10 POINTS CLÉS POUR ÉVITER UNE CYBERATTAQUE : RAPPEL DES PRÉCAUTIONS D'USAGE

Faire des sauvegardes

Effectuez régulièrement une copie de secours (ou back-up) des données et informations importantes. Conservez ce back-up dans un endroit sûr et veillez à ce qu'il soit toujours déconnecté du réseau. Gardez également sur un ordinateur qui n'est pas connecté au réseau ou sur papier les informations utiles, telles que les adresses e-mail et numéros de téléphone importants, ou encore les informations sur votre fournisseur d'accès à Internet.

Mettre à jour les logiciels et les antivirus de votre ordinateur

Vous pouvez configurer votre ordinateur pour que le système d'exploitation procède automatiquement et régulièrement à une mise à jour de tous vos logiciels avec les derniers correctifs de sécurité. Effectuez des sauvegardes régulières de votre système afin de pouvoir le restaurer. Mettez à jour régulièrement vos logiciels et téléchargez les programmes uniquement sur les sites officiels des éditeurs.

Protéger votre smartphone avec un antivirus, surtout si vous le synchronisez avec votre ordinateur

Être vigilant avec les expéditeurs vos emails

Vérifier la cohérence entre l'expéditeur présumé et le contenu du message. En cas de doute sur l'émetteur : N'ouvrez pas la pièce jointe, ne cliquez pas sur les liens web. Attention : ce n'est pas parce que l'adresse de l'expéditeur est connue qu'elle n'est pas usurpée. Ne répondez jamais par courriel à une demande d'informations personnelles ou confidentielles.

Utiliser des mots de passe forts et variés

Idéalement votre mot de passe doit être de 12 caractères minimum. Il doit comprendre des caractères de type différent (majuscules, minuscules, chiffres, caractères spéciaux), ne pas être en lien avec vos informations personnelles (noms, dates de naissance,...) et ne pas être utilisé pour différents accès.

Être vigilant les paiements en ligne

Vérifiez que le site de paiement a bien un accès https. Préférez les méthodes de paiement impliquant la réception d'un code de confirmation par sms. Ne répondez jamais à un email vous demandant de renvoyer vos informations bancaires.

Protéger les informations des postes de travail en entreprise

Naviguez jamais sur internet sur la session administrateur. Sécurisez l'accès wi-fi de l'entreprise et désactivez-le lorsqu'il n'est pas utilisé. Eteignez les ordinateurs pendant les périodes d'inactivité, nuits, week-end, vacances.
Lors de vos déplacements : désactivez les fonctions wi-fi ou bluethooth, ne laissez pas vos appareils sans surveillance dans votre hôtel par exemple. Signalez la perte ou le vol d'un matériel informatique appartenant à l'entreprise

Cartographier et surveiller l'ensemble de l'infrastructure et des réseaux

Séparer les usages personnels des usages professionnels

Source ANSSI : www.gouv.fr/en-cas-d'incident

Réalisé par ATIXNET
2 bis avenue Foch 94160 Saint-Mandé - TEL. 01 84 23 00 60 – www.atixnet.fr