Check-list
E-mails d’hameçonnage (phishing)

GENERALI

Voici comment protéger vos données personnelles

Les e-mails provenant d’escrocs qui souhaitent obtenir vos données personnelles tels que les accès à vos comptes, mots de passe et codes PIN ont souvent l’air authentiques. Mais avec un peu de prudence et en sachant à quoi faire attention, il est souvent possible de reconnaître les e-mails d’hameçonnage envoyés par des criminels.

1. Soyez particulièrement prudent avec les e-mails que vous n’attendiez pas.
2. Dans les e-mails d’hameçonnage, on vous demande de nommer, en lien avec vos comptes, des données confidentielles telles que des mots de passe, des codes TAN ou PIN ainsi que des numéros de client ou de connexion.
3. L’e-mail contient des polices et des tailles d’écriture différentes.
4. L’e-mail présente des fautes de grammaire et d’orthographe.
5. Les trémas et accents ne sont pas écrits correctement ou manquent complètement.
6. L’entête est impersonnel (Cher client de l’établissement financier ABC).
7. La formule de salutations est impersonnelle (Votre banque ABC).
8. Un e-mail d’hameçonnage ne vous est pas adressé personnellement, il est envoyé par exemple à une adresse collective (clients@banque-abc.ch).
9. On vous menace dans l’e-mail (par exemple de fermeture de compte).
10. L’e-mail contient un formulaire ou un lien vers un formulaire dans lequel vous devez entrer des données personnelles telles que des codes PIN ou TAN, votre numéro de compte, vos numéros de client et de connexion.
11. L’e-mail contient un lien qui a l’air vrai au premier coup d’œil. Certains éléments de l’URL écrits de façon inhabituelle ou fausse montrent cependant qu’il s’agit d’une fausse adresse Internet.

Quelques points auxquels vous devriez encore être attentif :

Pour vous connecter aux sites d’établissements financiers, n’utilisez jamais un lien qui vous a été envoyé par e-mail ou qui doit être scanné par QR-Code.

Entrez toujours manuellement l’adresse de la page de connexion de votre établissement financier.

Ne remplissez aucun formulaire vous ayant été envoyé par e-mail et vous demandant d’indiquer des données de connexion.

Ne donnez aucune information confidentielle lors d’échanges téléphoniques.