Initiation à la sécurité informatique 09/2024

1. Sécurité des appareils mobiles

Les appareils mobiles sont vulnérables aux cyberattaques en raison de leur usage quotidien pour accéder à des données sensibles. Les principaux risques incluent la perte ou le vol de l'appareil, l'installation d'applications non fiables, et les connexions sur des réseaux Wi-Fi publics non sécurisés.

Mesures :

- Utiliser des codes d'accès robustes et activer le chiffrement des données.
- Appliquer les mises à jour de sécurité pour le système d'exploitation et les applications.
- Installer des solutions antivirus adaptées aux appareils mobiles.
- Éviter l'installation d'applications provenant de sources non officielles et surveiller les autorisations accordées aux applications.
- Sauvegarder régulièrement les données et éviter de stocker des informations sensibles sans protection.

2. Sécurité sur les réseaux sociaux

Les réseaux sociaux sont des cibles fréquentes pour des activités malveillantes telles que l'usurpation d'identité, le chantage, ou la diffusion de fausses informations. Ces plateformes contiennent des données personnelles très recherchées par les cybercriminels.

Mesures :

- Utiliser des mots de passe solides et activer l'authentification à deux facteurs.
- Vérifier régulièrement les paramètres de confidentialité pour limiter la visibilité des informations personnelles.
- Faire preuve de discernement dans les publications et éviter de partager des données sensibles.
- Éviter les connexions via des ordinateurs ou des réseaux Wi-Fi publics non sécurisés.

3. Séparation des usages professionnels et personnels

L'usage des appareils numériques pour des activités à la fois personnelles et professionnelles présente des risques importants, notamment l'exposition d'informations professionnelles à des cybercriminels via des canaux personnels non sécurisés.

Mesures :

- Utiliser des mots de passe différents pour les comptes personnels et professionnels.
- Ne pas mélanger les messageries professionnelles et personnelles pour éviter les erreurs de destinataires.
- Ne pas stocker d'informations professionnelles sur des services de cloud personnels non sécurisés.
- Faire les mises à jour de sécurité sur tous les appareils et utiliser des antivirus à jour.
- Éviter les réseaux Wi-Fi publics ou non sécurisés pour échanger des informations professionnelles.

4. Mesures essentielles pour assurer la cybersécurité

La cybercriminalité profite de la croissance de l'usage des outils numériques. Les risques incluent le piratage, l'hameçonnage, les rançongiciels et les infections par virus.

Mesures :

- Protéger les accès avec des mots de passe solides.
- Sauvegarder régulièrement les données.
- Appliquer systématiquement les mises à jour de sécurité.
- Utiliser des solutions antivirus fiables et n'installer que des applications provenant de sources officielles.
- Se méfier des messages ou fichiers inattendus pouvant contenir des malwares.

5. Sécurité sur les sites de vente entre particuliers

Les plateformes de vente entre particuliers (Leboncoin, Vinted, etc.) sont souvent ciblées par des escrocs, qui cherchent à voler de l'argent ou des informations personnelles.

Mesures :

- Vérifier les conditions générales d'utilisation des plateformes et les modalités de paiement sécurisées.
- Méfiez-vous des annonces trop attractives et des invitations à quitter la plateforme pour échanger via des messageries instantanées.
- Utilisez le système de paiement sécurisé proposé par la plateforme et évitez les moyens de paiement alternatifs (Western Union, Transcash, etc.).
- Procédez à l'échange de produits dans un lieu public pour plus de sécurité.
- Sécurisez l'accès à vos comptes avec des mots de passe uniques et complexes, et activez l'authentification à deux facteurs lorsque cela est possible.

Les règles principales de la « **nétiquette** » pour écrire des mails de manière respectueuse et professionnelle

- **Objet clair et concis** : Indiquez un objet précis pour permettre au destinataire de comprendre rapidement l'objectif du mail.
- **Formule de politesse** : Commencez par une formule de salutation adaptée au contexte et au niveau de formalité (par exemple : "Bonjour" ou "Madame/Monsieur").
- **Courtoisie** : Soyez respectueux et évitez les phrases abruptes ou agressives. L'utilisation du "s'il vous plaît" et du "merci" est fortement recommandée.
- **Clarté et concision** : Allez droit au but, en évitant les longues digressions. Un mail bien structuré facilite la lecture et la compréhension.
- **Langue correcte** : Relisez votre mail pour corriger les fautes d'orthographe et de grammaire. Utilisez un langage approprié, sans abréviations excessives ni jargon.
- **Utilisation appropriée de la copie** : Ne mettez en copie que les personnes concernées par le sujet du mail. Limitez l'usage du "Répondre à tous" si ce n'est pas nécessaire.
- **Ne pas écrire en majuscules** : Les majuscules peuvent être perçues comme agressives, donc à éviter sauf pour les acronymes ou les sigles.
- **Structure et paragraphe** : Utilisez des paragraphes pour aérer le texte et faciliter la lecture.
- **Pièces jointes** : Mentionnez les pièces jointes dans le corps du mail et assurez-vous qu'elles sont bien attachées avant l'envoi.
- **Signature professionnelle** : Concluez avec une formule de politesse et ajoutez une signature qui contient vos coordonnées (nom, poste, entreprise, numéro de téléphone, etc.).
- **Ne pas répondre dans la précipitation** : Prenez le temps de réfléchir avant de répondre, surtout si le message vous a contrarié.
- **Ne pas spammer** : Évitez l'envoi d'e-mails non sollicités ou répétitifs.