RAIFFEISEN

Banque Raiffeisen
de Troistorrents-Morgins

Guide des bonnes pratiques sur internet

Phishing

Soyez vigilant et critique envers les emails, SMS et appels téléphoniques:

□ Est-ce que le contenu est cohérent? Est-ce que j'attends un email, SMS ou appel ? (suis-je client(e) ?)

□ Est-ce que le contenu est personnalisé? Est-ce que le contexte est alléchant ou inquiétant?

□ Est-ce que l'adresse email, le n° de tél m'est connu(e) ? Est-ce que l'adresse email est étrange?

□ Qui est l'expéditeur ? Est-ce que je le/la connais ?

□ S'il y a un lien dans le message, vers quel site internet conduit-il vraiment? (glisser la souris sur le lien sans cliquer)

□ Rechercher l'email, le titre du message sur internet (p. ex. avec Google) si cette arnaque est connue

□ Dans le doute: ne pas ouvrir de pièce jointe, ne pas cliquer sur le lien et effacer le message

Vol d'identité

□ S'assurer que le site sur lequel les données de connexion sont entrées est bien le site officiel : https://login.raiffeisen.ch/fr?applicationId=ebanking
Présence du cadenas et adresse du site correctement orthographiée

□ Définir un mot de passe difficile et unique (incluant 12 caractères, minuscules, majuscules, chiffres, symboles, pas de mot du dictionnaire)

□ Utiliser un gestionnaire de mots de passe fiable (NordPass, LastPass, 1Password, Keepass, Apple, Edge)

□ Activer la double authentification *(MFA)* : p. ex. un mot de passe et un code par SMS ou sur une application

□ Vérifier si votre email a été compromis
https://haveibeenpwned.com/
Si oui, changez votre mot de passe !

□ Ne jamais donner vos données de connexion (bancaires. Twint ou autres) à qui que ce soit ! En cas de doute, contacter votre banque

RAIFFEISEN

Banque Raiffeisen
de Troistorrents-Morgins

Achats en ligne

□ Vérifier le site internet (petit cadenas, commentaires de clients)

□ Renseignez-vous sur le site ou le revendeur en recherchant sur Internet (Google)

□ Restez sur des sites connus et si possible suisses : aller voir sous «Contact», «Livraison» ou les conditions de vente, si la livraison s'effectue depuis la Suisse. Un site en **.ch** ne signifie pas forcément que le vendeur se trouve en Suisse !

□ S'il s'agit de petites annonces, soyez critique (prix trop bas, seule possibilité de paiement par prépaiement,
frais supplémentaires cachés, vendeur vient de créer son profil)

□ Pour les paiements en ligne, vous pouvez utiliser une carte à prépaiement (en cas d'abus, cela limite la somme de la fraude)

□ Pour les plus avancés, vérifier si les images de l'annonce viennent bien du vendeur en effectuant une
recherche d'image sur Google : https://images.google.com/

Virus informatiques

□ Installer un bon antivirus donc payant (Bitdefender, Microsoft Defender…)

□ Mettre à jour régulièrement tous les appareils (smartphones, tablettes, PC personnels)

□ Télécharger uniquement des applications connues, bien notées et depuis une source officielle (site de l'entreprise, Apple Store, Google Store).
Les applications/ jeux gratuits, ont des chances d'être malveillants

□ Ne pas faire de paiements en ligne depuis un ordinateur sur lequel se trouve des produits piratés

□ Ne pas utiliser de souris, clavier, autre équipement informatique achetés sur des sites étrangers (Aliexpress, Wish, Temu, etc.), car ils contiennent peut-être des virus !

□ Dans les réglages de votre navigateur internet (Safari, Google…), choisir d'effacer automatiquement les cookies, cache, etc.

□ Ne pas utiliser les Wifi publics (hôtel, McDonalds, etc.) pour accéder à des données sensibles (E-Banking, emails…) ou utiliser un VPN, car ces établissements peuvent lire vos données !

□ Sauvegarder régulièrement vos documents, photos… sur un autre support (disque dur externe, « cloud » comme OneDrive ou iCloud et Samsung Cloud

Banque Raiffeisen de Troistorrents-Morgins – M. Steven Premand – Responsable Sécurité –
steven.premand3@raiffeisen.ch