CLCV
CONSOMMATION LOGEMENT ET CADRE DE VIE
citoyens au quotidien

Se prémunir du piratage

- L'importance de bien choisir ses mots de passe
- Le phishing
- Le ransomware
- L'arnaque au faux support technique

La prévention reste la meilleure solution pour profiter pleinement et paisiblement des ressources disponibles sur internet.

On doit donc équiper son matériel d'un logiciel de sécurité complet et performant (virus, malware) et le mettre à jour. Les mises à jour de sécurité de son système d'exploitation et de ses logiciels permettent de minimiser les risques d'attaques. Mais le bon sens de l'internaute reste la meilleure arme contre le piratage et les dérives sur le net en général.

Des outils pédagogiques *« vie privée »* sont disponibles sur le site *Educnum.fr*

Une victime de cyber-délinquance pourra trouver des conseils et de l'assistance technique autour de chez elle sur le site *Cybermalveillance.gouv.fr*

L'importance de bien choisir ses mots de passe

Un bon mot de passe doit éviter la facilité. Une méthode simple permet de retenir facilement des mots de passe élaborés avec un mélange de lettres majuscules, minuscules et de chiffres :

- mémoriser une phrase
- conserver les initiales des mots
- choisir une suite de chiffres ou une date importante pour vous
- alterner lettres et chiffres comme bon vous semble

Exemple : ***« Mon chéri est parti à St Nazaire »*** + 9 janvier 2004. On peut vous suggérer le mot de passe suivant : Mc09ep01aSN04.

Il est conseillé de mémoriser les mots de passe et de ne pas le stocker dans son ordinateur. Cela fait fonctionner sa mémoire. Cela implique de pas accepter que le navigateur web enregistre les identifiants et mots de passe.

Mars 2018

En dernier recours, quand on ne peut pas mémoriser tous les mots de passe :

- conserver les mots de passe dans un lieu caché, à l'abri des regards.
- ne pas noter sur un papier ou un post-it à proximité de son ordinateur ou de son smartphone.

Le phishing

Le phishing (ou hameçonnage ou filoutage) est une escroquerie qui a fait plus de 2 millions de victimes en France en 2015.

Un mail de phishing est envoyé par un pirate informatique, il imite un message qu'aurait pu envoyer un interlocuteur avec lequel on a l'habitude de correspondre (fournisseur d'énergie, banque, impôts, fournisseur internet …). Il comporte le nom et le logo habituellement utilisés par le professionnel dont l'identité est usurpée.

Les pirates vont décrire une situation d'urgence pour inciter le consommateur à agir le plus vite possible et ainsi ne pas trop réfléchir au bien-fondé de la demande. Les scénarios utilisés sont très nombreux : éviter une coupure du service suite à un soi-disant impayé, recevoir le remboursement d'un trop perçu imaginaire Le but du phishing est toujours le même, obtenir des coordonnées bancaires ou des codes confidentiels pour pouvoir ensuite prélever frauduleusement sur le compte en banque de la victime.

Un piège de plus en plus perfectionné

Les avertissements répétés auprès du grand public se heurtent à une évolution constante de cette arnaque :

- les scénarios développés par les pirates sont multiples et les mails de phishing ne sont aujourd'hui plus des imitations grossières repérables aux nombreuses fautes d'orthographe.
- certains pirates informatiques sont en mesure d'adresser des mails de phishing avec les nom et prénom de leur victime.
- un mail de phishing peut contenir deux sortes de pièges :
  - ◆ un lien cliquable qui mène vers un faux site internet du professionnel dont l'identité est usurpée, l'internaute est alors incité à rentrer ses codes d'accès,
  - ◆ une pièce jointe qui, si elle est ouverte, infectera l'ordinateur avec un logiciel malveillant qui prendra discrètement possession de l'ordinateur en captant les données sensibles (comme les données bancaires). Ce logiciel malveillant peut également prendre possession de la boite mail du consommateur et envoyer en son nom des mails de phishing à ses contacts.

Les règles à adopter

Face à cette recrudescence de e-mails de phishing et aux refus de remboursement, très contestables, opposés par certaines banques la prudence doit être de mise :

- doit être considéré comme frauduleux un e-mail qui vous demande des coordonnées bancaires ou de l'argent, même s'il comporte vos nom et prénom et/ou semble provenir d'une adresse mail connue. En cas de doute, et malgré l'urgence qui est décrite, il faut prendre le temps de vérifier directement auprès de l'expéditeur supposé s'il en est bien l'auteur,
- sur ces emails suspects, il ne faut jamais ouvrir les pièces jointes, utiliser les liens cliquables ou les coordonnées téléphoniques qui y figurent. Tous ces éléments font partie du piège,

- il existe certains outils pour vous aider à lutter contre ce fléau. La plupart des navigateurs internet disposent d'une fonctionnalité d'avertissement contre le phishing et il existe des logiciels de filtre anti-SPAM. Mais ces logiciels ne sont pas parfaits et ne remplacent pas la vigilance de l'internaute.

Le ransomware

Le ransomware (ou rançongiciel) est un logiciel malveillant qui bloque l'accès à l'ordinateur ou aux fichiers des victimes.

Il peut être attrapé en ouvrant une pièce jointe infectée, en cliquant sur un lien malveillant ou en navigant sur de sites internet compromis par des pirates.

L'objectif des pirates est d'obtenir de la victime le paiement d'une somme d'argent, une rançon, en échange de la promesse, pas toujours tenue de débloquer l'accès à l'ordinateur. Il est donc déconseiller de payer la rançon demandée.

Les règles à adopter

- Les pirates exploitent fréquemment des vulnérabilités connues dans les logiciels dont les correctifs n'ont pas été mis à jour par l'internaute. Il est donc indispensable d'appliquer systématiquement les mises à jour de sécurité de votre système d'exploitation et des logiciels installés.
- N'ouvrez pas les mails suspects.
- Faites une sauvegarde régulière de vos données et de votre système pour pouvoir les réinstaller en cas de besoin.
- Appliquez une désinfection du système lorsque c'est possible, à défaut il faut réinstaller le système ce qui entraînera la perte des fichiers.
- Déposez plainte.

L'arnaque au faux support technique

Cette escroquerie consiste à faire peur à l'internaute pour le pousser à contacter un soit disant support technique qui le convaincra de payer une fausse prestation technique.

L'arnaque peut être initiée par téléphone, SMS, e-mail. Cela peut prendre également la forme d'une alerte sur le PC, un écran apparaît pour signaler un problème technique grave et demander de rappeler un faux numéro d'assistance qui correspond en réalité aux pirates.

Une fois en ligne, le consommateur se verra facturer une prestation technique imaginaire. L'arnaque peut aller jusqu'à la prise de contrôle du PC par les pirates avec menace de détruire les données si l'internaute refuse de payer.

Un tel *« message d'alerte »* doit donc éveiller la méfiance de l'internaute qui doit s'abstenir d'appeler. Les règles à adopter sont similaires à celles pour le ransomware.