MINISTÈRE DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

Direction centrale de la sécurité publique
Direction départementale de la sécurité publique de Seine-et-Marne

Circonscription d'Agglomération de Melun Val de Seine

POLICE NATIONALE

La Police Nationale vous informe:

Commerçants, P.M.E., particuliers:

Les 10 mesures essentielles pour assurer votre cybersécurité

Que ce soit dans un cadre professionnel ou personnel, l'utilisation des outils numériques ne cesse de croître et de se diversifier. Ordinateurs de bureau ou portables, téléphones mobiles, tablettes, objets connectés… Ils font de plus en plus partie de notre quotidien. Cette intensification des usages représente pour les cybercriminels une opportunité de développer leurs attaques. Comment se protéger au mieux face à ces risques ? Voici 10 bonnes pratiques essentielles à adopter pour assurer votre cybersécurité.

1. Protégez vos accès avec des mots de passe solides

Utilisez des mots de passe suffisamment longs, complexes et différents sur tous les équipements et services auxquels vous accédez, qu'ils soient personnels ou professionnels. La majorité des attaques est souvent due à des mots de passe trop simples ou réutilisés. Au moindre doute changez les, et régulièrement en prévention, changez-les tous les six mois. Utilisez un gestionnaire de mots de passe et activez la double authentification chaque fois que c'est possible pour renforcer votre sécurité. Choisissez des mots de passe à douze caractères, comportant des majuscules, des minuscules, des chiffres et des caractères spéciaux. Ces derniers ne doient avoir aucun lien avec vous ou votre famille.

2. Sauvegardez vos données régulièrement

En cas de piratage, mais également en cas de panne, de vol ou de perte de votre appareil, la sauvegarde est souvent le seul moyen de retrouver vos données (photos, fichiers, contacts, messages…). Sauvegardez régulièrement les données de vos PC, téléphones portables, tablettes et conservez toujours une copie de vos sauvegardes sur un support externe à votre équipement (clé ou disque USB) que vous débranchez une fois la sauvegarde effectuée.

3. Appliquez les mises à jour de sécurité sur tous vos appareils (PC, tablettes, téléphones…), et ce, dès qu'elles vous sont proposées

Vous corrigez ainsi les failles de sécurité qui pourraient être utilisées par des pirates pour s'introduire dans vos appareils, pour y dérober vos informations personnelles ou vos mots de passe, voire pour détruire vos données ou encore vous espionner

4. Utilisez un antivirus

Les antivirus permettent de se protéger d'une grande majorité d'attaques et de virus connus. Il existe de nombreuses solutions gratuites ou payantes selon vos usages et le niveau de protection ou de services recherchés. Vérifiez régulièrement que les antivirus de vos équipements sont bien à jour et faites des analyses (scans) approfondies pour vérifier que vous n'avez pas été infecté.

5. Téléchargez vos applications uniquement sur les sites officiels

N'installez des applications que depuis les sites ou magasins officiels des éditeurs (exemple : Apple App Store, Google Play Store) pour limiter les risques d'installation d'une application piégée pour pirater vos équipements. De même, évitez les sites Internet suspects ou frauduleux (téléchargement, vidéo, streaming illégaux) qui pourraient également installer un virus sur vos matériels.

6. Méfiez-vous des messages inattendus

En cas de réception d'un message inattendu ou alarmiste par messagerie (*email)*, SMS ou chat, demandez toujours confirmation à l'émetteur par un autre moyen s'il vous semble connu et légitime. Il peut en effet s'agir d'une attaque par **hameçonnage (*phishing*)** visant à vous piéger pour vous dérober des informations confidentielles (mots de passe, informations d'identité ou bancaires), de l'envoi d'un virus contenu dans une pièce-jointe qu'on vous incite à ouvrir, ou d'un lien qui vous attirerait sur un site malveillant.

7. Vérifiez les sites sur lesquels vous faites des achats

Si le commerce en ligne facilite les achats et offre l'opportunité de faire de bonnes affaires, il existe malheureusement de nombreux sites de vente douteux, voire malveillants. Avant d'acheter sur Internet, vérifiez que vous n'êtes pas sur une copie frauduleuse d'un site officiel, la crédibilité de l'offre et consultez les avis. Sans cette vérification, vous prenez le risque de vous faire dérober votre numéro de carte bancaire et de ne jamais recevoir votre commande, voire de recevoir une contrefaçon ou un produit dangereux.

8. Maîtrisez vos réseaux sociaux

Les réseaux sociaux sont de formidables outils de communication et d'information collaboratifs. Ils contiennent toutefois souvent de nombreuses informations personnelles qui ne doivent pas tomber dans de mauvaises mains. Sécurisez l'accès à vos réseaux sociaux avec un mot de passe solide et unique, définissez les autorisations sur vos informations et publications pour qu'elles ne soient pas inconsidérément publiques ou utilisées pour vous nuire, ne relayez pas d'informations non vérifiées (*fake news*)

9. Séparez vos usages personnels et professionnels

Avec l'accroissement des usages numériques, la frontière entre utilisation personnelle et professionnelle est souvent ténue. Ces utilisations peuvent même parfois s'imbriquer. Matériels, messageries, «clouds»… Il est important de séparer vos usages afin que le piratage d'un accès personnel ne puisse pas nuire à votre entreprise, ou inversement, que la compromission de votre entreprise ne puisse pas avoir d'impact sur la sécurité de vos données personnelles

10. Évitez les réseaux WiFi publics ou inconnus

En mobilité, privilégiez la connexion de votre abonnement téléphonique (3G ou 4G) aux réseaux WiFi publics. Ces réseaux WiFi sont souvent mal sécurisés, et peuvent être contrôlés ou usurpés par des pirates qui pourraient ainsi voir passer et capturer vos informations personnelles ou confidentielles (mots de passe, numéro de carte bancaire…). Si vous n'avez d'autre choix que d'utiliser un WiFi public, veillez à ne jamais y réaliser d'opérations sensibles et utilisez si possible un réseau privé virtuel (VPN).

Informations : **Cybermalveillance.gouv.fr**

NOTA: Dès que nécessaire, en cas d'e-escroquerie, déposez plainte en ligne facilement et rapidement grâce à la plateforme THESEE. (**Traitement harmonisé des enquêtes et signalements pour e-escroqueries**) Rendez-vous sur le site **service-public.fr** rubrique « arnaques sur internet » et laissez vous guider.
Les informations que vous communiquez sont analysées et recoupées par des experts de la Police Judiciaire qui mènent l'enquête.

Développer une culture de la cybersécurité devient nécessaire

Pour remédier à ces failles, il est nécessaire de «*développer une culture de la cybersécurité à l'échelle globale*», estime de nombreux spécialistes.

Afin d'opérer un changement de mentalité**, il faut notamment développer de bonnes pratiques le plus tôt possible.** Elle prend pour exemple l'usage d'un mot de passe différent pour chaque compte, ce que seulement 50% des salariés font au travail.

De bonnes pratiques qui doivent s'accompagner *de sensibilisation dans les entreprises, les collectivités*» et d'une «*généralisation de la communication*» sur les bons réflexes à avoir.

Cet enjeu demeure «*majeur*», il faut *considérer l'investissement dans la cybersécurité comme une épargne plutôt que comme un coût*»,

En 2021, l'autorité nationale en matière de sécurité et de défense des systèmes d'information (ANSSI) relevait 1082 intrusions avérées dans des systèmes d'information. Une hausse de 37% par rapport à 2020.