Bulletin d'information sur diverses fraudes modernes

À une époque où toutes les informations sont rassemblées sur la même toile, les pirates informatiques (hackers) s'en donnent à cœur joie.

Exploitant les failles humaines avec finesse et psychologie, ils piochent dans notre bonté innée, notre crédulité ou bien notre sensation de solitude pour s'en mettre plein les poches.

Ce bulletin a pour objectif de vous prémunir contre ces abus de confiance en connaissant les techniques de piratage les plus répandues.

Hameçonnage (phishing)

Technique destinée à leurrer l'internaute pour l'inciter à communiquer des données personnelles (comptes d'accès, mots de passe...) et/ou bancaires en se faisant passer pour un tiers de confiance.
Il peut s'agir d'un faux message, SMS ou appel téléphonique de banque, de réseau social, d'opérateur de téléphonie, de fournisseur d'énergie, de site de commerce en ligne, d'administrations, etc...

Aucun salarié/employé n'a le droit de vous demander vos données personnelles ou bancaires à distance lorsqu'il vous démarche. Les seules exceptions seront quand vous êtes à l'initiative de l'appel et encore, vous pouvez refuser de donner ces informations et poursuivre la démarche en présentiel.

Escroqueries au chèque bancaire

Le pirate va utiliser des chèques volés, fabriqués ou simplement falsifier les informations (destinataire, montant).
Il essaiera d'utiliser des personnes tierces pour encaisser ces chèques à leur place en échange d'une promesse d'argent ou en se faisant passer pour un proche en détresse.

Arnaques au CPF

Vous recevez un appel téléphonique, un mail ou un sms, d'une personne prétendant appartenir à la plateforme "Mon compte formation" ou à un autre organisme ; la personne vous demande votre numéro de sécurité sociale pour accéder à votre compte formation, le but étant de vous dérober vos crédits CPF.

Arnaques aux achats en ligne

Une offre trop belle pour être vraie ? Un compte à rebours pour vous donner l'impression de passer à côté de l'affaire du siècle ? Méfiance ! Demandez-vous pourquoi un parfait étranger aurait envie de vous rendre service sur internet.

Si ça brille et vous flatte, il est probable que ça soit faux.

Dropshipping

Les hackers créent des sites sur lesquels, ils promeuvent des produits donnés exactement comme dans le dropshipping. La différence est qu'ils ne disposent ni de stock, ni de fournisseur. Les offres sont souvent très alléchantes, ce qui peut permettre de détecter l'arnaque.

Vol de coordonnées bancaires

En consultant votre compte bancaire, vous découvrez des opérations réalisées à votre insu avec les références de votre carte bancaire que vous avez toujours en votre possession.

Cela signifie que vos coordonnées bancaires ont été volées, contactez votre banque au plus vite.

Faux ordres de virement

Les groupes criminels organisés usurpent l'identité de sociétés et incitent leurs clients à réaliser des paiements sur des comptes bancaires français ou étrangers en déclarant, par exemple, avoir changé de coordonnées bancaires ou avoir perdu votre RIB.

Fraudes aux réparations

Vous naviguez sur internet et un message bruyant et volontairement anxiogène apparaît simulant une erreur provenant de Windows. Pas de panique, n'appelez surtout pas le numéro affiché et redémarrez votre ordinateur si vous ne pouvez pas fermer le navigateur internet. Cette procédure cherche à exploiter le stress généré et la précipitation qui s'en suit.

Faux sites administratifs

De nombreux sites proposent, moyennant rémunération, de faciliter l'accomplissement de certaines démarches administratives courantes (demandes de permis de conduire, de carte grise, d'extrait d'acte de naissance...) ou encore de vous renseigner sur la mise en œuvre de réglementations spécifiques.

La plupart de ces services sont gratuits et les sites vous proposant d'effectuer ces démarches pour vous peuvent très bien exploiter les données personnelles que vous leur fournissez. Prenez rendez-vous avec votre conseiller numérique pour vous aider à faire ces démarches gratuitement !

Appels frauduleux aux dons

Technique subtile visant à vous faire croire que vous effectuez un don pour une ONG qui vous est chère mais le site internet par lequel vous allez passer est une copie conforme à l'original.

Dites vous que si vous êtes appelé, c'est déjà très mauvais signe, les suggestions dans ce domaine sont souvent frauduleuses. N'effectuez des dons que de votre propre initiative

RÉPUBLIQUE FRANÇAISE
Liberté Égalité Fraternité

CONSEILLER NUMÉRIQUE
France services

Besoin de conseils ?

Si des termes vous paraissent obscurs ou étrangers, venez me rendre une petite visite à la médiathèque les lundi et mardi ou à l'agence postale de Dun le reste de la semaine, je me ferai un plaisir de vous accueillir.

De plus je suis disponible pour vous accompagner dans diverses démarches administratives ou tout simplement vous aider à maîtriser votre matériel informatique.

Pour me joindre, composez le

06 79 76 56 97

Ou par mail à l'adresse :

remi.biolzi@conseiller-numerique.fr

À bientôt dans les locaux de la médiathèque ou de l'Agence Postale de Dun.

Rémi Biolzi