Internet, Courrier électronique, réseaux sociaux... Dangers, comment s'en protéger ?

Michel Picart, membre du CA de l'UTL, Sébastian Tessier, Informaticien

Internet histoire et fonctionnement :

Internet est le réseau informatique mondial accessible au public. C'est un réseau de réseaux, sans centre névralgique, composé de millions de réseaux aussi bien publics que privés, universitaires, commerciaux et gouvernementaux,.

Le Web www (World Wide Web**)**. C'est le **système** fonctionnant sur le réseau mondial Internet qui permet de consulter, avec un navigateur, des pages accessibles sur des sites. Aujourd'hui on ne fait pas toujours la distinction le Web et Internet.
L'information est transmise via Internet grâce à un ensemble standardisé de protocoles de transfert de données, qui permet des applications variées comme le courrier électronique, le World Wide Web, la messagerie instantanée. Un internaute est une personne qui utilise un accès à Internet. Cet accès peut être obtenu grâce à un fournisseur d'accès. Pour utiliser Internet, il faut un navigateur, Chrome, Edge, Firefox.. et un moteur de recherche, Google, Yahoo , Quant …

Dans les années 1990, l'apparition du Web a contribué à rendre internet accessible au grand public. Puis, depuis les années 2010, un nombre croissant de types d'objets divers ont été connectés à Internet, formant l'Internet des objets.

Internet sert à communiquer, s'informer, se divertir .. via l'E Mail, la messagerie, le web. Mais cette toile est devenue si énorme et son utilisation si complexe qu'elle nous échappe et peut présenter des risques. Ces risques concernent tout autant l'information, la vie privée et la cybercriminalité.

L'information

Après les journaux, la télévision, Internet est devenu le principale source d'information, grâce entre autres à la rapidité, la quantité et la diversité des informations. Google c'est aujourd'hui 6,9 milliards de requêtes par jour dans le monde.

A l'heure du "tout numérique", l'actualité et la connaissance font leur nid sur la toile. Tout est accessible, en toute langue à propos de tout, tout le temps. Pratique et efficace, les moteurs de recherche nous font accéder à l'information de manière rapide ! Aujourd'hui la connaissance, de la plus scientifique à la plus farfelue, est développée sur le web et accessible pour tous L'actualité elle aussi est disponible à tout instant et est actualisée minute par minute. L'information va tellement vite que les démentis sont parfois aussi rapides à apparaître que l'information elle même. Bobards, rumeurs, mensonges, fausses nouvelles, bourrage de crânes, propagande, intoxication, désinformation, ne sont pas l'apanage des temps récents mais sont aussi vieux que l'humanité. (Charnier de timisoara...ou encore plus loin le cheval de troie ..). Aujourd'hui on parle fake news au contenu trompeur, fabriqué, manipulé, du à de multiples raisons, non vérification des sources, « provocation », qui vise à créer du buzz, « partisanerie »,« influence politique » dans le but de la conquête du pouvoir, enfin « propagande », prête à tout pour faire triompher une cause.

Les réseaux sociaux sont en passe de devenir le cancer de l'information, nous ne contrôlons plus rien et certains en profitent. On peut trouve de multiples exemples de photos truquées, Ex : manif des gilets jaunes, Wuhan..

Publier d l'information, via un site Internet, un blog ou des réseaux sociaux n'est que très peu

réglementée. Ecrire une page, la publier sur un site, un blog ou les réseaux sociaux est à la portée de tous. Un simple logiciel permet de manipuler unephoto. Mais seuls, face à nos écrans, sommes-nous aussi critiques que nécessaires.

Quelle attitude adopter ?

La vie privée

Toutes nos données peuvent un jour ou l'autre nous échapper. Soit par accident, malveillance, erreur humaine d'où l'intérêt de se protéger, tout d'abord en sauvegardant ses données, fichiers personneles, photos etc .. sur un disque dur, le cloud, une clé USB. Les données personnelles que nous laissons sur Internet représente un ensemble de données devenu si volumineux qu'il dépasse l'intuition et les capacités humaines d'analyse et même celles des outils informatiques ce sont les « big data » conservées dans des « data centers ».

L'explosion de l'utilisation d'appareils connectés (30 milliards aujourd'hui, 75 dans cinq ans) a créé une myriade de points d'entrée vulnérables dans les réseaux domestiques. Un nombre étonnant de fabricants mettent en place des codes d'accès très basiques sur leurs appareils, parfois même aussi simples que 123456. Dans certains cas, les appareils ne comportent même pas de code. Le piratage et l'exploitation commerciale des données est le plus grand risque. Quelques conseils

La géolocalisation, les cookies, (dont le but est d'assurer une interaction plus aisée et plus rapide entre le visiteur et le site web, ils mémorisent vos préférences et vous permettent ainsi d'accélérer vos accès ultérieurs au site et de faciliter vos visites.) les pop up sont des fonctions destinées à recueillir le plus grand nombre de données personnelles alimentant les algorithmes permettant de cibler le consommateur.

En paramétrant sont navigateur, on peut amoindrir les risques de traçage, de pistage et de récolte de données.

La vie privée et communication :

Courier électonique, messagerie instantanée et réseaux sociaux
E.Mail : Utiliser la fonction Cci (copie carbone invisible) qui permet de cacher les adresses des différents destinataires.
Vie privée et réseaux sociaux : Devenu un outil d'annonces pour les personnalités publiques, politiques. Possibilité d'atteindre des milliers, voire millions de personnes en qq secondes. 70 % des utilisateurs des réseaux sociaux sont exposés aux risques de fuite d'informations sensibles du fait d'une utilisation maladroite des médias sociaux et d'une méconnaissance en matière de protection de la vie privée numérique. La vie privée des utilisateurs est hors de leur contrôle : une fois que vous êtes sur **Facebook** vous y resterez pour toujours. Vos informations les plus personnelles seront à jamais stockées dans les serveurs de ce réseau social ... Facebook est le paradis des voleurs d'identités, des détournements de photos et autres arnaques. Pour se faire passer pour une autre personne, il suffit juste de créer un profil au nom de cette personne. Facebook a des côtés positifs et ludiques mais ce réseau social est malheureusement aussi risqué car le grand danger reste la pédophilie. Les adolescents les plus vulnérables sont une proie facile pour les pédophiles et les délinquants sexuels. Les enfants et les adolescents ont en moyenne... 210 amis
Quelques conseils

La cybercriminalité

Domaine le plus important, le plus dangereux car c'est le domaine de l'argent, des hackers d'entreprises

Hammeçonnage : Technique utilisée par des fraudeurs pour obtenir des renseignements personnels dans le but de perpétrer une usurpation d'identité ou inciter l'internaute à communiquer des données personnelles (comptes d'accès, mots de passe…) et/ou bancaires en se faisant passer pour un tiers de confiance. (7.504.979 euros ont été dérobés par le biais de l'hameçonnage en 2019.) Voir Ouest France du 23/10/2020

Dans le cas de l'hammeçonnage (phishing) le pirate, grace à un e.mail frauduleux, dirige l'internaute vers un faux site qui lui permettra de voler ses données.
Quelques conseils de bon sens : Vérifier l'écriture du lien, de l'adresse URL, l'orthographe, la correspondance entre les adresses, la syntaxe...

Ransomware :

Un rançongiciel (de l'anglais **ransomware**), logiciel rançonneur, logiciel de rançon ou logiciel d'extorsion, est un logiciel malveillant qui prend en otage des données personnelles. Pour ce faire, un rançongiciel 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.

- 52% des entreprises françaises ont déjà subi une attaque par ransomware (1)
- 34% des personnes victimes d'un ransomware auraient payé la rançon
- 81% des attaques se font par emails
- 4.34% des emails sont des ransomwares (5)
- Les ransomwares infectent 20 000 ordinateurs en France tous les mois (6)

Le prix moyen de la rançon est d'env 450€ en 2019 .
Les virus (3,6 milliards ordis infestés en 2016 (Kapersky))
Comme en médecine, Un ***virus*** est un agent infectieux. Un virus informatique est un programme informatique qui se reproduit et provoque des dysfonctionnements au niveau de votre machine et endommage les informations enregistrées. Ils sont aujourd'hui devenus plus rares. Il se répand à travers tout moyen d'échange comme l'Internet, les messages électroniques ou de leurs pièces attachées, les logiciels téléchargés, les clés USB …Ils se répliquent et se propagent en s'insérant dans d'autres logiciels. Ils peuvent afficher un message inopiné à l'écran, surcharger le disque dur afin de l'engorger, affecter la mémoire afin de ralentir l'ordinateur, supprimer les fichiers de l'utilisateur, supprimer des fichiers fondamentaux du système d'exploitation.
Que faire ? Utiliser un **firewall** pour filtrer ce qui vient d'Internet, utiliser d'un **antivirus** à jour . Aujourd'hui , les outils intégrés dans Windows 10 sont pratiquement suffisants. Sauvegarder ses données, ne pas ouvrir les pièces jointes douteuses.
Les spams : Le spam est un courrier indésirable à but publicitaire ou frauduleux. Ne pas répondre ni cliquer sur les liens des vrais spams (provenant de sources ou sites web inconnus). Pour bloquer définitivement l'expéditeur en question, il vous suffit juste de copier-coller l'adresse mail de l'expéditeur puis dans les paramètres de configuration de votre boîte mail bloquer l'expéditeur concerné ! Ainsi, vous ne recevrez plus aucun mail de cet expéditeur ! Vous pouvez également placer tous les mails indésirables dans la section SPAM / courriers indésirables (aussi appelé Junk mail) de votre boîte mail. Ils seront supprimés automatiquement au bout de 30 jours. Configurer Thunderbird ou Orange pour bloquer les spams
Acheter en ligne : Les achats vus avec humour
Quelques conseils : En résumé, afin d'éviter les arnaques sur les sites de vente sur internet, préférez les sites les plus connus, fuyez les promotions trop « alléchantes », restez sur des sites hébergés dans votre pays d'origine, vérifiez la présence des informations légales
Aujourd'hui faciles à craquer, les mots de passe nécessitent une attention particulière.

Pour un mot de passe de douze caractères ou plus, votre phrase doit contenir au moins :
Un **nombre**
Une **majuscule**
Un **signe de ponctuation** ou un **caractère spécial** (dollar, dièse, ...)
Une **douzaine** de **mots**

8 conseils pour sécuriser vos mots de passe
Créer plusieurs **mots de passe**. ...Utiliser un générateur de **mot de passe**. ...Miser sur la longueur. ...Varier les caractères. ...Préférer l'aléatoire. ...Changer de **mot de passe** régulièrement. ...Retenir ses **mots de passe** sans les écrire. ...Utiliser un gestionnaire de **mot de passe**.
Conclusion. 10 conseils