Quelques informations sur le phishing, les chevaux de Troie, les ransomware, les mot de passe

Le phishing

Aussi appelé hameçonnage ou filoutage, le phishing consiste pour le fraudeur en envoyant un mail, à se faire passer pour un organisme qui vous est familier (banque, administration fiscale, caisse de sécurité sociale…), pour vous soutirer des informations personnelles telles que votre numéro de carte bancaire ou votre mot de passe ou d'autres informations personnelles

Comment s'en protéger ?

Soyez vigilant lorsqu'un courriel vous demande des actions urgentes.
Ne cliquez jamais sur une pièce jointe ou sur les liens d'un mail qui vous semble suspect.
Connectez-vous en saisissant l'adresse officielle dans la barre d'adresse de votre navigateur.
Sous Windows, vérifiez que votre antivirus est à jour. Utiliser régulièrement un logiciel pour détecter et effacer toute trace de logiciels malveillants.
Si vous pensez être victime de phishing, signalez-le sur :
Phishing Initiative
ou Signaler une page de phishing
ou internet-signalement.gouv.fr

Les chevaux de Troie

Ce sont des programmes ou fichiers qui tentent de nuire à votre système informatique. Ils sont souvent cachés souvent dans des logiciels gratuits, des documents à télécharger ou sur des clés USB. Ils prennent le contrôle de votre ordinateur à distance pour espionner vos actions, voler vos données personnelles, lancer des attaques, etc.
Ce ne sont pas des virus ou autres parasites. Ils tirent leur nom d'une célèbre légende utilisée par les Grecs pour conquérir la ville de Troie.

Comment s'en protéger ?

N'installez que des logiciels provenant de sources fiables.
Ne téléchargez jamais un logiciel qui vous est proposé gratuitement alors qu'il est normalement payant. Préférez les sites officiels des éditeurs. Utiliser de préférences des logiciels libres.
Enregistrez TOUJOURS le(s) fichier(s) et n'ouvrez JAMAIS le(s) fichier(s) en ligne (depuis une page Web).
Ne téléchargez du contenu que sur des sites Web de confiance : désactivez l'ouverture automatique des documents téléchargés et lancez une analyse antivirus avant d'ouvrir, afin de vérifier qu'ils ne sont pas infectés par un spyware ou virus. l'utilisation d'un antivirus peut s'avérer efficace, mais reste souvent insuffisante en cas de doute sérieux.
Ne connectez pas une clé USB sans être sûr de sa provenance.

Les sites marchands douteux

Les sites douteux existent. Boutiques en ligne en apparence, peuvent parfaitement plagier l'original. Alors prudence quand vous achetez en ligne : vos données de paiement ou mots de passe peuvent être récupérés par des attaquants.

Comment s'en protéger ?

Assurez-vous du sérieux du site marchand : il doit proposer des garanties de sécurité de paiement (nature des données bancaires demandées, chiffrement, possibilité de rétractation…).
Privilégiez les sites proposant l'envoi d'un code de transaction par SMS (type 3D secure).
Méfiez-vous des sites avec des fautes d'orthographe et proposant des offres trop alléchantes.
Vérifiez qu'un cadenas figure dans la barre d'adresse ou en bas à droite de la fenêtre de votre

navigateur Web.

Ne saisissez pas vos données de paiement ou mots de passe sur des sites web non sécurisés, c'est-à-dire ne commençant pas par https.

Les ransomwares

Les rançongiciels ou ransomware sont des programmes malveillants (WannaCry, Petya, Petrwrap, Locky, etc.), reçus par mail, dont le but est le chiffrement de vos données puis de vous demander d'envoyer de l'argent en bitcoins en échange de la clé (peut être) qui vous permettra de les décoder. (Nota : la plupart de ces malveillants attaquent uniquement **Windows**)

Comment s'en protéger ?

Sauvegardez régulièrement vos données sur un disque dur externe ou sur clef USB.
Mettez à jour régulièrement TOUS vos logiciels... Y compris votre antivirus et logiciels de sécurité !
N'ouvrez jamais les messages dont la provenance ou la forme est douteuse.
Méfiez-vous des extensions des fichiers douteuses (de type .scr ou .cab.).
Affichez **TOUJOURS** les extensions des fichiers sous Windows.

Les mots de passe

Pour voler les mots de passe, les malfaisants utilisent des logiciels qui génèrent un maximum de combinaisons possibles jusqu'à trouver le bon mot de passe. D'autres multiplient les essais d'après des informations obtenues sur les réseaux sociaux.

Comment faire ?

Oubliez le prénom de vos enfants ou de votre animal de compagnie comme mot de passe. Utilisez des mots de passe complexes contenant au moins 12 caractères (16 caractères est une bonne valeur) et 4 types différents : lettres majuscules, minuscules, chiffres et caractères spéciaux.
Changez de mot de passe pour chaque nouveau compte et renouvelez-les régulièrement.
Procurez-vous un anti-virus et un anti-spyware et mettez-les régulièrement à jour.
Éviter de stocker les mots de passe dans votre navigateur.

Pour stocker vos identifiants et mots de passe, vous pouvez, si vous le souhaitez, utiliser un gestionnaire de mots de passe : un seul mot de passe très robuste et vous accédez à tous vos comptes !
Pour information
- Les conseils de la CNIL pour un bon mot de passe https://www.cnil.fr/fr/les-conseils-de-la-cnil-pour-un-bon-mot-de-passe
- Vérifier si vous avez un compte mail qui a été compromis https://haveibeenpwned.com/
- Gestionnaire de mots de passe : on peut citer entre autres, parmi les logiciels libres régulièrement mis à jour : Keepass , dont la sécurité a été évaluée par l'Agence nationale de sécurité des systèmes d'information (ANSSI)

Crédits et sites Web d'information
Générateur de mot de passe et Tester vos mots de passe en ligne
Que faire en cas d'escroquerie ou de cyberattaque
Spam, phishing, arnaques : signaler pour agir
Escroquerie et cyber attaque : protégez-vous !
Les escroqueries et cyberattaques les plus fréquentes
La sécurité du numérique est à portée de clic !
Restreindre la collecte de données sous Windows 10
Sécuriser son ordiphone
Hoax: [hoks] nm, canular, gag (Fausses alertes aux virus, fausses chaînes de solidarité, fausses promesses, fausses informations ,,,
Pourquoi choisir Linux

Version originale du 23/10/2017
Document venant de http://normandietp.free.fr/ JC Etiemble