Les bases de la cybersécurité pour les débutants

Par Patrick Sentinel – 29a.ca

La cybersécurité est un enjeu important dans notre monde connecté. Que vous naviguiez sur Internet, utilisiez les réseaux sociaux, ou fassiez des achats en ligne, il est essentiel de protéger vos informations personnelles et vos appareils contre les menaces en ligne. Cet article vous guide à travers les bases de la cybersécurité, en vous fournissant des conseils simples pour améliorer votre sécurité numérique.

1. Créer et gérer des mots de passe forts

Les mots de passe sont la première ligne de défense contre les intrusions. Pour améliorer leur efficacité :

- **Utilisez des mots de passe longs et complexes** : Un bon mot de passe contient au minimum 12 caractères, avec une combinaison de lettres majuscules et minuscules, de chiffres et de symboles. N'hésitez pas à être créatif 😊.
- **Évitez les informations personnelles** : N'utilisez pas de mots de passe basés sur des informations facilement devinables comme votre nom, votre date de naissance ou le nom de votre animal de compagnie.
- **Utilisez un gestionnaire de mots de passe** : Un gestionnaire de mots de passe peut générer et stocker vos mots de passe pour vous, de sorte que vous n'avez pas à vous souvenir de chacun d'eux.

2. Identifier les courriels de phishing

Les attaques de phishing sont des tentatives de fraude visant à obtenir vos informations privés/sensibles en se faisant passer pour une entité légitime. Pour aider à les éviter :

- **Soyez vigilant face aux courriels non sollicités** : Méfiez-vous des courriels qui vous demandent des informations personnelles ou financières, surtout s'ils semblent urgents. Ne fournissez **JAMAIS** d'information!
- **Vérifiez l'adresse de l'expéditeur** : Les cybercriminels utilisent souvent des adresses similaires à celles de sources légitimes. Vérifiez minutieusement l'adresse électronique de l'expéditeur avant d'interagir avec le contenu. En général, si vous ne connaissez pas l'expéditeur vous devriez supprimer le courriel et ne pas cliquer sur les liens. Si c'était important on devrait vous appeler, ne vous inquiétez pas 😊
- **Ne cliquez pas sur les liens suspects** : Si un courriel vous semble suspect, ne cliquez pas sur les liens ou N'OUVREZ PAS les pièces jointes. Vous pouvez passer votre curseur sur un lien pour voir où il mène réellement.

3. Mettre à jour vos logiciels

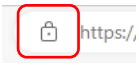
Les mises à jour logicielles sont cruciales pour votre sécurité en ligne. Elles corrigent souvent des vulnérabilités qui pourraient être exploitées par des cybercriminels. Pour aider à votre protection en ligne :

- **Activez les mises à jour automatiques** : Configurez vos appareils pour qu'ils installent automatiquement les mises à jour de sécurité. Vous ne savez pas comment? Demandez de l'aide!
- **Mettez à jour régulièrement vos applications** : Non seulement votre système d'exploitation, mais aussi vos applications doivent être mises à jour régulièrement.
- **N'ignorez pas les alertes de sécurité** : Si votre appareil vous alerte d'une mise à jour critique, installez-la sur le champ.

4. Naviguer sur Internet

La navigation sur Internet comporte des risques, mais en prenant quelques précautions, vous pouvez les réduire :

- **Utilisez une connexion sécurisée** : Assurez-vous que votre connexion Internet est sécurisée, en utilisant le Wi-Fi domestique avec un mot de passe fort ou en accédant aux sites via HTTPS (recherchez le cadenas dans la barre d'adresse, voir image ci-dessous).



- **Soyez prudent avec les informations que vous partagez** : Ne partagez pas d'informations personnelles sensibles sur des sites non sécurisés ou publics.
- **Utilisez un logiciel antivirus** : Installez un logiciel antivirus fiable pour protéger votre appareil contre les logiciels malveillants qui peuvent être téléchargés lors de la navigation.

5. Protéger vos appareils mobiles

Les smartphones et tablettes sont autant exposés aux menaces que les ordinateurs. Voici comment aider à les protéger :

- **Activez le verrouillage de l'écran** : Utilisez un code PIN, un mot de passe ou une reconnaissance biométrique (empreinte digitale, reconnaissance faciale) pour verrouiller votre appareil. Privilégiez un PIN ou un mot de passe.
- **Téléchargez des applications UNIQUEMENT depuis des sources officielles** : Évitez de télécharger des applications provenant de sources non vérifiées, car elles peuvent contenir des logiciels malveillants.
- **Sauvegardez régulièrement vos données** : En cas de perte ou de vol de votre appareil, une sauvegarde régulière de vos données vous aidera à les récupérer plus facilement.

Conclusion

La cybersécurité peut sembler complexe, mais en adoptant ces bonnes pratiques, vous pouvez réduire les risques de vous faire pirater. En sécurisant vos mots de passe, en étant vigilant face aux courriels de phishing, en mettant régulièrement à jour vos logiciels, et en protégeant vos appareils mobiles, vous prenez les premières étapes essentielles pour aider à protéger votre navigation sur Internet. Restez informé et conscient des menaces potentielles pour continuer à protéger vos informations et vos appareils.