L'@telier - Se protéger sur Internet

COMMENT SE PROTÉGER SUR INTERNET ?

Hameçonnage, rançongiciel, arnaque au service client, virus, malware...
Les dangers concernant la navigation sur Internet sont nombreux se dissimulent parfois sous les actes les plus communs que vous effectuez au quotidien sur le web.

Pour éviter au maximum ce type de souci, et se protéger sur Internet au mieux, l'ANSSI (Agence Nationale de la sécurité des systèmes d'information) donne 10 réflexes à acquérir :

1. Éviter de se rendre sur des sites douteux ou illégaux
2. Faire ses mises à jour de sécurité dès que possible
3. Choisir des mots de passes sécurisés
4. Bien choisir son pare-feu et son antivirus
5. Faire des sauvegardes régulières de ses données
6. Se munir d'un bloqueur de publicités
7. Redoubler de vigilance face aux messages d'inconnus
8. Faire attention à qui on transmet ses données
9. Réfléchissez bien avant de publier des informations sur Internet
10. N'oubliez pas vos téléphones et tablettes

ARNAQUES ET VIRUS : HAMEÇONNAGE

Vous recevez un message ou un appel inattendu, voire alarmant, d'une organisation connue et d'apparence officielle qui vous demande des informations personnelles ou bancaires ?
Vous êtes peut-être victime d'une attaque par hameçonnage (phishing en anglais) !

Objectif : Voler des informations personnelles ou professionnelles (identité, adresses, comptes, mots de passe, données bancaires...) pour en faire un usage frauduleux.

Conseils :
L'orthographe : la plupart des courriers malveillants sont envoyés depuis l'étranger, la syntaxe de ces messages est souvent très mauvaise.
Le sujet du message : les "spammeurs" veulent avant tout récupérer vos données bancaires, ou à défaut, vos identifiants de connexion (messagerie, banque, réseaux sociaux...). Une vraie banque ou un réseau social ne vous demandera jamais d'informations personnelles par mail.
L'adresse email de l'envoyeur : les courriers indésirables proviennent la plupart du temps d'une adresse "crédible". Cependant, quand on prend le temps de regarder l'adresse en détail, on y trouve souvent des fautes ou des orthographes différentes. Par exemple, faceboOk / labanquepostal / g-ogle...

L'@telier - Se protéger sur Internet

ARNAQUES ET VIRUS : LES RANÇONGICIELS

Vous ne pouvez plus accéder à vos fichiers et on vous demande une rançon ? Vous êtes victime d'une attaque par rançongiciel (ransomware).

Objectif : Réclamer le paiement d'une rançon pour rendre l'accès aux fichiers verrouillés.

Conseils : La meilleure solution est d'éteindre complètement l'ordinateur (en le débranchant si nécessaire) puis de porter plainte. L'ordinateur devra être complètement restauré pour se protéger complètement.

ARNAQUES ET VIRUS : LES FAUX SUPPORTS TECHNIQUES

Votre ordinateur est bloqué et on vous demande de rappeler un support technique. Vous êtes victime d'une arnaque au faux support.

Objectif : Inciter la victime à payer un "dépannage" informatique.

Conseils : Il ne faut bien entendu pas appeler le numéro donné. Prenez en photo le message affiché et gardez toutes les preuves disponibles (adresse du site web, numéro de téléphone...) qui seront utiles aux enquêteurs si vous portez plainte. Pour se débarrasser du message, vous pouvez redémarrer votre ordinateur (en le débranchant si nécessaire) et lancer une analyse antivirus.

OUTILS ET CONSEILS : LES GESTIONNAIRES DE MOTS DE PASSE

Les gestionnaires de mots de passe stockent tous vos mots de passe derrière un unique mot de passe « maître ». Une fois le logiciel installé, il faut télécharger une extension pour votre navigateur. Le logiciel vous demandera ensuite d'importer tous vos mots de passe, automatiquement ou en les saisissant un par un.

Le logiciel les gardera en mémoire et vous suggérera parfois de changer les moins sûrs. Si vous créez un compte sur un nouveau site, le gestionnaire vous proposera automatiquement un mot de passe grâce à un générateur intégré.

Chaque fois que vous démarrez votre ordinateur, vous devez saisir votre mot de passe maître. Vous êtes ainsi assuré que si quelqu'un d'autre utilise l'appareil, il n'aura pas accès à tous vos comptes. Ce mot de passe maître protège tous vos autres mots de passe. C'est le seul que vous devrez impérativement mémoriser.

OUTILS ET CONSEILS : LES BLOQUEURS DE PUBLICITÉ

Entre les fenêtres intempestives (pop-up), les bandeaux fixes et les vidéos à lecture automatique, la navigation sur Internet peut être compliquée. Pour limiter la gêne, vous pouvez installer un bloqueur, comme uBlock (pubs), Disconnect ou Ghostery (antitraceurs).