Jeune Chambre Economique
de Haguenau - Alsace du Nord
Le Mouvement des Jeunes Citoyens Entreprenants

SÉCURITÉ INFORMATIQUE : 6 REFLEXES A ADOPTER

« Lorsque deux forces sont jointes, leur efficacité est double »

Isaac Newton

La sécurité informatique est l'affaire de tous, vu l'augmentation importante des cyberattaques contre les entreprises, tout le monde a son rôle à jouer !

Nous vous invitons à adopter ces 6 réflexes pour assurer votre sécurité :

1. GARANTIR LA CONFIDENTIALITÉ

Sécuriser les échanges de données

Si un appareil personnel *(USB, tablette, téléphone...)* est branché sur le matériel professionnel, celui-ci doit être mis à jour, passé au contrôle de l'antivirus et sécurisé par un mot de passe.

Utiliser des mots de passe robustes

Renforcer les mots de passe :

- Minimum 8 caractères
- Mots n'existant pas dans le dictionnaire
- Utilisation de caractères spéciaux et de chiffres

Astuce : utilisez une phrase pour vous en souvenir
Ex : Le soleil c'est chaud devient [Lsc'ec]

Ne jamais stocker ses mots de passe de façon accessible et ne pas les communiquer.
N'utilisez pas l'option « mémorisez vos mots de passe ».
Ne communiquez à personne vos mots de passe.

Conseil : utilisez un gestionnaire de mot de passe sécurité

Ne pas divulguer les informations sensibles

Ne parlez jamais des données personnelles des clients ou procédures internes avec des tiers non autorisés.

Ne donnez jamais la possibilité à un tiers non autorisé de visualiser vos documents de travail, utilisez un filtre de confidentialité par exemple.

Verrouillez les ordinateurs dès que vous n'êtes pas à votre poste.

Mettez en place une procédure pour gérer le départ des collaborateurs et supprimer leurs accès.

3. ETRE VIGILANT SUR INTERNET

- Privilégiez des navigateurs internet récents et utilisez les versions les plus à jour
- Assurez-vous que sur le site interne le protocole HTTPS soit utilisé (présence d'une icône de cadenas vert à côté du nom du site)
- En cas de doute, ne cliquez pas !
- Méfiez-vous des offres trop alléchantes

2. UTILISER DES BOUCLIERS (ANTI-VIRUS, ANTI-SPYWARE, PARE-FEU, etc)

- Ayez un anti-virus et un anti spam actif en permanence
- Inspectez systématiquement le contenu des clés USB et fichiers téléchargés

Adoptez des mesures préventives :

- n'utilisez jamais une clé USB "abandonnée" ou dont vous ne connaissez pas l'origine
- avant toute utilisation, scannez et nettoyez la clé USB
- bloquez la fonction "Autorun"
- affectez une clé par usage
- chiffrez le contenu de vos clés USB.

- Vérifiez que les systèmes sont régulièrement mis à jour

4. ETRE VIGILANT EN RECEVANT DES EMAILS

- Soyez vigilant lorsque vous ne connaissez pas l'émetteur du mail
- Si le courrier n'a pas la même forme qu'habituellement, s'il a beaucoup de faute ou que ce n'est pas la même adresse qu'habituellement : ne pas l'ouvrir et prendre contact directement avec l'interlocuteur concerné
- Sauf à être certain de l'échange, ne pas saisir ses coordonnées bancaires par mail ou sur un site internet.
- En cas de doute ne jamais ouvrir la pièce jointe.

Nos partenaires :
LEVY • GEISSMANN & ASSOCIES
WWW.LGASSOCIES.COM
http://www.tsi-informatique.fr

5. ANTICIPER LA PERTE DES DONNEES

- Ayez une stratégie rigoureuse de sauvegarde

Raisonnez par priorité et protégez les informations les plus sensibles.

Isolez informatiquement et physiquement le lieu de stockage des fichiers de sauvegarde

Multipliez les sauvegardes et vérifiez régulièrement qu'elles fonctionnent

- Prenez des précautions dans l'utilisation des supports

Vérifiez l'intégrité du support de sauvegarde

Veillez à la confidentialité des données sensibles en rendant leur lecture impossible à des personnes non autorisées

- Soyez vigilant en prenant connaissance des conditions générales d'utilisation des services

6. RENFORCER LES PROCEDURES INTERNES

- Organisez des réunions d'informations pour alerter les collaborateurs sur les nouveaux types de menaces, sensibilisez, informez, avertissez les collaborateurs via des mesures de bons sens.
- Mettre en place des procédures pour prévenir les attaques

Exemples :

- en cas de demande de modification de RIB fournisseur prévoir une validation ou un contre-appel vers un numéro préalablement référencé
- pour les demandes de virement / déblocages de fonds prévoir une procédure spécifique uniquement connu en interne

- Procédez à des simulations pour tester la vigilance des collaborateurs
- Ne payez jamais les rançons demandées en cas d'attaque virus

COMMENT REAGIR EN CAS D'ATTAQUE ?

Adoptez une méthodologie de traitement du risque au jour de l'attaque

- Débranchez immédiatement votre ordinateur du réseau (câble Ethernet) et coupez votre wifi.
- Arrêtez d'utiliser l'équipement corrompu afin de ne pas effacer les preuves.
- Signalez l'attaque au service informatique ou au prestataire dans les plus brefs délais afin qu'il puisse intervenir pour évaluer les dommages et limiter les conséquences.
- Signalez l'attaque simultanément et portez plainte auprès de la gendarmerie ou de la police nationale.
- En cas de *ransomware* : ne payez pas la rançon.
- Procédez à une analyse complète par l'antivirus, si cette étape n'est pas concluante, il faudra alors procéder au formatage (effacement de toutes les données) du disque dur.
- Lancez la restauration des données à partir d'une sauvegarde.
- Établissez un plan de communication en cas de crise suite à une cyberattaque grave.

Contactez les structures d'assistance aux victimes de cyberattaques

- ACYMA : plateforme d'assitance aux victimes d'actes de cybermalveillance. Grâce à ses réponses au questionnaire, la victime est orientée vers les prestataires de proximité susceptibles de répondre à son besoin technique.
- CERT : centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques.
- Cybermalveillance.gouv.fr : plateforme d'assitance du risque numérique mise en place par l'ANSSI.
- Stopransomware (réseau Cecyf prévention).