Arnaques très diversifiées Les escrocs de plus en plus inventifs !

Hameçonnage par usurpation d'identité

Un courriel à l'entête de votre banque vous signale un problème sur votre compte et vous propose de le régler en cliquant sur un lien contenu dans le message. Vous voilà sur la page de connexion de votre espace bancaire. Vous entrez en toute confiance vos identifiants. Problème : ce site est en fait une copie créée par des pirates. Et vous vous apercevez vite , mais trop tard, que des virements ont été passés vers des comptes basés à l'étranger, ou que votre carte bancaire a été utilisée pour des achats en ligne.

Détournement par des escrocs du code d'authentification

Vous faites un achat sur Internet ; le fournisseur doit vous envoyer un code d'authentification par SMS pour valider l'achat. Vous attendez ce code, votre téléphone en main. Enfin il arrive ! Vous notez bien ce code reçu par SMS sur votre site d'achat . Sauf qu'une minute après, vous recevez un deuxième SMS. Et cette fois c'est le bon, mais trop tard ! Votre versement à bien été fait, mais sur un compte basé à Abu Dabi où ailleurs.

Phishing aux impôts

Vous recevez un courriel de la Direction Générale des Finances Publiques (DGFIP) vous invitant à cliquer sur un lien pour accéder à votre dossier personnel au prétexte d'un remboursement d'impôts. Le site ressemble à s'y méprendre au site officiel. Et pourtant c'est un faux ; vous êtes victime d'un hameçonnage. Et les ennuis commencent !

Comment les éviter ? Quelles précautions prendre ?

- Ne communiquez jamais votre code confidentiel,
- Saisissez vous-même les données de votre carte à chaque paiement : ne les enregistrez pas dans votre compte client sur le site marchand,
- Vérifiez que le site sur lequel vous payez est sécurisé (un petit cadenas apparaît en bas de page),
- Conservez toujours la confirmation du montant, de la date et la référence de l'opération,
- Utilisez des mots de passe différents et complexes pour chaque site et application,
- Sachez qu'aucune administration ou société commerciale sérieuse ne vous demandera vos données bancaires ou vos mots de passe par message électronique ou par téléphone. Même chose pour le paiement d'un impôt ou le remboursement d'un crédit d'impôt, pas plus que pour compléter vos données personnelles.

Si vous êtes victime

Si vous avez malencontreusement communiqué des éléments sur vos moyens de paiement ou si vous avez constaté des débits frauduleux sur votre compte : **FAITES OPPOSITION IMMÉDIATEMENT** auprès de votre organisme bancaire ou financier et déposez plainte au commissariat de police ou à la gendarmerie la plus proche.
Si vous avez constaté que des éléments personnels servent à usurper votre identité, **DÉPOSEZ PLAINTE** au commissariat de police ou à la gendarmerie la plus proche.

Si vous êtes victime d'une usurpation de votre adresse de messagerie ou de tout autre compte, **CHANGEZ IMMÉDIATEMENT VOS MOTS DE PASSE.**
Vous devez déclarer l'arnaque immédiatement sur **Perceval** (plateforme gouvernementale dédiée aux détournements de CB).

Vous pouvez bien sûr venir nous voir à nos permanences. Nous pourrons certainement vous aider à faire les démarches nécessaires.

Pour en savoir plus sur vos droits et conseils sur les fraudes à la carte bancaire, ***voir le site de l'uFC-Que Choisir***