Octobre 2024

Mois de sensibilisation à la cybersécurité

Protégez-vous !

1. **Méfiez-vous des e-mails d'hameçonnage**
   On parle d'hameçonnage lorsque des cybercriminels essaient de soutirer de vous vos informations en vous envoyant de faux e-mails. Ils prétendent être quelqu'un d'autre et vous demandent de cliquer sur des liens malveillants. Si un e-mail vous semble bizarre, méfiez-vous, vérifiez qui vous l'a envoyé pour voir s'il correspond à la personne qui prétend l'avoir expédié.

2. **Utilisez une authentification multifactorielle**
   Obtenez une couche de protection supplémentaire contre les pirates informatiques en utilisant une authentification multifactorielle (MFA) lorsque vous vous connectez en ligne. C'est pareil à un texte ayant un code secret qui expire après l'avoir utilisé une seule fois.

3. **Utilisez un mot de passe ou une phrase secrète assez difficile à deviner**
   N'utilisez pas le même mot de passe sur tous vos réseaux ! Utilisez des lettres, des chiffres et des symboles.
   Plus le mot de passe est long, plus il est sécurisé. Les phrases d'authentification peuvent également mieux convenir.

4. **Mettez toujours à jour vos logiciels**
   Cela diminue les risques d'infection suite à l'installation de logiciel par des pirates qui peuvent s'emparer de vos informations ou propager des virus dans votre ordinateur.

5. **Toujours agir après mûre réflexion, assurer votre sécurité sur les réseaux sociaux !**
   En partageant vos informations personnelles, telles que la date de votre naissance, l'adresse de votre maison ou l'endroit où vous vous trouvez, vous risquez qu'on les utilise pour usurper votre identité ou pour vous intimider.

6. **Protégez-vous, utilisez un Wi-Fi sécurisé**
   Les réseaux publics ne sont pas sécurisés. Quelqu'un pourrait voir ce que vous faites en ligne, et notamment se connecter à vos e-mails et à vos comptes bancaires

7. **Découvrez les escroqueries menées par le biais d'intelligence artificielle**
   Les cybercriminels ont recours à l'intelligence artificielle (AI) pour créer des images, des textes, des voix humaines, et des vidéos. Ce qui rend l'hameçonnage et d'autres escroqueries plus difficiles à détecter. Soyez vigilants et vérifiez deux fois (par exemple, vérifiez la source, cherchez à repérer les signaux d'alerte AI et les « artefacts » tels que des mots urgents, des voix étranglées, ou des images un peu flous, etc.) avant de vous assurer de l'authenticité de toute communication imprévue.