***** Escroqueries en lignes / via SMS ou appels *****

*** Quelques conseils ***

- Prenez le temps d'analyser les SMS ou courriels que vous recevez = assurez-vous de connaître l'expéditeur et attention aux faux sites/sites copiés et aux numéros d'appels usurpés ;

- **Vos mots de passes doivent rester « vos mots de passes »** = les communiquer à une autre personne c'est s'exposer à ce qu'ils soient divulgués par ce tiers à un moment donné ;

- Ne cliquez **JAMAIS** sur l'hyperlien présent dans le « SMS » ou le courriel, pas même sur les pièces jointes = faites la démarche d'aller chercher le site vous-même et de vous y connecter. C'est certes plus long mais c'est surtout plus sûr pour vos données personnelles et vos économies ...;

- Ne communiquez **JAMAIS** vos mots de passe ou coordonnées bancaires / carte bancaire que ce soit par courriel ou au téléphone = pas même à un individu qui vous contacte en indiquant être votre conseiller bancaire ;

- **JAMAIS** votre banque ne vous enverra un courtier pour récupérer votre carte bancaire = si un individu doit se présenter pour ce faire, contactez le « 17 » pour le signaler ;

- **Diversifiez vos mots de passe** sur vos différents comptes et ne les recyclez pas vous évitera de compromettre l'intégralité des comptes sur différents sites = c'est comme si vous n'aviez qu'une seule clé pour sécuriser votre maison, vos voitures et votre coffre-fort… **L'astuce est de recourir à un gestionnaire de mots de passes.**

- **Activez systématiquement la double authentification** dès qu'un site vous le propose à la création de votre compte = renforce la sécurité et atténue fortement le risque d'usurpation de votre identité ;

- **Évitez les ordinateurs et les connexions aux réseaux Wifi publics** ;

- **Supprimez les comptes dont vous n'avez plus l'utilité** = vous pourrez toujours vous réinscrire si un jour vous devez effectuer un nouvel achat ;

- **Sécurisez votre ordinateur/smartphone** = Installer un antivirus et acceptez les mises à jour officielles ;

- Ne rechargez **JAMAIS** votre smartphone en le branchant sur un ordinateur = privilégiez les recharges via le réseau électrique ;

- Ne branchez **JAMAIS** un support inconnu sur vos appareils électroniques = le risque de propager un virus/logiciel malveillant est trop important ;

- Ne rappelez **JAMAIS** un numéro inconnu qui ne vous laisse pas de message sur le répondeur = vous éviterez ainsi de composer un numéro surtaxé ou d'entrer en contact avec un escroc ;

- Méfiez-vous des QR codes.

**** Réactions face à une escroquerie en ligne ****

- Transmettez le courriel suspect en tant que pièce jointe à signal-spam@gendarmerie.interieur.gouv.fr ;

- Contactez-vous même et de suite le service opposition de votre carte bancaire = enregistrez ce numéro dans vos contacts vous fera gagner du temps ;

- **Pour évaluer votre situation et vous guider dans les démarches à accomplir** : https://17cyber.gouv.fr/

****** Rejoignez nous via "Ma Sécurité" ******

Soit via cet hyperlien : https://www.masecurite.interieur.gouv.fr/fr

Soit via l'application mobile

Astuce : Renseignez votre code postal et abonnez-vous aux notifications afin de rester informés et d'avoir les signalements de la Brigade de Feurs.