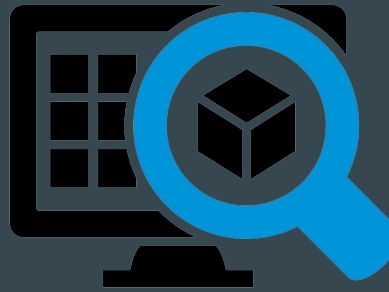
Les bonne pratiques du numérique

Hugo Boilly
Raphaël Berrichon

Téléchargez les versions officiels d’un logiciel (disponible sur le site de l’éditeur)

Si vous voulez télécharger des logiciels pour vos besoins personnels, vous vous dirigez sûrement vers des sites internet dont la page n’est pas celle de l’éditeur, et cela peut avoir de grandes répercussions sur l'appareil personnel et professionnel que vous utilisez.

Il est possible, par exemple, que certaines personnes malveillantes créent une « fausse » mise à jour pour vous induire en erreur et infecter votre ordinateur via des virus.



Comment éviter les risques:

De télécharger vos programmes sur les sites des éditeurs ou des sites de confiance.

De penser à désactiver toutes les cases proposant d'installer des logiciels complémentaires.

De rester vigilants concernant les liens sponsorisés et de faire attention avant de cliquer sur des liens.

De désactiver l'ouverture automatique des documents téléchargés et de lancer une analyse antivirus avant de les ouvrir.

Utilisez des mots de passe différents pour tous les services professionnels et personnels auxquels vous accédez

Si vous ne le faites pas et qu'un des services auquel vous accédez se fait pirater, le vol de votre mot de passe permettra à une personne malveillante d'accéder à tous vos autres services y compris les plus critiques (banque, messagerie, sites marchands, réseaux sociaux...).

Si vous utilisez ce même mot de passe pour accéder au système informatique de votre entreprise, c'est elle que vous mettez aussi en péril, car un cybercriminel pourrait utiliser vos identifiants de connexion pour voler ou détruire des informations.

Evitez les risques liées au mot de passe

De ne pas utiliser le même mot de passe pour tous les sites Web auxquels je me suis inscrit.

De changer régulièrement de mot de passe.

D’utiliser des mot de passe robuste, proposé par les navigateurs qui seront stocké dans un coffre-fort

Utilisez des gestionnaire de mot de passe comme par exemple Keepass

Utilisez des caractères spéciaux comme “@,!”

Faites les mise à jour de sécurité de vos équipement

Sur vos moyens informatiques personnels (ordinateur, téléphone, tablette), mais également sur vos moyens professionnels si cela relève de votre responsabilité, il est important d'installer sans tarder les mises à jour dès qu'elles sont publiées.

Elles corrigent souvent des failles de sécurité qui pourraient être exploitées par des cybercriminels pour prendre le contrôle de votre appareil et accéder à vos informations ou à celles de votre entreprise.

Evitez les risques

Vérifiez les mise à jour des équipement le plus souvent possible

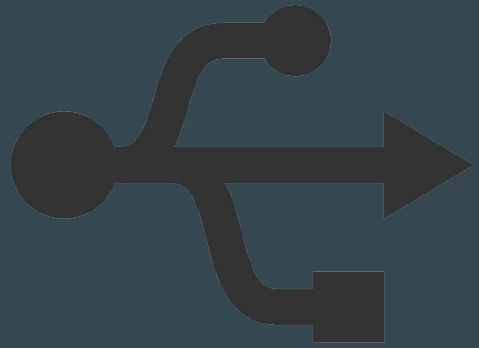
Se tenir au courant des failles présentes sur vos systèmes et des logiciels.

Faire les mise à jours sur les sites officiel de l’éditeur pour éviter les divers danger présent sur internet, qui sont principalement causées par des logiciel non défectueux

Méfiez vous des support USB

Si on vous donne ou que vous trouvez une clé USB. Dites vous que c'est un piège puisque cela peut vous engendrer de gros problème.

Ne la branchez jamais sur un de vos appareils informatique personnel ou même professionnel, ce qui risquerait de permettre à un utilisateur malveillant de compromettre toutes vos données personnelles et professionnelles.



Comment éviter les risques

N’utilisez pas votre clé USB personnelle sur votre lieu professionnel

Si vous recevez une clé USB, d’une personne inconnue ou même de confiance, ne l'acceptez pas et détruisez- la sans même regarder son contenu, ce qui pour infecter votre appareil ainsi que tous les autre appareil qui l’entoure

Utilisé des solutions contre les virus et tout autre type de menace

Sur vos moyens informatiques personnels (ordinateur, téléphone, tablette), mais également sur vos moyens professionnels si cela relève de votre responsabilité, utilisez une solution antivirus et tenez-la à jour.

Même si aucune solution n'est totalement infaillible, de nombreux produits peuvent vous aider à vous protéger des différentes attaques que peuvent subir vos équipements comme les virus, les rançongiciels (ransomware), l'hameçonnage (phishing)…

Si un cybercriminel prenait le contrôle de vos équipements personnels, il pourrait accéder à toutes vos informations, mais aussi au réseau de votre entreprise si vous vous y connectez avec ce matériel.

Comment éviter les risques liées aux virus

Installer des logiciels qui mettent à jour leur base de données sur les différents virus qui peuvent apparaître chaque jour.

Éviter d'utiliser des logiciels d’antivirus gratuit, ils ont moins d’avantage et une base de données très peu mise à jour ce qui avantage le cybercriminel.

Conclusion

Il est très important de s’informer sur les risques et les bonnes pratique sur internet

En espérant que votre lecture à était bonne.

Merci.