laboutic.fr
fiche pratique

COMMENT SE PROTÉGER CONTRE LES CYBERATTAQUES ?

Pourquoi se protéger ?

- **Renvoyer une bonne image à vos clients**
- **Conserver votre trésorerie intacte**
- **Investir du temps dans votre métier**

Les fondamentaux

Les PME courent le plus grand risque de cyberattaques car elles sont souvent plus vulnérables. En effet, 60% des petites entreprises cessent leur activité dans les 6 mois suivant une attaque malveillante. D'où l'intérêt de mettre en place de bonnes pratiques pour s'en protéger.

Par où commencer ?

1. Adopter une politique de mot de passe rigoureuse.
2. Etre vigilant sur les liens ou les pièces jointes contenus dans les messages électroniques.
3. Sauvegarder ses données régulièrement sur 3 supports différents.
4. Faire ses mises à jour régulièrement sur ses appareils (ordinateur, téléphone et tablette).
5. Se protéger des virus et autres logiciels malveillants.
6. Contrôler les permissions des comptes utilisateurs lorsque vous travaillez sur le même poste, serveur ou logiciel.

Avant d'aller plus loin...

Vous souhaitez plus de conseils sur la sécurisation de vos mots de passe en 10 points, il suffit de consulter la fiche adaptée :

Voir la fiche pratique : sécuriser-vos-mots-de-passe.pdf (laboutic.fr)

laboutic.fr
fiche pratique

6 attaques à gérer facilement

Encore aujourd'hui, les entreprises doivent s'adapter pour ne pas être victime de cyberattaques, sachant que 50% des logiciels malveillants proviennent du courrier électronique.

1

Face au vol de mot de passe

Utilisez un mot de passe différent pour chaque accès, à conserver dans un gestionnaire de mots de passe. Fortifiez celui de votre messagerie qui contient tous les liens de vos autres comptes.

Recommandation :
10 à 14 caractères avec des minuscules, majuscules, chiffres et caractères spéciaux.

2

Contre l'hameçonnage ou le phishing

Lors de la réception de mails avec un lien, positionnez le curseur de la souris pour vérifier son nom et celui de l'expéditeur. Faites attention aux fautes d'orthographe, aux mails alarmants et à leur objet. Pareil pour l'adresse des sites Web.

Recommandation :
Un doute : contacter l'organisme concerné.

3

Panne, perte et vol de données

Faites des sauvegardes régulières de vos données en les stockant sur une clé USB ou un disque dur chiffrés, sur un stockage en ligne (cloud) et sur votre ordinateur.

Recommandation :
N'attendez pas d'être victime pour mettre en place cette routine.

4

Face aux attaques numériques

Faites des mises à jour manuelles ou automatiques, régulièrement, pour que vos logiciels soient performants. Téléchargez les mises à jour sur les sites officiels et vérifiez leur URL.

Recommandation :
Anticipez la durée des mises à jour le matin ou le soir.

5

Se protéger des virus et logiciels malveillants

Utilisez un pare-feu et un antivirus pour analyser vos appareils. N'utilisez jamais un équipement inconnu ou perdu, chiffrez le contenu de vos appareils et attribuez un usage différent pour chaque clé USB.

Recommandation :
Ver, Cheval de Trois et Spyware doivent être repérés rapidement pour les éliminer.

6

Diviser les risques d'attaques

Donner des permissions utilisateurs différentes selon les besoins et fonctions des collaborateurs, pour assurer un niveau d'accès limité au système d'exploitation. Personnalisez les attributions et séparez le privé du professionnel sur les machines.

Recommandation :
La double authentification limite les risques.

Besoin d'un conseil, d'un accompagnement… contactez votre conseiller local

CHAMBRE DE COMMERCE ET D'INDUSTRIE

CONNAITRE LE VOCABULAIRE DE LA CYBERSÉCURITÉ

laboutic.fr fiche pratique

Un peu de vocabulaire

Les termes techniques à retenir :

- **Antivirus :** logiciel qui détecte les virus et les élimine.
- **Cyberattaque :** attaque de pirates informatiques sur internet qui volent des données.
- **Gestionnaire de mots de passe :** logiciel qui stocke tous les mots de passe à un seul endroit.
- **Hameçonnage (phishing) :** technique de fraude dans le but d'inciter une personne qui reçoit un mail ou SMS à donner des informations personnelles ou bancaires.
- **Logiciel malveillant (malware) :** logiciel qui nuit à la sécurité de l'ordinateur et de ses données.
  - ◊ **Cheval de Troie :** qui créé une faille de sécurité pour que le pirate accède aux données.
  - ◊ **Spyware :** logiciel espion qui regarde le contenu de l'ordinateur à l'insu de son propriétaire.
  - ◊ **Ver :** contenu souvent dans la pièce jointe d'un mail, il ralentit l'ordinateur ou l'endommage.
- **Pare-feu :** logiciel de sécurité qui contrôle le trafic entrant et sortant de l'ordinateur.
- **Serveur :** Ordinateur ou système qui héberge des ressources, données, services et logiciels.
- **Stockage en ligne (cloud ou nuage) :** moyen en ligne de sauvegarder une copie des ses données dans un serveur à distance.
- **Virus :** petit programme codé qui infecte l'ordinateur et l'endommage.

Pour aller plus loin ...

Vous souhaitez plus de conseils sur la manière de se prémunir des cyberattaques et comprendre davantage la cybermalveillance :

Voir la fiche pratique : se-prémunir-des-cyberattaques.pdf (laboutic.fr)

Boite à outils

Gestionnaires de mots de passe :

- LockPass
- Dashlane
- Bitwarden

Logiciels de chiffrage :

- BitLocker pour Window
- FileVault pour MacOs
- Luks pour Linux

Stockage en ligne (cloud) :

- LockFiles
- Google Drive
- One Drive

Besoin d'un conseil, d'un accompagnement... contactez votre conseiller local

CHAMBRE DE COMMERCE ET D'INDUSTRIE