le grand nombre de fonctions (caméra intégrée, agenda, jeux, fonctions SMS et MMS, périphériques à infrarouge et Bluetooth, possibilité de surfer sur Internet), a transformé le portable en un petit appareil multifonction. Les assistants numériques personnels (PDA, Personal Digital Assistant) possèdent généralement une fonction Bluetooth. Mais plus

[12] http://findicons.com/search/bluetooth

l'offre en fonctions est grande, plus la probabilité de points faibles augmente. Et notamment la technologie Bluetooth, installée dans les portables, a déjà montré plusieurs faiblesses dans quelques téléphones de divers fabricants.

Conséquences et danger

- Risques de Bluetooth: Certaines implémentations de la technologie de Bluetooth permettent la lecture non autorisée de l'agenda, du carnet d'adresse, voire même des messages SMS enregistrés. De plus, l'activation cachée d'appels ou l'envoi de SMS ainsi que la propagation de vers affectant les téléphones portables sont possibles.
- Autres risques liés aux téléphones portables: conclusion non voulue d'abonnements (coûteux) en téléchargeant des sonneries ou des jeux. Messages SMS invitant à rappeler des numéros de téléphone à valeur ajoutée du type 0900.

Contre-mesures[13]

A - Mesures à prendre en cas d'utilisation de Bluetooth

- **N'activer le Bluetooth qu'en cas de besoin**
  N'activez Bluetooth que quand vous l'utilisez! Désactivez Bluetooth dès que vous avez fini de vous en servir.
- **Recours à Bluetooth uniquement dans un contexte sécurisé**
  N'utilisez Bluetooth que si cela est vraiment nécessaire et uniquement dans un environnement sécurisé (pas dans les lieux publics).
- **Mode "discoverable" de l'appareil Bluetooth activé uniquement si nécessaire**
- **Utiliser les options de sécurité**
  Informez-vous (en lisant le mode d'emploi ou en interrogeant votre vendeur) à propos des options de sécurité de votre appareil Bluetooth, et activez si possible l'authentification et le chiffrage.

B - Mesures à prendre en cas d'utilisation de téléphones portables

- **Mise à jour des firmware (microprogramme)**
  Comme pour les systèmes d'ordinateur, il existe aussi des mises à jour pour les portables. Celles-ci peuvent être installées chez le fabricant ou auprès d'un magasin spécialisé. Il faut s'informer régulièrement concernant les mises à jour des microprogrammes (firmware) et les installer.
- **Lecture des rubriques en petits caractères**
  Veillez en téléchargeant des jeux ou des sonneries aux éventuelles conditions d'utilisation du fournisseur de service.
- **Attention en cas de SMS envoyés par des inconnus**
  Evitez de répondre aux SMS envoyés par des personnes inconnues.

[13] http://www.melani.admin.ch/themen/00166/00195/index.html?lang=fr

2.11 Wireless LAN

14

15

Un WLAN (Wireless Local Area Network) est un réseau local sans fil. Dans un tel réseau, les terminaux (p. ex. ordinateurs portables, agendas électroniques (PDA), etc.) communiquent sans fil avec un point d'accès WLAN (WLAN Access Point), relié à Internet ou à un réseau local. L'avantage du WLAN est que ses utilisateurs sont davantage mobiles étant donné que leurs terminaux ne sont pas câblés. Dans les bâtiments, la portée dépend du type de construction et est nettement plus réduite qu'à l'extérieur où une connexion WLAN est possible à plus de 200 m.

Conséquences et danger

- Une configuration irréfléchie du point d'accès WLAN entraîne un accès total au réseau local. Il devient alors possible d'accéder aux ordinateurs et aux données ainsi que de pirater les raccordements à Internet.
- Un cryptage insuffisant des connexions WLAN permet à des tiers de lire des données en recourant à des moyens techniques relativement simples.

Contre-mesures[16]

- **Protection de la page administration**
  La plupart des points d'accès WLAN disposent pour l'administration d'une interface utilisateur accessible avec un navigateur (par une adresse de forme suivante : http://ADRESSE_IP_DU_POINT_D'ACCES). Cette interface permet les configurations ci-après. La page administration est protégée par un mot de passe standard, qu'il faut modifier immédiatement. Modifiez l'identification du réseau (SSID) attribuée de manière standard.
- **Bloquer l'envoi de l'identification du réseau**
  Empêchez que le point d'accès envoie régulièrement son identification de réseau (SSID) en configurant l'option "Broadcast SSID" sur "Non".
- **Restriction d'accès aux terminaux**
  Limitez l'accès à votre point d'accès WLAN afin que seuls vos terminaux puissent communiquer avec lui, en saisissant chacune de leur adresse MAC.

[14] http://findicons.com/search/wlan
[15] http://www.zeit.de/digital/internet/2010-05/wlan-bgh-unterlassung
[16] http://www.melani.admin.ch/themen/00166/00196/index.html?lang=fr

- **Enclencher le cryptage**
  Activez le cryptage WPA ou WPA2 de votre matériel WLAN en choisissant un mot de passe «fort», c'est-à-dire difficile à deviner (voir «Règles de comportement»). Si votre matériel WLAN ne soutient pas encore le protocole WPA ou WPA2, activez le cryptage WEP. La clé WEP (de la longueur de votre choix, si possible de 128 Bit) doit être connue aussi bien du point d'accès que du terminal.
- **Recours à des protocoles sûrs**
  Pour transmettre des données confidentielles via le WLAN, il est recommandé de recourir à des protocoles qui cryptent les données à envoyer (p. ex. VPN, https, ssh, etc.).

2.12 Intermédiaires online pour prestations financières

À l'étranger et toujours plus en Suisse également, les entreprises qui œuvrent en tant qu'intermédiaires lors de prestations financières en ligne, telles que des paiements et des informations sur un compte, ont une popularité toujours croissante. Certaines bénéficient d'un label émis par l'Etat, ce qui devrait garantir une certaine sécurité.

Les utilisateurs doivent normalement fournir à ces agents financiers les codes d'identification afin d'accéder au compte bancaire (nom d'utilisateur, mot de passe et chiffre d'une liste à biffer ou autre). Des données utilisées ensuite par ces sociétés pour effectuer les paiements ou accéder à des informations sur les comptes ou les paiements au nom de leurs clients.

MELANI émet généralement des réserves sur le fait de fournir de telles données sensibles à des tiers. Cela pourrait en effet se traduire par un enrichissement illégitime d'autrui. Il y a aussi le danger que des tiers puissent recueillir des informations sur les transactions et l'état de votre compte. Certaines banques suisses refusent déjà les paiements ou demandes d'informations effectuées par ces intermédiaires; si vous souhaitez recourir à de tels services, veuillez vous assurer que votre institut les autorise.

Contre-mesures

Vous retrouverez d'autres informations utiles, ainsi qu'un mode d'emploi pour un e-banking sans risques, dans la rubrique «Services ».

3 Protection d'après MELANI

3.1 Logiciels antivirus

Les logiciels antivirus protègent vos données contre les virus, les vers et les chevaux de Troie.

- Installer un logiciel antivirus
- Actualiser régulièrement votre logiciel antivirus
- Vérifier la validité de la licence

3.2 Faire preuve de prudence avec le courrier électronique

Virus, vers et chevaux de Troie

- Prudence avec le courrier électronique dont l'expéditeur est inconnu

Méfiez-vous du courrier électronique dont l'adresse d'expédition vous est inconnue. Dans un tel cas, n'ouvrez aucun document ou programme joint et ne sélectionnez aucun des liens y figurant.

- S'assurer de la fiabilité des sources

  N'ouvrez que des fichiers ou des programmes provenant de sources dignes de confiance et ne le faites qu'après les avoir vérifiez avec un logiciel antivirus actualisé.

- Prudence avec les noms de fichiers à deux extensions

  N'ouvrez aucune annexe de courrier électronique à deux extensions (p. ex. picture.bmp.vbs). Ne vous laissez pas tromper par l'icône d'un tel fichier. Dans Explorer, à la rubrique Paramètres du Panneau de configuration à Options des dossiers à Affichage, désactivez l'option "Cacher les extensions des fichiers dont le type est connu.

- Mise à jour du programme de courrier électronique

  Les programmes de courrier électronique peuvent aussi présenter des lacunes de sécurité. Vérifiez régulièrement l'existence de mises à jour pour ce programme et installez-la.

Pourriel (spam)

- Ne pas donner son adresse e-mail à toute occasion

  Communiquez votre adresse électronique à un minimum strict de personnes et utilisez-la exclusivement pour la correspondance importante.

- Se doter d'une deuxième adresse e-mail

  Il est indiqué d'utiliser une deuxième adresse e-mail pour remplir des formulaires sur la Toile, s'abonner à des bulletins, écrire dans des livres d'hôte, etc.

  Il est possible d'en obtenir une gratuitement auprès de divers fournisseurs. Si du pourriel est distribué à cette adresse, on peut la supprimer ou en définir une nouvelle.

- Ne pas répondre aux pourriels

  Si vous répondez aux pourriels, l'expéditeur saura que votre adresse électronique est valable et continuera d'expédier du courrier non sollicité. Prudence aussi avec le pourriel offrant une "option de désabonnement". On vous promet de vous tracer de la liste des destinataires si vous envoyez un courrier électronique d'une certaine teneur. On se montrera tout aussi prudent à l'égard des réponses automatiques en cas d'absence du bureau. Elles devraient être uniquement renvoyées aux expéditeurs connus.

Canulars (hoaxes)

- Les virus ne sont pas annoncés par courrier électronique

  Les alertes expédiées par courrier électronique relatives à des virus sont le plus souvent des canulars (hoaxes). Ne suivez en aucun cas les recommandations formulées. Cela concerne surtout la suppression de fichiers, l'installation d'un programme cité

ou la transmission de l'avis à des connaissances. En cas de doute, consultez les pages Web des fabricants de logiciel antivirus.

- Prudence avec les lettres en chaîne

  Ce qui vaut pour les canulars, vaut par analogie pour les chaînes de courriels retraçant le destin d'une personne ou vous promettant des offres lucratives.

3.3 Prendre ses précautions en naviguant sur l'Internet

La navigation sur la Toile expose aussi à des dangers susceptibles d'avoir une influence sur la sécurité de vos données et de votre ordinateur. Quelques-uns d'entre eux, et les mesures de protection adaptées, font l'objet de la liste suivante :

Virus, vers, chevaux de Troie, logiciel espion

- **Ne pas télécharger de programme inconnu**

Ne téléchargez aucun programme inconnu (jeux, économiseurs d'écran, etc.) depuis l'Internet. Cliquez sur "Interrompre" ou sur "non" lorsqu'une fenêtre de téléchargement s'affiche sans que vous ne l'ayez voulu.

- **Se procurer les mises à jour auprès du fabricant seulement**

Téléchargez les mises à jour ou les pilotes exclusivement sur les sites Web du fabricant concerné. Vérifiez-les ensuite au moyen d'un logiciel antivirus actualisé.

Social Engineering, hameçonnage (phishing), escroquerie

- Prudence en cas de transmission d'informations

  Ne donnez à personne votre nom d'utilisateur ou votre mot de passe. Aucun fournisseur sérieux ne vous demandera votre mot de passe (même par téléphone). Cette remarque vaut également lorsque la demande paraît crédible et comporte des caractéristiques d'identification évidentes du fournisseur (p. ex. adresse électronique, site Internet, etc.). En cas de doute, ne répondez pas et posez la question à votre fournisseur

- S'enquérir du sérieux du fournisseur

  Lors d'achats en ligne, il faut veiller à ne traiter qu'avec les fournisseurs sérieux. N'entrez votre numéro de carte de crédit que sur des pages Web utilisant un protocole sécurisé. On les reconnaît à la petite clé dorée s'affichant sur le bord inférieur gauche du navigateur ou au protocole indiqué dans l'URL (https au lieu de http).

- Prendre congé en bonne et due forme

  Utilisez toujours la déconnexion prévue pour quitter les applications Web (p. ex. Webmail, transactions bancaires).

Protection des données

- Etre sur ses gardes quand on remplit des formulaires web

  Évitez de disséminer des données personnelles. Cela concerne spécialement le remplissage de formulaires sur le Web.

- Prudence en rédigeant des textes dans les forums de discussion

Pensez que ce que vous écrivez dans le cadre de groupes de discussion ou de forums, ou encore dans des livres d'hôte, reste accessible encore pendant des années.

Configuration du navigateur

Chaque page Web est composée des instructions écrites en code HTML. Ces instructions indiquent au navigateur (Internet Explorer p. ex.) comment représenter le contenu du site sur l'écran du client. Certains sites du Web ne comprennent que des documents sans fonctions additionnelles (ce sont des pages statiques). D'autres proposent des contenus dynamiques. Citons pour exemple les textes défilants, les formulaires électroniques pour des achats en ligne, des images animées ou des bannières publicitaires dynamiques. Ces fonctions dynamiques peuvent être implémentées à l'aide d'ActiveX Controls ou de JavaScript. Ceux-ci peuvent malheureusement être détournés pour définir et exécuter des actions indésirables ou nocives pour l'ordinateur client.

- Brider JavaScript

  Tentez de limiter le plus possible (ou même désactiver), via la configuration (menu "Outils" - "Options Internet") de votre navigateur, l'exécution des JavaScripts (Active Scripting). Il faut cependant savoir que si JavaScript est désactivé, le contenu de nombreux sites Internet ne s'affiche plus correctement. Si cela devait entraver trop fortement votre navigation, relâcher les restrictions (graduellement) jusqu'à obtenir une navigation satisfaisante (c-à-d. l'affichage normal des informations qui vous intéressent).

- Limiter ActiveX Controls (Internet Explorer seulement)

  Tentez de limiter le plus possible, via la configuration de votre navigateur, l'exécution d'ActiveX Controls.

  Réglage des paramètres de sécurité d'Internet Explorer sur «Elevé»

  Changez les paramètres de sécurité d'Internet Explorer en les réglant sur «Elevé». A cet effet, des explications détaillées figurent aux pages 5 et 6 des «Paramètres de sécurité de Windows XP» (ces instructions valent également pour les autres systèmes d'exploitation de Windows).

  Important: Ces réglages ne permettront plus d'accéder normalement aux nombreux sites Internet recourant à la technique Active Scripting. Il est donc recommandé d'accepter sur la liste des «sites de confiance» les sites régulièrement visités (auxquels vous faites confiance). Les instructions à ce sujet figurent également dans le document «Paramètres de sécurité de Windows XP», à la page 6.

3.4 Software Updates

- Mettre régulièrement à jour système d'exploitation et les applications

  Quelques produits proposent une fonction de mise à jour automatique ; faites-en impérativement usage. Vérifiez régulièrement si elle est toujours activée. Pour cela, consultez les informations actuelles sur les mises à jour sur le site Internet du fabricant concerné.

- Suivre les informations relatives aux mises à jour des logiciels

  D'autres organes informent régulièrement sur les nouveaux trous de sécurité, vulnérabilités et des mises à jour pertinentes (et d'autres mesures).

3.5 Pare-feu personnel

- Recourir à un pare-feu personnel

  Comme les programmes antivirus, les pare-feu personnels sont disponibles sous forme de logiciels additionnels et certains peuvent être téléchargés gratuitement depuis l'Internet. Quelques systèmes d'exploitation (comme Windows XP, Mac OS X ou Linux) sont déjà équipés d'un pare-feu personnel.

- Installer le pare-feu avant la connexion Internet

  Si votre ordinateur est équipé d'un pare-feu personnel, activez-le impérativement avant de connecter votre ordinateur (pour la première fois) à l'Internet. Il ne faudrait procéder au téléchargement de mises à jour de logiciels, d'autres programmes et fichiers que lorsque le pare-feu personnel est activé.

3.6 Configuration du système

- Mot de passe fort

  Choisissez un mot de passe fort pour chaque compte utilisateur existant.

- Supprimer tout partage des espaces disques

  Vérifiez qu'aucune modalité de partage (Windows shares) ne soit installée sur votre ordinateur. Les partages permettent sur un système Windows de mettre à disposition d'autres utilisateurs via le réseau des fichiers, voire tous les disques. Les partages représentent non seulement des points d'attaque pour les virus et les vers mais peuvent également rendre accessibles vos données (même confidentielles) à un large cercle d'utilisateurs (dans le pire des cas à tous les internautes).

3.7 Informations actualisées sur les brèches de sécurité

www.cert.ssi.gouv.fr

http://www.cert-ist.com

www.cases.public.lu

http://www.heise.de/security (allemand)

http://www.buerger-cert.de (allemand)

http://www.kb.cert.org/vuls (anglais)

http://www.first.org (anglais)

3.8 Stratégie à deux navigateurs et autres possibilités

Il est aujourd'hui généralement d'usage d'installer régulièrement, de préférence automatiquement, les mises à jour de sécurité des systèmes d'exploitation et des applications. On rencontre néanmoins régulièrement des failles «zero day», soit des lacunes pour lesquelles il n'existe pas encore de mise à jour de sécurité. Presque tous les jours, de telles failles de sécurité sont identifiées dans toutes sortes d'applications. Les navigateurs Internet ne font pas exception à la règle. Selon la gravité de la vulnérabilité découverte, il peut être judicieux de changer de navigateur jusqu'à ce que le fabricant ait résolu le problème.

Ce qui n'est qu'une simple formalité pour un ordinateur privé peut s'avérer un vrai casse-tête dans le monde professionnel. Car à la différence des ordinateurs privés, il est souvent délicat pour une entreprise de changer de navigateur. Par exemple faute d'avoir prévu une stratégie à deux navigateurs. Cela est fréquemment le cas, afin que le service chargé des TIC ne doive assumer la maintenance que d'un seul navigateur.

En cas de grave faille de sécurité, des données confidentielles voire secrètes risquent aussi d'être menacées. Il est par conséquent judicieux de parer à toute éventualité, dans la vie privée comme dans le cadre professionnel, afin de pouvoir au plus vite se rabattre sur un navigateur de rechange.

Les possibilités suivantes seraient envisageables dans le monde professionnel (l'énumération n'étant pas exhaustive):

- Equipement de tous les postes avec au moins deux navigateurs

  Tous les postes de travail d'une entreprise comportent au moins deux navigateurs. En cas de nécessité, le personnel sera prié de ne plus utiliser le navigateur problématique jusqu'à nouvel avis. Il serait également possible, le cas échéant, d'agir directement via le serveur mandataire (proxy), en empêchant ce navigateur d'accéder à Internet. Mais une telle solution serait coûteuse, en obligeant à assurer la maintenance de plusieurs navigateurs. Quant aux utilisateurs, ils hésiteraient souvent sur le navigateur à utiliser.

- Equipement ponctuel d'au moins deux navigateurs

  Seuls les postes de travail ayant impérativement besoin d'Internet seront équipés de plusieurs navigateurs. A supposer que l'un d'eux présente une faille de sécurité, il ne sera plus utilisable et il faudra en changer. Le grave inconvénient de cette solution tient à ce qu'en cas d'urgence, une partie du personnel serait momentanément privée d'accès à Internet. Même si cela ne joue peut-être pas un rôle important pour leur travail, les utilisateurs concernés risquent de se sentir infantilisés ou discriminés.

- Liste blanche

  Tous les départements de l'entreprise signalent au service TIC les URL dont ils ont absolument besoin même en cas d'urgence. Les liens correspondants seront inscrits sur une liste blanche.

  En cas de faille de sécurité, tous les URL absents de cette liste seront bloqués. Une telle mesure permettrait de faire l'économie d'un second navigateur. Le risque de dommages sera réduit au minimum, puisque seuls des URL bien précis resteront accessibles. Tout risque n'est pas pour autant écarté. D'où la nécessité d'installer au plus vite les mises à jour de sécurité, afin de pouvoir renoncer au blocage temporaire des URL absents de la liste blanche.

3.9 Informations sur les canulars (hoaxes)

http://www.sophos.fr/virusinfo/hoaxes (anglais)

http://www.f-secure.com/virus-info/hoax (anglais)

http://hoax-info.tubit.tu-berlin.de/hoax/ (allemand)

www.hoaxbuster.com

3.10 E-banking en toute sécurité

Les escroqueries signalées contre les internautes inquiètent toujours plus les usagers des services de e-banking. Or le trafic électronique des paiements par Internet est tout à fait sûr, à condition de respecter certaines règles.

Liste de contrôle "e-banking en toute sécurité"

Liste de contrôle avec instructions "e-banking en toute sécurité"

En complément, nous mettons à votre disposition l'aide-mémoire sur la sécurité dans le trafic des paiements publié par l'Association suisse des banquiers.

Sécurité du trafic des paiements

3.11 Informations sur les pourriels (spam)

http://www.bakom.admin.ch/dienstleistungen/info/00542/00886/

http://www.spamfighter.com/Lang_Other/Default_FR.asp

www.cloudmark.com/ (anglais)

Services de messagerie gratuits :

http://www.yahoo.com/

www.hotmail.com

http://www.gmx.ch

https://gmail.com

3.12 Listes de contrôle et instructions

Les documents suivants sont autant d'aides concrètes pour utiliser en toute sécurité les nouvelles technologies de l'information et de la communication.[17] (disponibles sur Melanie) :

Sécurité informatique: aide-mémoire pour les PME

Instructions relatives à la suppression des maliciels sur les sites Internet

Instructions relatives à la suppression des maliciels

Mesures de prévention pour les systèmes de gestion de contenu (CMS)

Mesures de protection des systèmes de contrôle industriels (SCI)

[17] http://www.melani.admin.ch/dienstleistungen/00132/index.html?lang=fr

4 D'autre types d'attaque

L'arsenal des hackers n'en finit pas de s'élargir… Voici quelques types d'attaques supplémentaires.

4.1 Les rogues

[18]

Les rogues sont des faux logiciels de sécurité. En octobre 2009, apparait le rogue Security Tool, un faux logiciel anti-spyware. Il s'installe sans permission et vous incite, par le biais d'un message alarmant, à acheter et installer un logiciel "frauduleux" pour soit disant désinfecter votre ordinateur. A ne pas faire ! (Assistance Orange) [19]

4.2 Les RansomWare

[20]

D'après Wikipedia :[21]

[18] http://www.repairwin.com/mr-pc-cleaner-rogue-program-removal-guide/
[19] http://assistance.orange.fr/virus-ver-cheval-de-troie-les-differencier-878.php
[20] http://www.malekal.com/wp-content/uploads/Ransomware_sur_votre_ordinateur_est_infecte.jpeg
[21] http://fr.wikipedia.org/wiki/Ransomware

Un ransomware, ou rançongiciel, est un logiciel malveillant qui prend en otage des données personnelles. Pour ce faire, [il] chiffre des données personnelles puis demande à leur propriétaire d'envoyer de l'argent en échange de la clé qui permettra de les déchiffrer.

Un ransomware peut aussi bloquer l'accès de tout utilisateur à une machine jusqu'à ce qu'une clé ou un outil de débridage soit envoyé à la victime en échange d'une somme d'argent. Les modèles modernes de rançongiciels sont apparus en Russie initialement, mais on constate que le nombre d'attaques de ce type a grandement augmenté dans d'autres pays, entre autres l'Australie, l'Allemagne, les États-Unis. …

En novembre 2012, « McAfee, l'éditeur de logiciels de sécurité, rapporte avoir enregistré 120 000 nouveaux échantillons de ce genre de virus au deuxième trimestre 2012, soit quatre fois plus qu'à la même période l'année d'avant. »[22]

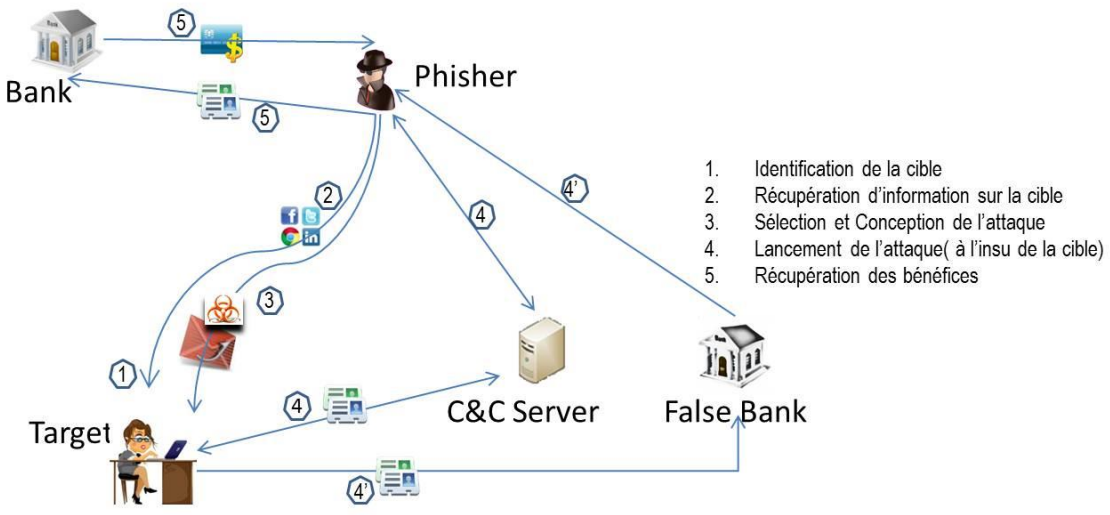
Le premier rançongiciel référencé datait de 1989 : "PC Cyborg" Trojan(en), codé par Joseph Popp, qui possédait une payload qui avertissait l'utilisateur qu'une certaine licence d'un certain logiciel aurait expiré, en chiffrant des fichiers sur le disque dur, et en demandant à l'utilisateur de payer 189$ à la société "PC Cyborg Corporation" pour déverrouiller le système. (Wikipédia).

Ces « virus-rançon » sont en fait des **cryptovirus**.

4.3 Le Spear phishing

Variante plus subtile du phishing, le spear-phishing (de « to spear » = harponner) vise une ou quelques cibles méticuleusement choisies pour exfiltrer des données sensibles. Cette technique utilise un collecte d'information préalable, puis un email personnalisé et soigneusement rédigé qui comporte une pièce jointe avec une extension trompeuse ou un lien.

Lire la description dans l'article http://blog.conixsecurity.fr/?p=1069.



[22] http://www.slate.fr/story/63737/virus-rancon-hackers-chantage

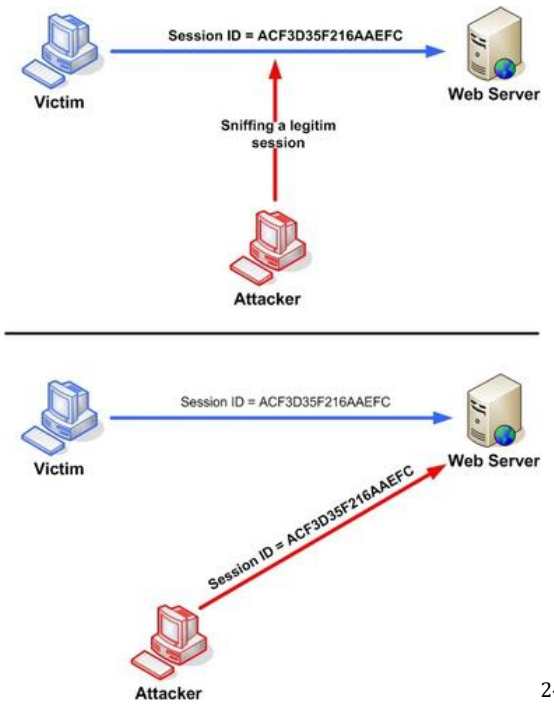
Contre-mesures (selon http://blog.conixsecurity.fr/?p=1069):

- S'assurer de la fiabilité de l'expéditeur : analyser scrupuleusement (au caractère près !) l'adresse email de l'expéditeur et notamment le nom de domaine indiqué après le « @ ».
- Ne pas cliquer sur des pièces jointes ou des liens avant d'être convaincu de l'authenticité de l'expéditeur.
- S'assurer de la pertinence de la destination des hyperliens : lorsqu'un mail contient un ou plusieurs liens, prendre connaissance de l'adresse Internet vers laquelle ils pointent avant de cliquer dessus, par exemple en survolant (sans cliquer) avec le curseur.
- Vérifier l'intitulé parfois trompeur des liens affichés : les URL raccourcies (notamment dans les tweets) cachent souvent des liens distincts malveillants. Après avoir cliqué sur un lien, au niveau du navigateur, contrôler la réputation du site indiqué par les éventuels plugins de protection anti-phishing.
- Ne jamais communiquer de données sensibles sur des sites non-sécurisés : s'assurer de la connexion en https tout en contrôlant les informations du certificat du site.

5 Nouvelles attaques web : les attaques client

De nos jours, nombre de serveurs sont correctement protégés (mis à jour, sécurisés) ; il devient beaucoup plus efficace pour les hackers de s'attaquer aux clients. Vous trouverez ci-après quelques types d'attaques de ce type (inspiré d'un cours SCRT de 2012)[23] et comment s'en protéger (ma proposition).

5.1 Cross-site Scripting (XSS)



[24]

Le hacker peut utiliser une autre fenêtre ou un autre programme pour bénéficier de votre authentification sur la session « critique ».

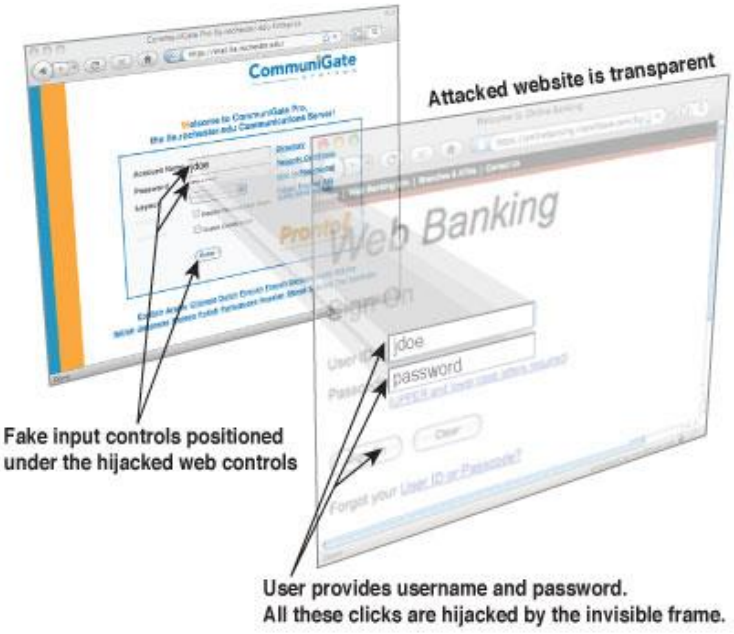
Protection

- Ne pas naviguer sur plusieurs sites à la fois
- Effacer automatiquement le cache à chaque fermeture du navigateur
- Fermer le navigateur avant et après d'aller sur un site bancaire

5.2 Clickjacking / Likejacking / Dragjacking…

Le **détournement de clic** (clickjacking) est une technique malveillante visant à pousser un l'utilisateur à cliquer – et éventuellement entrer des informations – sur ce qui semble être une page Web normale mais utiliser une page transparente ajoutée en surcouche à son insu. Illustration :

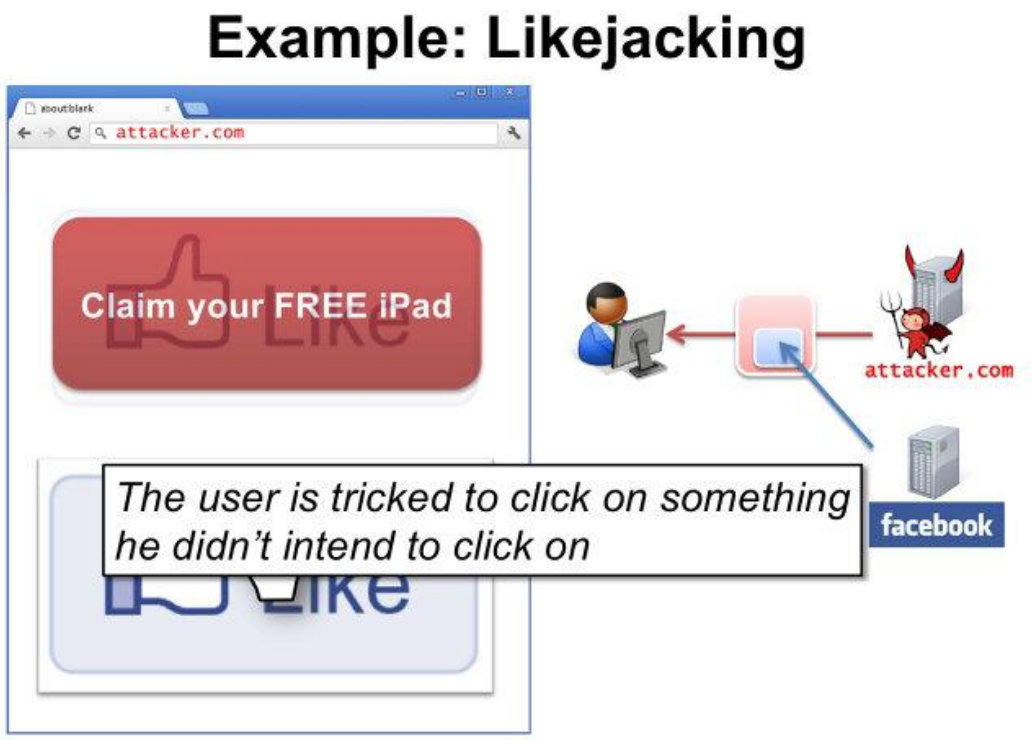
[23] SCRT – Nouvelles attaques Web – Exploitation des clients
[24] http://hackingstuffs.com/attacks/xss-css-script-attack/



25

26

[25] http://www.lle.rochester.edu/resources/computer_support/
[26] http://niebezpiecznik.pl/post/clickjacking-i-framebusting-czyli-ochrona-przed-clickjackingiem/



27

Protection

- Etre suspicieux à l'excès
- Ne jamais lancer des jeux sur les postes de travail
- Ne jamais accepter l'installation de nouveaux codecs ou logiciels sans passer par le service informatique qui testera la légitimité de la demande et son caractère inoffensif sur des stations de test.
- Se méfier des cookies : les refuser autant que possible, faire le ménage dans les cookies installés.
- Installer NoScript
- Bloquer les scripts, augmenter le niveau de sécurité du navigateur : voir http://fr.wikipedia.org/wiki/D%C3%A9tournement_de_clic

Le **Dragjacking** est une variante plus sophistiquée ou l'on vous fait déplacer des objets à votre insu (par exemple en simulant un jeu ou il faut placer des objets dans un coffre).

5.3 DNS Rebinding

Section à compléter dans une édition ultérieure.

[27] http://www.crazylearner.org/clickjacking-example/

6 Notes sur les SPAM

Historiquement, le premier SPAM date du 3 mai 1978 lorsqu'un commercial de DEC a envoyé sur Arpanet un message à tous les utilisateurs, soit 6000 personnes, au lieu d'un group limité de personnes.

Le nombre d'utilisateurs sur internet a bien progressé depuis et certains estiment que si les spammeurs ont un retour aussi bas que 1 sur 100 million cela reste un commerce économiquement rentable : le problème ne risque pas de disparaitre de lui-même.

Plusieurs techniques permettent de filtrer les spam :

- Listes noires (black list)
- Correspondances de motif (pattern match)
- Filtres de Bayes
- Utilisation de modules externes

7 Notes sur les virus et les malware

Frederick B. Cohen inventa l'utilisation du mot « virus » en informatique et proposa des techniques de défense[28].

Cohen démontra en 1987 qu'il n'y a aucun algorithme susceptible de détecter tous les virus.

Ce qui rend toujours plus difficile la détection des virus et malware, c'est les mécanismes de furtivité mis en place par les pirates, tels :

- La désactivation des anti-virus
- Le blocage des mises à jour
- Eviter la détection
- Eviter certains utilisateurs, certaines cibles, pour pouvoir se propager plus tranquillement et ne pas être détecté trop vite par les laboratoires anti-virus
- Mise en veille, comportements variables

Des virus font appel au **polymorphisme** : par exemple Dark Avenger dans les années 90. Un moteur polymorphic est capable de ré-écrire différemment le code (même résultat mais avec des instructions différentes) ; il peut aussi utiliser des technique d'encryption ou d'obfuscation. Comme le code change en permanence, l'utilisation de signatures pour le détecter est illusoire.

Ralph Burger écrivit en 1986 le premier virus qui infectait plusieurs types de fichiers.

8 Le projet macaron

http://macaron.googlecode.com

[28] 1984 http://web.eecs.umich.edu/~aprakash/eecs588/handouts/cohen-viruses.html

Pertinence de cette référence à évaluer dans une édition ultérieure.

9 Sept conseils pour éviter de se faire pirater (BILAN, Avril 2015)

http://www.bilan.ch/techno-plus-de-redaction/sept-conseils-eviter-de-se-faire-pirater

CYBERSÉCURITÉ

Qui n'a a jamais ouvert un fichier attaché dans un mail obscur, puis regretté deux secondes après? Ou encore acheté ses billets d'avion via une connexion WiFi dans un café à la gare? Tout appareil connecté à Internet est potentiellement attaquable. Une réalité que nous finissons souvent par négliger, autant à titre privé qu'au travail.

Et pourtant, les chiffres de la cybercriminalité sont vertigineux. Quatre cents millions de personnes sont concernées par des cyberattaques chaque année selon Symentec, l'un des leader dans la protection informatique. Le cabinet Capgemini estime qu'entre 2013 et 2014, le nombre de cyberattaques a augmenté de 120% dans le monde, tandis que le coût de la cybercriminalité pour les entreprises s'élèverait en moyenne à 7,6 millions de dollars par an. Soit une augmentation de 10%.

Et les smartphones ne sont pas épargnés : dans 33% des cas, l'introduction d'un malware est réalisée au travers d'une application mobile.

Un journaliste du site *Business Insider*, spécialiste des questions de cybersécurité, rappelle sept points fondamentaux pour minimiser les chances de se faire pirater. Petite piqûre de rappel.

400 millions de personnes sont concernées par des cyberattaques chaque année.

1. Méfiez-vous des e-mails: Simple et accessible, l'email est une arme de choix pour les cyberattaques. La technique de l' "**hameçonnage**" (**phishing**) consiste à envoyer un mail d'apparence inoffensif, qui redirigera la victime vers un faux site où elle devra rentrer ses coordonnées. Une des meilleures précautions est d'être certain de l'identité de l'expéditeur. Vérifiez si l'adresse mail correspond avec le site internet dont vous supposer l'origine. Si vous souhaitez être encore plus prudent, n'hésitez pas à **vérifier l'adresse IP de l'expéditeur**. Pour ce faire, il faut aller à la source du mail et

trouver l'adresse IP qui suit la ligne "Received: from". Petit conseil, si vous avez plusieurs "Received: from", il faut prendre en considération celui en dernier sur la page. Il est possible après d'identifier l'adresse IP sur Google ou via des sites spécialisés comme **Ip-Tracker**.

Comment trouver l'adresse IP d'un mail dans Gmail ?

> Cliquez sur la petite flèche noire localisée en haut à droite et déroulez son menu;

> Cliquez sur "Affichez l'original";

> Une nouvelle page s'ouvre, et vous cherchez le fameux "Received: from". L'adresse IP est composée de 4 nombres entiers et notée sous la forme xxx.xxx.xxx.xxx.

Comment trouver l'adresse IP d'un mail sous Outlook ?

> double-cliquez sur un mail pour l'ouvrir dans une nouvelle fenêtre;

> prenez le chemin suivant : Fichier / Propriété;

> sur la nouvelle boîte de dialogue, regardez dans "En-têtes internet" (zone encerclée de rouge sur l'image), et chercher le "Received: from".

2. Vérifiez l'origine des liens: Les mails inconnus contiennent souvent des liens pour des sites eux aussi inconnus. Vous prenez le risque d'être redirigé sur un faux site internet, avec de grandes chances d'être victime d'un "phishing". Ou pire, d'un virus ou un logiciel malveillant qui s'installe à votre insu sur votre ordinateur ou Smartphone. Si c'est un lien sous forme de raccourci, n'hésitez pas à utiliser des outils comme **URL X-Ray** pour en déterminer l'origine. Les sites encryptés sont en général sûrs, portant la mention **HTTPS** visible dans l'adresse URL, et avec l'**icône d'un cadenas**.

3. Ne jamais ouvrir les pièces jointes: A moins d'être sûr à 120% de la provenance de l'email, il est déconseillé de les ouvrir. Pour placer leurs virus, les hackers ont l'habitude de les intégrer dans des fichiers joints aux emails. Situation fréquente dans les entreprises, les employés négligents téléchargent le logiciel malveillant, qui va finir par infecter l'entier du réseau. Les fichiers les plus suspects se trouvent sous le format **Word, PDF** et **.EXE**.

4. Utilisez l'authentification à deux facteurs: L'authentification à deux facteurs requiert non seulement d'entrer un mot de passe mais aussi exige une deuxième confirmation pour valider l'accès, sous la forme par exemple d'un code envoyé sur le téléphone. Le procédé est plutôt efficace en cas de vol des mots de passe, et de plus en plus d'entreprises l'adoptent dans leurs standards de sécurité.

5. Optez pour un mot de passe perfectionné: Un conseil tellement évident, mais au final souvent sous-estimé. Un mot de passe qui augmente les chances de sécurité inclut des **majuscules, minuscules, chiffres, signes de ponctuation et du non-sens**. Ne faites **aucune référence personnelle**, et ne sauvegardez pas vos mots de passe sur un fichier. Et le plus important, n'utilisez pas le même mot de passe pour tous vos comptes. N'hésitez pas à les **changer régulièrement**, spécialement pour les comptes les plus délicats comme les emails ou celui d'e-banking.

6. Restez sur vos gardes en sauvegardant sur le Cloud: Qu'importe le niveau de sécurité de la plateforme Cloud, gardez à l'esprit que vous confiez vos données à une tierce personne. De nombreux experts maintiennent que **tout ce qui est mis online, dont le Cloud, a des chances d'être visible par la suite**. Les entreprises, dont la protection des données est un élément central, doivent être particulièrement attentives sur ces questions. Faut-il donc ne rien enregistrer sur le Cloud ? Pas nécessairement. Il faut savoir où vont vos fichiers, et connaître les pratiques de stockage de votre fournisseur Cloud. **Si vous effacez des fichiers sur votre ordinateur ou téléphone, assurez-vous qu'ils le soient également sur le Cloud.**

7. Vous êtes sur un réseau WiFi public ? Attention. Vous pensiez acheter votre billet d'avion ou vérifier votre compte bancaire dans un café ? Réfléchissez-y à deux fois, car vous n'avez aucune idée du niveau de sécurité de la connexion. Idem dans les hôtels ou les centres de conférences. Des chercheurs ont décelé une f**aille qui rend les trafics sur WiFi dans les plus grands hôtels du monde vulnérables aux attaques**. Il est pratiquement impossible de s'en rendre compte. Si vous devez accéder à des informations aussi privées, il est conseillé d'utiliser certains outils. Par exemple, une **connexion VPN** (Virtual Private Network), qui crypte le trafic. Ainsi, le réseau Wifi ne peut pas voir sur quel site vous vous rendez. Ou encore, configurez votre propre point WiFi en utilisant votre mobile.

10 S'adresser à des enfants

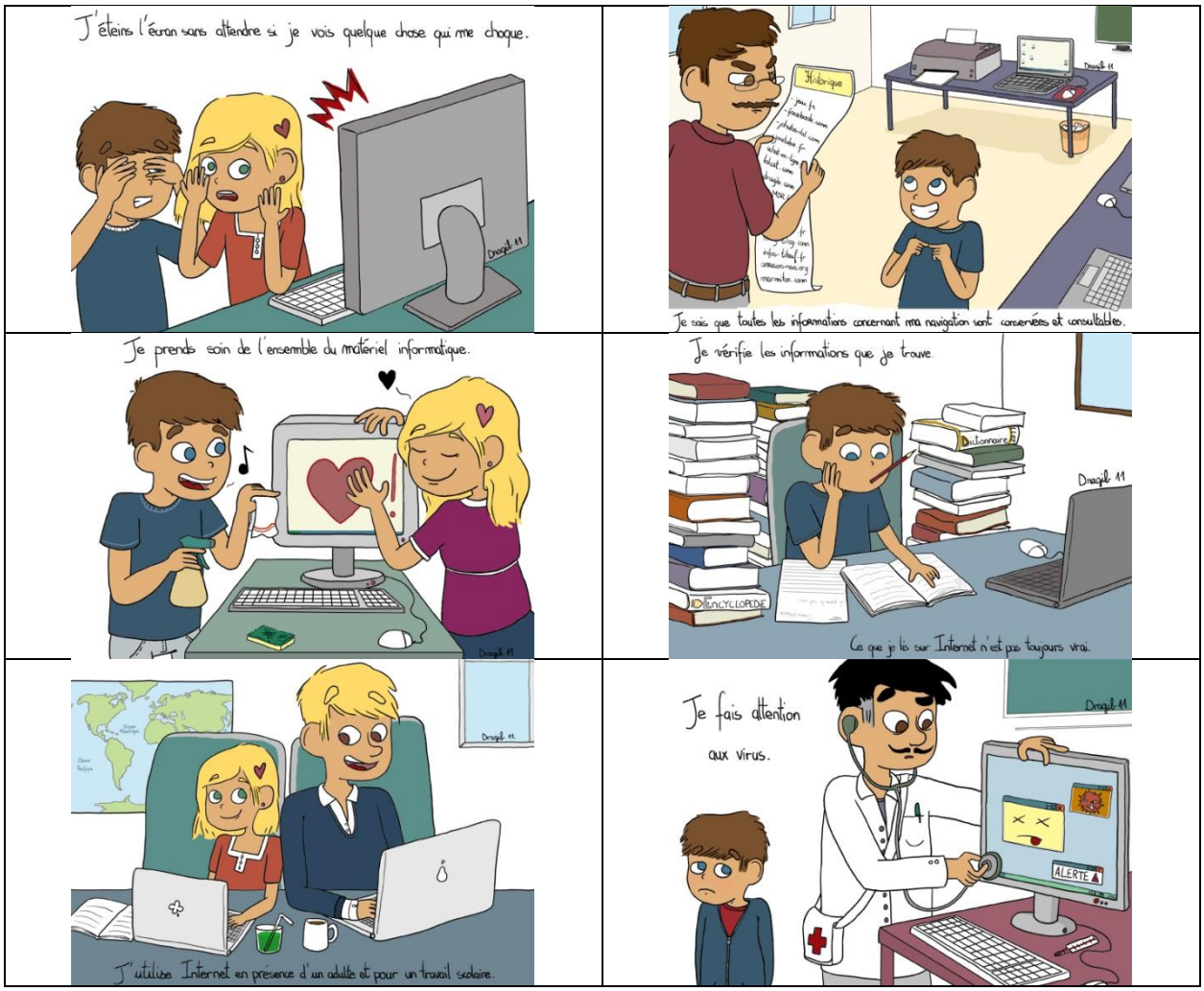
http://laguenne.com/charte/chartece1.htm Charte pour une école primaire en Corrèze

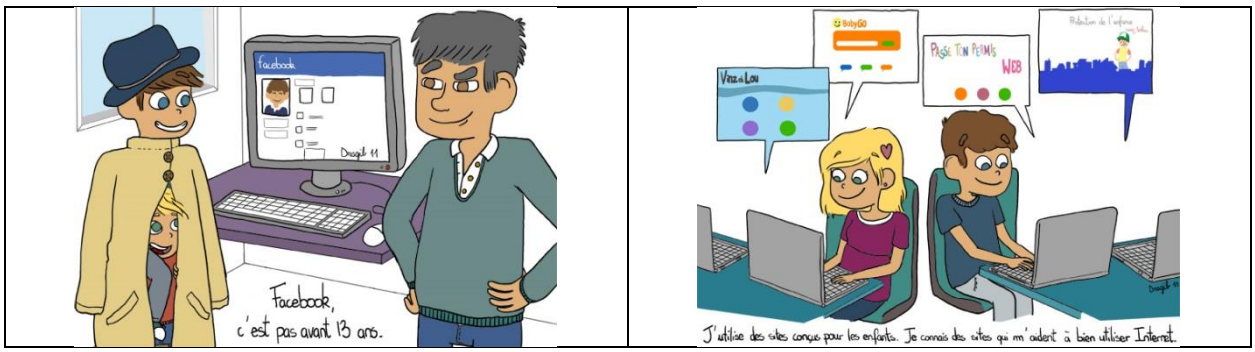
Un immense merci à Ghislaine Boutigny, illustratrice, qui a bien voulu participer, à distance, à cette petite aventure !
Dans un premier temps, les élèves du CE1 de Laguenne ont écrit le texte de la charte.
Ghislaine a par la suite et avec beaucoup de talent, donné vie en images, à ce travail.

École élémentaire de Laguenne en Corrèze
écoles internet
http://pagesperso-orange.fr/laguenne.19/

Charte pour utiliser les ordinateurs et Internet à l'école de Laguenne (CE1)

(Ensemble des règles communes qu'élèves et enseignants doivent suivre et respecter dans l'intérêt de tous)





Attention, ces images ne sont pas libres de droits.

11 Protéger sa vie privée

http://www.techrepublic.com/blog/five-apps/five-utilities-that-help-protect-your-online-privacy/

- **Blur (anciennement DoNotTrackMe)**

La version gratuite peut bloquer les trackers, gérer vos mots de passe, les formulaires de automatiques et masquer votre email.

- **Adblock**

Bloque la publicité

- **Web of Trust**

Indique par un code de couleur le niveau de sécurité évaluée des sites

- **Spotflux**

La version gratuite fournit un cryptage Web de basique.

- **CyberScrub Privacy Suite**

Effectue une suppression sécurisée des traces de la navigation ; supprime également des preuves à partir d'emplacements tels que le fichier d'échange Windows, les fichiers temporaires, et Index.dat. Gratuit 15 jours.