SENSIBILISATION AUX RISQUES SUR INTERNET

Document réalisé par le Lieutenant Lorraine SCHULZ
Communauté de Brigades de Castelginest

INDEX

Comment bien choisir son mot de passe ?

<u>Différent pour chaque service</u>

En cas de vol de votre mot de passe, tous les services utilisant ce dernier seront piratables

<u>Complexe : au minimum 12 caractères mélangeant</u>

- majuscule,
- minuscule,
- chiffres,
- caractères spéciaux

<u>Impossible à deviner</u>

Évitez les informations personnelles facile à trouver sur les réseaux (ex : date anniversaire...) ou les suites logiques (ex : 1234, azerty...)

Gendarmerie nationale

CE QU'IL NE FAUT PAS FAIRE !

Comment sécuriser son compte sur les réseaux sociaux ?

- Utilisez un mot de passe pour chaque réseau social
- Vérifiez les paramètres de confidentialité
- Ne diffusez aucune information personnelle ou sensible pouvant être utilisée pour vous nuire
- N'envoyez jamais de photos ou vidéos intimes à des contacts virtuels
- Vérifiez les autorisations des applications tierces (jeux, quiz…) qui proposent d'interagir avec vos comptes de réseau social
- Vérifiez régulièrement les connexions à vos comptes

Comment sécuriser son appareil mobile ?

Installez un code d'accès difficile à deviner

Appliquez les mises à jour de sécurité

Chiffrez les données de l'appareil (paramètre à activer)

Il est toujours possible d'installer un antivirus sur son smartphone

En quoi est-ce important d'effectuer des sauvegardes et des mises à jour ?

En cas de perte, de vol, de panne ou de destruction de vos appareils numériques, **sans sauvegarde**, vous perdrez les données enregistrées sur ces supports.

Ne pas mettre à jour un appareil ou un logiciel, c'est prendre le risque de l'exposer à une faille de sécurité qui pourrait ouvrir une brèche dans votre environnement numérique.

LES BONNES PRATIQUES :

- Identifiez les appareils et les supports qui contiennent vos données
- Sélectionnez les données qui doivent être sauvegardées
- Planifiez vos sauvegardes et les mises à jour lors de périodes d'inactivité
- Déconnectez votre support de sauvegarde après utilisation (mettez-le hors-ligne)
- Téléchargez les mises à jour uniquement depuis les sites officiels
- Activez l'option de téléchargement et d'installation automatique des mises à jour

Quelles sont les techniques d'arnaque sur Internet ?

L'HAMEÇONNAGE

Le fraudeur leurre l'internaute en l'incitant à communiquer des données personnelles (comptes d'accès, mot de passe, identifiants bancaires…) en se faisant passer pour un tiers.

<u>Les fraudeurs peuvent utiliser différents moyens de communication :</u>

- un faux message SMS
- un faux appel téléphonique (de banque, de réseau social, de site internet…)
- un faux mail (d'une institution, d'un fournisseur d'énergie…)

Quelles sont les techniques d'arnaque sur Internet ?

LES RANÇONGICIELS

A l 'aide d'un logiciel malveillant, le fraudeur bloque l'accès à l'ordinateur ou à des fichiers en les chiffrant. Il réclame ensuite à la victime le paiement d'une rançon pour en obtenir de nouveau l'accès.

<u>Les fraudeurs peuvent utiliser différentes techniques pour infecter l'ordinateur :</u>

- envoyer une pièce-jointe, qui une fois ouverte infectera votre PC
- envoyer un lien malveillant qui infectera votre PV après avoir cliqué dessus
- utiliser des sites compromis (en navigant dessus, votre PC sera infecté)
- s'introduire dans votre PC par une cyberattaque massive

Quelles sont les techniques d'arnaque sur Internet ?

L'ARNAQUE AU FAUX SUPPORT TECHNIQUE

Le fraudeur effraie la victime en lui indiquant un problème technique grave et un risque de perte de ses données ou de l'usage de son équipement ; afin de la pousser à contacter un prétendu support technique officiel. Il propose ensuite à la victime un pseudo-dépannage informatique et peut l'inciter à acheter des logiciels nuisibles.

<u>Les fraudeurs peuvent utiliser différents moyens de communication :</u>

- un message SMS
- un message sur un faux « tchat »
- un courriel
- ou faire apparaître un faux message d'erreur sur votre écran

Comment se protéger des escroquerie sur Internet ?

L'HAMEÇONNAGE

Ne jamais communiquer d'information sensible par messagerie ou téléphone.

Vérifier l'adresse du site qui s'affiche dans le navigateur

Si vos moyens de paiement ont pu être communiqués, faites opposition immédiatement.

Si vous êtes victime d'une usurpation d'adresse de messagerie, changez votre mot de passe.

Si votre identité a été usurpée, déposez plainte dans un commissariat ou une gendarmerie.

Comment se protéger des escroquerie sur Internet ?

LES RANÇONGICIELS

Effectuez régulièrement les mises à jour de sécurité

Tenez à jour l'antivirus et configurez le pare-feu

N'ouvrez pas les courriels ou pièces-jointes provenant d'une chaîne de message

N'installez pas de programme ou logiciel d'origine douteuse

N'utilisez pas un compte de messagerie avec des droits « administrateur »

Éteignez votre PC quand vous ne vous en servez pas

Si vous êtes victime, ne payez pas la rançon : débranchez votre PC et déposez plainte

Comment se protéger des escroquerie sur Internet ?

L'ARNAQUE AU FAUX SUPPORT TECHNIQUE

Évitez les sites non-sûrs ou illicites

Effectuez régulièrement les mises à jour de sécurité

Tenez à jour l'antivirus et configurez le pare-feu

N'ouvrez pas les courriels ou pièces-jointes provenant d'une chaîne de message

Si vous êtes victime, ne répondez pas aux sollicitations et conservez toutes les preuves.

Purgez le cache, supprimez les cookies et désinstallez toute application suspecte.

Si vous avez fourni vos coordonnées bancaires, faites opposition.

Gendarmerie nationale

EN TOUT ÉTAT DE CAUSE, SI VOUS ÊTES VICTIME D'UNE CYBERMALVEILLANCE QUELCONQUE, SIGNALEZ LES FAITS SUR LA PLATEFORME :

www.internet-signalement.gouv.fr

Sources – Crédits images

- https://www.h24info.ma/lifestyle/high-tech/video-voici-choisir-de-passe/
- https://www.numerama.com/tech/227814-vous-voulez-creer-un-bon-mot-de-passe-la-cnil-vous-explique-comment-faire.html
- https://www.phonandroid.com/proteger-vie-privee-internet-combien-coute.html
- https://www.maghrebinfo.dz/2020/06/29/comment-securiser-votre-smartphone-votre-tablette-ou-votre-pc-le-guide-ultime/
- https://www.nomai.fr/securiser-son-smartphone/
- https://www.frandroid.com/android/mises-a-jour-android/189619_compte-rendu-des-mises-jour-android-chez-sfr-en-janvier-2014
- https://www.adealis-amiconseils.com/differents-types-de-sauvegarde-des-donnees-pour-les-entreprises/
- https://www.pg1.fr/5-conseils-de-bonnes-pratiques-pour-un-site-e-commerce/
- https://www.presse-citron.net/phishing-testez-ce-quizz-de-google-pour-reconnaitre-une-tentative-dhameconnage/
- https://www.patriote.info/technologie/victime-de-ransomware-devez-vous-payer/
- https://www.ouestpc.fr/actualites/larnaque-aux-faux-support-technique/
- SIRPA GENDARMERIE
- Cybermalveillance.gouv.fr