Techniques frauduleuses : les bonnes pratiques pour lutter contre l'hameçonnage

Phishing

Du 29 octobre 2024 au 30 décembre 2024

L’hameçonnage (phishing en anglais) est une technique frauduleuse destinée à leurrer l’internaute pour l’inciter à communiquer des données personnelles (comptes d’accès, mots de passe, etc) et/ou bancaires en se faisant passer pour un tiers de confiance.

Il peut s’agir d’un faux message, SMS ou appel téléphonique soi-disant de banque, de réseau social, d’opérateur de téléphonie, de fournisseur d’énergie, de site de commerce en ligne, d'administrations, de service informatique, etc.

Voici 4 bonnes pratiques pour ne pas être victime d’hameçonnage :

1. **Avant de cliquer sur un lien douteux**, positionnez le curseur de votre souris sur ce lien (sans cliquer) :
   - l’adresse du site vers laquelle le lien pointe réellement s’affichera. Vous pourrez ainsi vérifier la vraisemblance de cette adresse ;
   - en cas de doute, contactez si possible directement l’organisme concerné pour confirmer le message que vous avez reçu.
2. Si vous devez communiquer des informations sensibles sur un site internet, **vérifiez l’adresse du site qui s’affiche dans votre navigateur.**
3. Si l’adresse du site affichée dans la barre d’adresse du navigateur ne correspond pas exactement au site concerné, c’est très certainement un site frauduleux. Parfois, un seul caractère peut changer dans l’adresse du site pour vous tromper. Au moindre doute, ne fournissez aucune information et fermez immédiatement la page correspondante. Si vous allez régulièrement sur le site, préférez l’accès au site via vos favoris.
4. **Utilisez des mots de passes différents et complexes pour chaque site et application**
   Ainsi, le vol d’un de vos mots de passe ne compromet pas tous vos comptes personnels. Vous pouvez également utiliser des coffres forts numériques pour stocker de manière sécurisée vos différents mots de passe.

Source : cybermalveillance.gouv.fr