OCTOBRE - DÉCEMBRE 2019 | N°3

Oceanis
services numériques

CYBERSECURE

FEDERATION EBEN
ENTREPRISES DU BUREAU ET DU NUMERIQUE

AU SOMMAIRE

A la Une : attaques par mail

QUAND LE GROS POISSON C'EST VOUS !

Les arnaques via messagerie électronique se multiplient et les techniques sont variées. Le mail est la porte d'entrée sur les données personnelles les plus essentielles : lien avec les organismes administratifs (banque, impôt…), comptes des sites d'achat et donc données bancaires… Qui ne consulte pas sa boîte mail plusieurs fois par jour ? De chez soi ou au travail ? De son smartphone ou de son poste informatique ? Les occasions ne manquent pas aux hackers et autres individus malintentionnés pour dérober les données personnelles ou professionnelles d'un utilisateur.

Les techniques les plus diverses

Ainsi, en juin dernier, 2000 comptes en ligne du site Impots.gouv.fr ont été piratés. Les hackers ont ainsi accédé aux données des contribuables concernés et ont modifié leurs déclarations. Bercy s'en est aperçu lorsqu'une avalanche de demandes de renouvellement de mots de passe a déferlé sur le site. En cause, les boîtes mail des contribuables qui n'étaient pas suffisamment protégées et qui ont permis aux pirates d'envoyer des demandes de renouvellement de mots de passe. Depuis, les services fiscaux ont renforcé leur politique de sécurité et se sont empressés d'avertir les contribuables en leur recommandant de mieux sécuriser leurs mots de passe.

Autre cas, autres méthode, celle de l'hameçonnage (ou phishing en anglais) qui consiste à se faire passer pour un tiers de confiance afin de récupérer les données de l'utilisateur. Ainsi, pendant plusieurs mois, 850 000 ordinateurs à travers le monde ont été infectés par le virus « Retadup », chez des particuliers comme dans des entreprises, via des liens frauduleux contenus dans des mails proposant de gagner de l'argent ou encore d'accéder à des photos érotiques. Un clic a donc suffi ! Depuis un serveur basé en Ile-de-France, les pirates ont pu dérober des données de patients et fabriquer de la cryptomonnaie. En tout 140 pays ont été touchés, dont la France. Le réseau criminel à l'origine de ce virus a pu officier pendant plusieurs mois sans que les utilisateurs des ordinateurs infectés ne s'en rendent compte.

De même, un hôpital privé de Nantes a été victime, en mai et juin dernier, de campagnes de mail frauduleux : les salariés de l'établissement ont reçu une invitation à renouveler leurs mots de passe et identifiants de connexion au système informatique de l'établissement. Se faisant, les utilisateurs ont transmis leurs données d'accès qui ont permis aux pirates de pénétrer le système.

Messagerie électronique

LES RÈGLES DE PRUDENCE

- Utilisez des mots de passe différents et complexes pour chaque site et application, à commencer par votre messagerie.
- Ne communiquez jamais d'informations sensibles par messagerie ou téléphone : aucune administration ou société commerciale sérieuse ne vous demandera vos données bancaires ou vos mots de passe par message électronique ou par téléphone.
- Ne mélangez pas votre messagerie professionnelle et personnelle afin d'éviter les erreurs de destinataire ou de mettre en danger votre entreprise en cas de piratage de votre boîte personnelle (souvent moins bien sécurisée).
- Evitez les réseaux wi-fi publics ou inconnus lorsque vous consultez votre messagerie.
- Ne cliquez pas trop vite sur un lien contenu dans un mail : positionnez le curseur de votre souris sur ce lien (sans cliquer) ce qui affichera alors l'adresse vers laquelle il pointe réellement afin d'en vérifier la vraisemblance ou allez directement sur le site de l'organisme en question sans passer par ce lien.
- Vérifiez l'adresse de l'expéditeur avant toute ouverture de mail. Bien souvent, l'origine frauduleuse se détecte à la lecture de l'adresse. Si le doute persiste n'hésitez pas à contacter directement l'organisme concerné pour demander une confirmation.
- Ne relayez pas les canulars et autres chaînes de lettres, porte-bonheur... vous prenez le risque d'accroître la viralité d'un mail frauduleux et de surchargez les systèmes.

Gestion des mots de passe

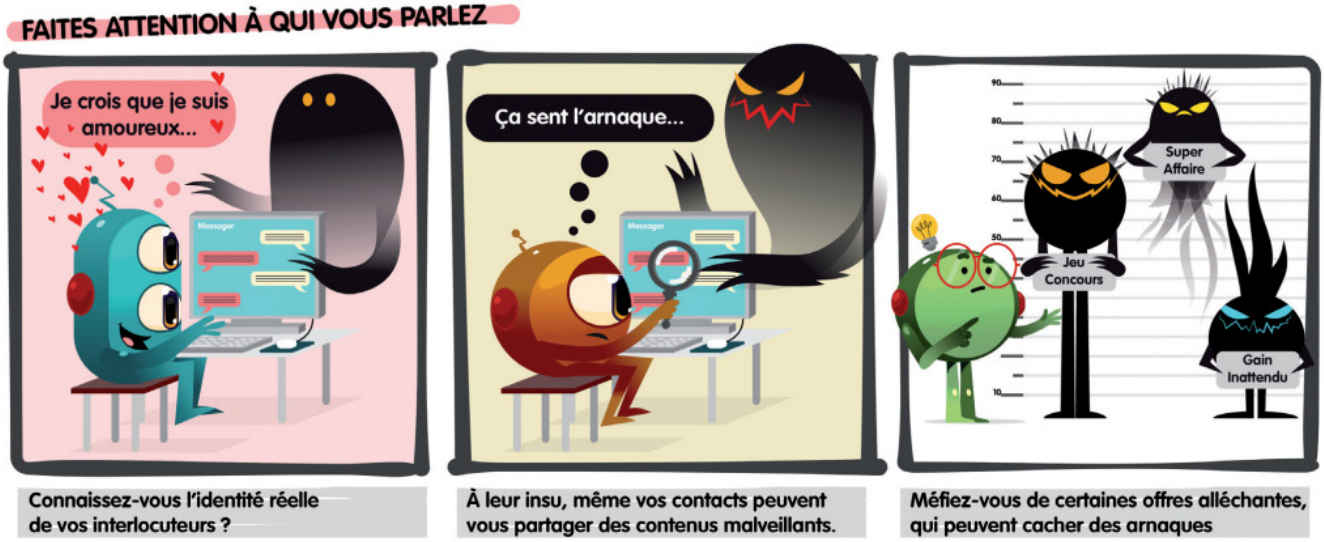
10 CONSEILS POUR ÊTRE EFFICACE

- Utilisez un mot de passe différent pour chaque service
- Utilisez un mot de passe suffisamment long et complexe
- Utilisez un mot de passe impossible à deviner
- Utilisez un gestionnaire de mot de passe
- Changez votre mot de passe au moindre soupçon
- Ne communiquez jamais votre mot de passe à un tiers
- N'utilisez pas vos mots de passe sur un ordinateur partagé
- Activez la «double authentification» lorsque c'est possible
- Changez les mots de passe par défaut des différents services auxquels vous accédez
- Choisissez un mot de passe particulièrement robuste pour votre messagerie

Petite astuce pour un mot de passe solide et mémorisable

Faites une phrase dont vous vous souviendrez facilement, par exemple «J'aime les gateaux au chocolat de ma grand-mère». Prenez la première lettre de chaque mot, en veillant à mettre certaines en majuscules et à transformer certains mots en chiffres.

Cela donne : **J'**alg**O**c**2**mg-m



Cette lettre d'information vous est offerte par votre prestataire

Oceanis
services numériques

3, impasse de l'Aube
Parc d'Activités Le Soleil Levant
85800 Givrand

02 51 60 05 05

www.oceanis.fr

Fédération EBEN
69, rue Ampère
75017 Paris
www.federation-eben.com

MEMBRE DU DISPOSITIF
CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention du risque numérique

Directeur de la publication : Loïc Mignotte
Rédaction : Fédération EBEN, Cybermalveillance.gouv.fr
Photos : Unsplash, Adobe Stock
Maquette : Emmanuelle Bauvais