Projet DUCKWARE

6 habitudes à prendre

pour sécuriser ses appareils contre le phishing

Sami GHORZI
Étudiant MMI SNCDE

.1 Utiliser un mot de passe rigoureux

d'au moins 12 caractères pour chaque nouvelle inscription.

Évitez toutes informations personnelles qu'une personne extérieure pourrait deviner (date d'obtention de votre diplôme, votre animal de compagnie...).

Ne communiquez jamais votre mot de passe à un tiers.

Aucune société ou organisation sérieuse ne vous demandera vos mots de passe.

Si l'on vous demande votre mot de passe après avoir cliqué sur un courriel, considérez que vous êtes face à une tentative de piratage ou d'escroquerie.

L'adresse de messagerie est la cible principale dans les cyberattaques.

Si un cybercriminel parvenait à pirater votre messagerie, il pourrait prendre le contrôle de tous vos comptes en ligne (réseaux sociaux, comptes bancaires, sites administratifs, etc.).

Vous pouvez utiliser un gestionnaire de mot de passe pour les conserver.

Changez votre mot de passe au moindre doute d'utilisation frauduleuse.

Dans le cadre professionnel, n'attendez pas de soupçonner une fraude, modifiez vos mots de passe régulièrement

.2 Sauvegarder ses données

en mettant en place une routine de sauvegarde régulière

vous permet de vous protéger en cas de passe, de perte, de vol, de piratage d'informations ou de casse.

N'attendez pas d'être victime
pour commencer à protéger vos données.

La majorité des internautes mettent en place ces routines qu'après avoir subi une première perte de données.

Utilisez une clé USB. Vous pouvez aussi opter pour un service de stockage en ligne cloud, pour un stockage de données faible.

Pour des données plus conséquentes, le disque dur externe est la meilleure option. Sinon, pouvez également envisager le stockage via votre propre serveur FTP ou par Network Attached Storage (NAS).

.3 Mettre à jour vos logiciels

au risque de devenir vulnérable face à de nouvelles attaques

Faites les mises à jour qui vous sont proposées et assurez-vous qu'elles proviennent des sites officiels des éditeurs.

Restez vigilant face aux fausses mises à jour sur internet. Il peut s'agir d'une technique d'escroquerie.

.4 Se protéger des virus

et logiciels malveillants

Les fichiers malveillants sont nombreux et restent les techniques couramment utilisées par les pirates informatiques.

Pour vous protéger, il est indispenssable de posséder ces deux outils : un antivirus ou un pare-feu bien configuré.

Réalisez des analyses sur votre ordinateur, votre téléphone, votre tablette régulièrement pour identifier la présence de programmes malveillants

Les bonnes pratiques pour utiliser des appareils de stockage externes

- N'utilisez jamais un service ou un équipement inconnu ou abandonné.
- Attribuez un usage spécifique à chaque clé USB pour réduire les effets d'une éventuelle contamination.
- Chiffrez le contenu de vos appareils de stockage pour éviter le piratage.

.5 Éviter les réseaux wifi publics

qui sont un point d'accès facile pour intercepter vos données personnelles.

Voici quelques conseils pour éviter de vous connecter à ces réseaux ou, le cas échéant, vous en servir de façon sécurisée :

- Commencez par désactiver les connexions sans-fil (Wi-Fi, Bluetooth, NFC, ...) lorsque vous ne vous en servez pas.
- Privilégiez la connexion privée 3G/4G associée à votre abonnement mobile.
- Sécuriser votre partage de connexion d'un mot de passe pour éviter que n'importe qui puisse accéder à vos données mobiles.
- Veillez à ne jamais y réaliser d'opérations à caractère sensible (achat, déclaration d'impôts, etc...) sur un réseau public

.6 Restez vigilant sur les liens

et pièces jointes présentes sur des messages électroniques.

Le phishing reste la technique la plus utilisée et la plus efficace pour récupérer des informations confidentielles.

Voici les recommandations à prendre pour l'éviter :

1. Ne communiquez jamais vos informations personnelles ou professionnelles par messagerie ou par téléphone.
2. Positionnez le curseur de votre souris (sans cliquer) sur ce lien, ou, faites un appui long sur mobile, pour afficher l'adresse vers laquelle pointe le lien.
3. Vérifiez l'adresse d'un site Internet avant de vous renseigner. Si cela ne correspond pas exactement au site concerné, il s'agit certainement d'un site frauduleux.
4. Si le site le permet, activez la double authentification pour sécuriser vos accès.
5. Utilisez des mots de passe différents et complexes pour chaque site et application.
6. Saisissez directement dans votre navigateur l'adresse du site concerné.

En cas de doute, contactez directement l'organisme concerné pour confirmer le message ou l'appel que vous avez reçu. Si vous avez communiqué des informations bancaires, faites opposition à vos moyens de paiement et déposez plainte.

DUCK WARE

Projet DuckWare
Projet réalisé dans le cadre d'un travail étudiant

Sami Ghorzi
BUT MMI SNCDE 3
sami.ghorzi@edu.univ-fcomte.fr