sosafe

Cyberattaques et attaques phishing

Ce que vous avez besoin de savoir

LE SAVIEZ-VOUS ?

Phishing : action visant à « pêcher » (« to fish », en anglais), ou dérober des informations sensibles telles que des données d'accès, des informations de paiement et les secrets professionnels par le biais d'e-mails frauduleux, de sites Internet, de messages ou d'appels téléphoniques.

1 utilisateur sur 3

clique sur le contenu malveillant des e-mails de phishing.

#1

№ 1

Les cyberincidents constituent le risque № 1 pour les entreprises.

4,35 millions de dollars

Coût moyen d'une attaque par rançongiciel pour une société, hors rançon.

À savoir

- Votre adresse e-mail et celles de vos collègues peuvent être copiées ou falsifiées en quelques secondes.
- Un lien peut vous rediriger vers une destination complètement différente de ce qu'il indiquait a priori. Soyez vigilants!
- Un seul clic suffit pour infecter votre ordinateur ou le réseau de votre société.

Protection

- Vérifiez que l'adresse de l'expéditeur est authentique en plaçant votre curseur sur le nom de l'expéditeur et relevez tout ce qui peut paraître suspect (p. ex. une adresse de réponse).
- Avant de cliquer sur un lien, passez votre curseur dessus et contrôlez l'URL cible dans votre navigateur/logiciel de messagerie.
- Les e-mails de phishing contiennent souvent des pièces jointes dangereuses. Si vous n'attendez pas de fichier, ne cliquez pas sur les pièces jointes. Des formats de fichiers courants (.docx, .pdf, etc.) peuvent cacher des virus.