ÉLECTIONS LÉGISLATIVES

ASSUREZ VOTRE SÉCURITÉ NUMÉRIQUE !

Vous êtes candidat aux élections législatives et recevez sur votre messagerie un courriel dont l'origine vous est inconnue. Mis en confiance par le logo officiel apposé dans la signature de l'émetteur ou la présentation du message, vous répondez favorablement à la requête de ce dernier et lui transmettez les codes d'accès à votre messagerie ou à d'autres comptes personnels.

QUE SE PASSE-T-IL ?

Vous êtes victime de hameçonnage (ou *phishing* en anglais), un type d'attaque auquel ont recours de très nombreux cybercriminels. En se faisant passer pour une personne ou un tiers de confiance (banque, Impôts, fournisseur d'accès à Internet, etc.), les attaquants tentent de soutirer à la victime des informations confidentielles (mots de passe, coordonnées bancaires, etc.). Quelles sont leurs méthodes ?

- Envoi à une liste de contacts d'un courriel frauduleux les invitant à mettre à jour leurs informations personnelles.
- Incitation par courriel à télécharger une pièce-jointe piégée ou à cliquer sur un lien redirigeant vers la contrefaçon d'un site Internet.

PROTÉGEZ-VOUS

- Ne cliquez jamais sur un lien ou une pièce-jointe dont l'origine ou la nature vous semblent douteuses. **Au moindre doute, privilégiez l'accès au site web visé en tapant directement l'adresse** dans la barre de recherche.
- Ne répondez jamais à un courriel vous demandant des informations confidentielles. **Au moindre doute, n'hésitez pas à contacter l'expéditeur** par un autre canal, par exemple téléphonique.
- Choisissez bien vos mots de passe. **Disposer d'un mot de passe unique pour chaque application,** au moins pour l'accès à vos comptes de messagerie, évite l'effet boule de neige d'une attaque par hameçonnage en épargnant vos autres comptes.
- Activez si possible l'authentification à double facteur [suivez le guide au verso]
- Vérifiez les paramètres de sécurité de votre compte de messagerie. N'hésitez pas à demander conseil.

VOUS PENSEZ AVOIR ÉTÉ VICTIME ?

- **Procédez immédiatement au renouvellement des identifiants** compromis et signalez l'incident aux personnes ou organisations concernées (banque, Impôts, fournisseur d'accès à Internet, etc.).
- **Déposez plainte** auprès des services de Police nationale ou de Gendarmerie nationale et munissez-vous des éléments suivants : adresse de messagerie ou postale, identifiants, numéros de téléphone, copie des courriels échangés, etc.
- Pour être conseillé, appelez INFO ESCROQUERIES par téléphone au 0 805 805 817 (numéro gratuit)
- Pour contribuer à la lutte contre ce phénomène, il est important de signaler l'adresse du site d'hameçonnage sur la plate-forme de signalement PHAROS (www.internet-signalement.gouv.fr). Vous pouvez aussi le faire sur le site de Phishing-Initiative, site recommandé par le Ministère de l'Intérieur (www.phishing-initiative.fr).

ANSSI
www.ssi.gouv.fr

LES 7 RÈGLES D'OR

- Séparez strictement vos usages à caractère personnel de ceux à caractère professionnel
- Protégez vos accès par des mots de passe complexes, uniques et secrets
- Protégez vos données et ne laissez pas vos équipements sans surveillance
- Protégez votre espace de travail
- Protégez votre messagerie professionnelle
- Préservez votre identité numérique
- Ne connectez pas vos équipements professionnels sur des réseaux non maîtrisés

AUTHENTIFICATION À DOUBLE FACTEUR

SUIVEZ LE GUIDE !

Activez si possible l'authentification à double facteur à votre messagerie électronique (ex. : envoi d'un code de confirmation par SMS)

- Google : www.google.com/landing/2step/
- Facebook : www.facebook.com/help/148233965247823?helpref=faq_content
- Twitter : support.twitter.com/articles/20170429
- Yahoo! : fr.aide.yahoo.com/kb/sln5013.html
- Microsoft : support.microsoft.com/fr-fr/help/12408/microsoft-account-about-two-step-verification
- Apple : support.apple.com/fr-fr/HT207198