Mini-Guide de Sensibilisation à la Cybersécurité en Entreprise

Pourquoi la cybersécurité est essentielle

La cybersécurité protège les données et les systèmes informatiques contre les cybermenaces. En entreprise, une faille peut compromettre la confidentialité, la réputation et même la pérennité d'une organisation.

1. Sécurité sur Internet et déplacements professionnels

- Les dangers sur Internet :
  -Sites frauduleux et malwares
  -Phishing (usurpation d'identité via email)
  -Failles de sécurité sur les réseaux Wi-Fi publics

- Bonnes pratiques :
  -Vérifier que les sites web sont sécurisés (HTTPS)
  -Ne jamais cliquer sur des liens douteux dans les emails
  -Utiliser un VPN lors des connexions en déplacement
  -Activer l'authentification à deux facteurs sur les comptes professionnels

2. Sécurité des mots de passe et authentification

- Les risques liés aux mots de passe faibles :
  -Piratage de comptes
  -Attaques par force brute
  -Réutilisation du mot de passe sur plusieurs services

- Bonnes pratiques :
  -Utiliser un mot de passe long et complexe (>12 caractères)
  -Ne jamais utiliser d'informations personnelles (date de naissance, prénom…)
  -Utiliser un gestionnaire de mots de passe sécurisé (Bitwarden, KeePass)
  -Activer la double authentification pour les accès sensibles

3. Sécurité des e-mails

- Menaces courantes :
  -Pièces jointes infectées (ransomware, virus)

-Liens de phishing menant à des sites frauduleux
-Usurpation d'identité via emails frauduleux

- Bonnes pratiques :
  -Vérifier l'expéditeur avant d'ouvrir un email
  -Se méfier des messages urgents ou des demandes de paiement inattendues
  -Ne jamais télécharger une pièce jointe suspecte
  -Signaler les emails douteux à la cellule de sécurité informatique

4. Phishing, ransomware et séparation des usages

- Attaque de phishing :
  -Technique utilisée pour voler des identifiants via un faux email
  -Exemple : Un message imitant la banque demandant une vérification de compte

- Fonctionnement d'un ransomware et conséquences :
  -Un logiciel chiffre toutes les données et exige une rançon
  -Impact : Perte des fichiers, blocage du réseau, impact financier

- Bonnes pratiques :
  -Se méfier des emails demandant une action immédiate
  -Sauvegarder régulièrement les données sur un support sécurisé
  -Séparer les usages professionnels et personnels sur les appareils

Que faire en cas d'incident

- Si vous recevez un email frauduleux, ne cliquez pas et signalez à l'équipe IT
- Si votre poste est infecté, déconnectez-le du réseau et contactez la sécurité
- Si vous avez un doute sur une demande de transfert de données, vérifiez la légitimité avant d'agir

Conclusion

La cybersécurité est l'affaire de tous.

- Appliquez ces bonnes pratiques au quotidien
- Soyez vigilants face aux tentatives de fraude
- Sensibilisez vos collègues pour renforcer la sécurité collective

En sécurisant nos outils et nos comportements, nous protégeons l'entreprise et nos données.