SÉCURITÉ CITOYENNE N°6

Le Phishing

La municipalité et le Conseil de Sages de Violaines vous invitent à prendre connaissance du feuillet n°6 « Sécurité Citoyenne » joint à l'Echo.
La délinquance n'est pas toujours une fatalité, nous vous soumettons quelques règles simples, qui, mises en applications, vous prémuniront contre :

LE PHISHING

LE PHISHING

L'hameçonnage, le phishing en anglais est une tentative d'usurpation qui consiste généralement à vous envoyer des mails frauduleux. Une approche détournée qu'utilisent les cyber escrocs pour vous pousser à révéler des informations personnelles, comme des mots de passe , des numéros de carte de crédit, de sécurité sociale ou de comptes bancaires etc…Se faisant passer pour des organismes ou de grandes sociétés qui vous sont familiers , ils tentent ainsi de détourner des fonds.

Cette technique est d'autant plus dangereuse que l'email revêt toutes les apparences de ceux habituellement émis par les entreprises : logo, nom... tout est faux et presque parfaitement imité.
Généralement, les victimes sont attirées par l'annonce d'un remboursement imprévu ou d'une perte de leurs coordonnées.

Exemple :
« Suite à un incident technique, nos services ont malencontreusement perdu vos cordonnées, afin de retrouver vos droits veuillez remplir le formulaire... » « Nous vous informons que nous devons vous rembourser la somme de xxx euros »
L'email vous invite à cliquer sur le lien, envoyer vos coordonnées bancaires et/ou vos identifiants, mots de passe.
Autres types d'email frauduleux qui circulent :
- Une demande d'envoi d'argent de la part de l'un de vos proches en situation difficile (maladie, vol de papiers à l'étranger etc…) mais là **encore tout est faux** !
- **«On est tous Paris»** si vous recevez cet email accompagné d'une photo de bébé avec un bracelet de naissance, vous invitant à cliquer dessus, **NE CLIQUEZ PAS**, ce message contient **un Malware (virus)** qui permet à votre interlocuteur de prendre le contrôle à distance de votre ordinateur, de récupérer toutes vos données et mots de passe.
Il est très important de ne pas répondre, voire de transmettre le courriel aux Services de Police ou de la Gendarmerie.

COMMENT FAIRE FACE À CES ARNAQUES ?

Sachez que, sécurité oblige, les banques et l'administration ne demandent jamais vos numéros de cartes de crédit ou les mots de passe de vos comptes ou coordonnées bancaires par email.
Ne répondez jamais à ce type d'emails, ne les transférez pas.
En cas de doute, ne cliquez jamais sur les liens ni les pièces jointes.
Soyez vigilants lorsque l'on vous réclame une réponse urgente.

Supprimez toujours ces messages.
Dans le doute contactez un autre moyen l'expéditeur officiel.
Signalez tout email suspect à l'organisme dont l'identité a été usurpée et immédiatement à la plateforme PHAROS accessible sur le site : **www.internet-signalement.gouv.fr**
Saisissez vous-même l'adresse lorsque vous vous rendez sur un site internet. Lors d'un paiement ou d'échanges de données personnelles, vérifiez que le site est sécurisé : un cadenas apparait dans le navigateur et l'adresse du site commence par « https » au lieu de « http »
Autre arnaque à la mode, la victime est informée d'une mise à jour du nombre de points de son permis de conduire et guidée pour plus de renseignement vers un numéro payant.

ARNAQUE TÉLÉPHONIQUE

La victime reçoit un message vocal ou SMS plusieurs fois dans la journée .Ce message ou SMS conduit à contacter d'urgence un numéro surtaxé. Tous les prétextes sont bons et nombreux, par exemple :

- Le contrat d'assurance doit être soi-disant modifié exemple (modification de la responsabilité civile, limite d'âge du contrat, augmentation de la cotisation).
- L'évolution de la Loi entraînerait la nécessité de faire évoluer les garanties de votre mutuelle santé par exemple
- La présence de détecteur de fumée doit être soi-disant vérifiée
- Le contrat actuel doit être mis à jour, il manque certaines coordonnées bancaires.
- La cotisation n'a pas été payée, l'assurance va être résiliée
- Une remise exceptionnelle, un tarif très attractif sont proposés si souscription immédiate…

Lorsque la victime compose le numéro indiqué à rappeler d'urgence, il arrive qu'un enregistrement lui signifie que toutes les lignes sont occupées et lui demande de patienter, ce qui contribue à augmenter les frais de communication.

COMMENT FAIRE FACE À CES ARNAQUES

Vérifiez que le numéro communiqué n'est pas surtaxé (numéro à 10 chiffres commençant par 081, 082, 089 et certains numéros courts à 4 chiffres commençant par 1 ou 3)
Ne rappelez jamais un numéro surtaxé que vous ne connaissez pas.

Appelez rapidement votre conseiller, numéro figurant sur votre contrat afin de vérifier les dires. Un simple appel de vérification permet d'éviter de nombreux désagréments.
Soyez très prudents face à des offres alléchantes.

Signalez les appels ou SMS frauduleux au 33700, dispositif de signalement mis en place par la fédération française des télécom.

Pour tout renseignement complémentaire, reportez-vous aux textes applicables ou rapprochez-vous d'une direction départementale de la protection des populations DDPP ou direction départementale de la cohésion sociale et de la protection des populations (DDCSPP)

Conception, impression : service communication - Mairie de Violaines