Ville de Saint-Louis
Ile de La Réunion

Envoyé en préfecture le 06/11/2024
Reçu en préfecture le 06/11/2024
Publié le
ID : 974-219740149-20241029-DCM133_2024-DE

LA CYBERSÉCURITÉ AU SERVICE DE LA MAIRIE DE SAINT LOUIS

Bulletin proposé par la Direction Informatique

“L'hameçonnage vise notre mairie !”

L’hameçonnage (phishing en anglais) est une technique frauduleuse destinée à vous inciter à communiquer des données personnelles (comptes d’accès, mots de passe…) et/ou bancaires en se faisant passer pour un tiers de confiance.

Il peut s'agir d'un faux message, SMS ou appel téléphonique se faisant passer pour des entreprises locales, des fournisseurs de services ou des partenaires financiers.

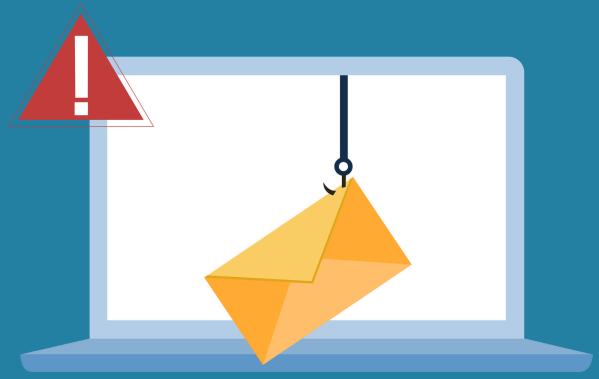
BUT RECHERCHÉ

Voler des informations personnelles ou professionnelles (comptes, mots de passe, données bancaires…) pour en faire un usage frauduleux.

LA BONNE PRATIQUE

Quand je reçois un mail suspect :

- Je ne clique pas sur les liens
- Je ne transmets pas mon mot de passe
- Je n'ouvre pas la pièce-jointe



Comment reconnaître un email frauduleux ?

1. **Demandes d'informations sensibles** : Soyez vigilant avec les demandes inattendues.
2. **Urgence exagérée** : Méfiez-vous des messages pressants.
3. **Fautes de langue** : Attention aux erreurs grammaticales ou orthographiques.
4. **Adresses email suspectes** : Vérifiez l'authenticité de l'adresse de l'expéditeur.
5. **Liens douteux** : Survolez les liens avant de cliquer.

En cas de doute, contactez-nous : **dpo@saintlouis.re**

Ville de Saint-Louis
Ile de La Réunion

Envoyé en préfecture le 06/11/2024
Reçu en préfecture le 06/11/2024
Publié le
ID : 974-219740149-20241029-DCM133_2024-DE

LA CYBERSÉCURITÉ AU SERVICE DE LA MAIRIE DE SAINT LOUIS

Bulletin proposé par la Direction Informatique

“Protégez votre identité numérique.”

Vos identifiants et mots de passe sont essentiels pour accéder à votre poste de travail, aux applications, aux dossiers et au réseau interne de la mairie de Saint Louis. Ils garantissent votre sécurité et votre identité professionnelle.

Chaque utilisateur est responsable de la gestion et de l'utilisation de ses mots de passe.

Considérez-les comme la serrure et la clé de votre espace de travail numérique : ils sont personnels et doivent rester confidentiels.

Sécurisez votre identité, essentielle au Travail comme à la Maison

LA BONNE PRATIQUE

Quand j’utilise un mot de passe :

- Je définis un mot de passe robuste
- Je protège mon mot de passe
- Je ne réutilise pas le même mot de passe

Comment définir un mot de passe ?

1. **Longueur :** Utilisez un mot de passe d'au moins 12 caractères
2. **Complexité :** Utilisez des caractères minuscules, majuscules, chiffres et caractères spéciaux.
3. **Difficilement devinable :** Le mot de passe ne doit pas contenir votre nom/prénom.

Une question ? Contactez-nous : **dpo@saintlouis.re**

Ville de
Saint-Louis
Ile de La Réunion

Envoyé en préfecture le 06/11/2024
Reçu en préfecture le 06/11/2024
Publié le
ID : 974-219740149-20241029-DCM133_2024-DE

LA CYBERSÉCURITÉ AU SERVICE DE LA MAIRIE DE SAINT LOUIS

Bulletin proposé par la Direction Informatique

“Les dangers cachés des applications non autorisées”

L'utilisation de logiciels et d'applications non autorisés peut mettre en danger la sécurité de nos systèmes informatiques et la confidentialité de nos informations à la mairie de Saint Louis.

Pour protéger notre lieu de travail, il est essentiel que chaque agent utilise seulement les outils informatiques approuvés.

Utiliser des programmes non vérifiés peut créer des risques de sécurité, compromettant la sûreté de tous.

Et n’oubliez pas, au Travail comme à la Maison, si le service est gratuit, alors vous êtes probablement le produit.

LA BONNE PRATIQUE

Quand j’envoie des données :

- J’utilise uniquement ma messagerie professionnelle
- J’évite de transférer mes emails vers ma messagerie personnelle
- Je privilégie OneDrive pour les transferts de fichier

La mairie vous met à disposition des outils pratiques :

1. **Email sécurisé :** Utilisez vos services de messagerie installés et configurés par la Commune
2. **Partage de fichiers interne :** Privilégier le stockage réseau et OneDrive Professionnel
3. **Partage de fichiers externe :** Transférer avec OneDrive Professionnel

A bannir : *les messageries personnelles comme Gmail ou Yahoo, les services de stockage cloud non officiels comme Dropbox, et les outils de transfert de fichiers tel que WeTransfer*

Une question ? Contactez-nous : **dpo@saintlouis.re**