URGENT - IMPORTANT - URGENT - IMPORTANT

Sécurité économique territoriale
Auvergne - Rhône-Alpes

Deux nouvelles escroqueries touchant aussi bien les particuliers, les acteurs du monde économiques ou certaines institutions ont été détectées au cours de la semaine écoulée.

1 - ESCROQUERIES DE TYPE "SEXTORSION" :

*Un nouveau type d'escroquerie de type « **Sextorsion** » est apparue au cours de l'été dernier.*
*Particuliers et professionnels reçoivent des messages intitulés « **ceci concerne votre sécurité** » mentionnant que l'expéditeur a en sa possession leurs mots de passe ainsi que des vidéos compromettantes prises avec leurs propres webcams.*
Dans leurs e-mails, les maîtres-chanteurs informent leurs victimes que les vidéos seront transmises à l'ensemble de leurs contacts en cas de non-paiement d'une rançon en bitcoins.
Ces attaques cybercriminelles sont susceptibles de se multiplier de façon exponentielle dans un avenir proche.
Le site gouvernemental d'assistance aux victimes d'actes de cybermalveillance a émis des alertes sur ce sujet et prodigue les conseils suivants aux potentielles victimes :

- Ne surtout pas **PANIQUER** !
- Ne pas **RÉPONDRE.**
- Ne pas **PAYER.**
- **CONSERVER** l'ensemble des preuves.
- **CHANGER** immédiatement le mot de passe de l'adresse mail concernée.
- **SIGNALER** les faits le lien suivant : https://www.cybermalveillance.gouv.fr/.

2 - ESCROQUERIES DE TYPE "FAUSSE COMMANDE FNAC" :

Ces derniers jours, des courriels semblant émaner de la FNAC ont été transmis sur les boîtes mails principales de plusieurs mairies. Ceux-ci mentionnent la confirmation de l'achat de smartphones par les Maires. Hors, après vérifications, il appert que les édiles n'ont jamais effectué ces commandes auprès de cette grande enseigne.
En réalité, ces mail sont piégés et permettent de pirater les comptes des victimes dès lors qu'elles cliquent sur le lien "ANNULER LA COMMANDE".

Il convient de faire preuve d'une vigilance de tous les instants dès lors qu'il est question de commande d'articles, de récupérer des informations personnelles ou bancaires, ...
Dans la mesure du possible "**ne jamais cliquer sur un lien ou une pièce jointe**" émanant d'un expéditeur inconnu.
Et les conseils de base pour limiter les risques de fishing sont les suivants :

- ***Protégez vos mots de passe*** et ne les révélez à personne.
- ***Maintenez votre navigateur à jour*** et appliquez les correctifs de sécurité.
- ***Surveillez les e-mails qui viennent de marques célèbres***. Le site OpenPhish rassemble les marques les plus utilisées par les cybercriminels pour mener à bien leurs attaques de phishing. Parmi eux, Apple, Google et Paypal figurent dans le top dix des plus touchés par ce type de campagne. Les raisons sont évidentes: ils sont extrêmement populaires, il est donc plus susceptible de réussir à usurper l'identité des victimes potentielles.
- ***Vérifiez l'URL (adresse web) des sites web***. Dans de nombreux cas d'hameçonnage, l'adresse web peut sembler légitime, mais l'URL peut comporter une faute d'orthographe ou le domaine peut être différent (".com" au lieu de ".gov"). Si vous constatez une modification de l'URL, c'est qu'il s'agit sûrement d'un site miroir frauduleux.
- Dans la mesure du possible "***ne jamais cliquer sur un lien ou une pièce jointe***" émanant d'un expéditeur inconnu.
- Vérifiez la présence du **cadenas** sur toutes les pages de type formulaire ou paiement en ligne.
- Assurez-vous que vous êtes bien sur la ***version sécurisée*** du site en vérifiant la présence du «***https***» et du cadenas.
- Méfiez-vous de la notion "d'urgence". **il y a généralement un sentiment d'urgence pour donner nos données personnelles** (*exemples* : le compte est fermé, vous perdrez de l'argent, votre colis sera envoyé....).
- Vérifiez les fautes d'orthographe sur la page. Même s'ils se sont améliorés dans ce domaine, des fautes d'orthographe et de formulation sont encore souvent présentes. **Il reste toujours quelques erreurs de base**, souvent en raison de mauvaises traductions.
- Aucune banque ou organisme d'État ne vous demandera de communiquer vos coordonnées bancaires ou personnelles.

Si toutefois vous avez cliqué sur un mail phishing et saisi par exemple votre numéro client et votre code confidentiel :

- Contactez au plus vite le service relations clients ou votre conseiller bancaire pour faire réinitialiser vos codes de banque à distance,
- Surveillez votre compte et en cas de débit frauduleux, contestez l'opération auprès de votre banque.