Structure de la formation : Initiation à la Cybersécurité !

Objectifs de la session

- Comprendre les principes de base de la cybersécurité.
- Apprendre à protéger ses données personnelles et professionnelles en ligne.
- Adopter des bonnes pratiques pour naviguer et utiliser Internet de manière sécurisée.

---

1. Introduction

- Présentation des objectifs de la session.
- Importance de la cybersécurité aujourd'hui : statistiques et exemples d'attaques.
- Exemples de conséquences d'une mauvaise sécurité (vol d'identité, perte de données).

---

2. Principes de base de la cybersécurité

- **Définition de la cybersécurité** : protection des systèmes informatiques contre les attaques numériques.
- **Concept de CIA** : Confidentialité, Intégrité, et Disponibilité.
- **Types de menaces** : virus, logiciels malveillants, phishing, ransomware.
  L'hameçonnage ou phishing est une forme d'escroquerie sur internet.
  Le fraudeur se fait passer pour un organisme que vous connaissez (banque, service des impôts, CAF, etc.), en utilisant le logo et le nom de cet organisme. Il vous envoie un mail vous demandant généralement de "mettre à jour" ou de "confirmer vos informations suite à un incident technique", notamment vos coordonnées bancaires (numéro de compte, codes personnels, etc.).
- **Exemples d'attaques récentes** : discutons brièvement d'incidents notables pour sensibiliser.

---

3. Protection des données personnelles

a. Ce que sont les données personnelles : informations personnelles, financières, professionnelles.

1. **Chiffrement des données** : explication simple du concept de chiffrement.

Qu'est-ce que le chiffrement des données ?
Le chiffrement des données est une technique utilisée pour protéger les informations en les transformant en une forme codée que seules les personnes autorisées peuvent lire. Cela empêche les personnes non autorisées d'accéder aux informations sensibles.

Comment ça marche ?

- **Chiffrement** : Lorsque vous voulez protéger des données, vous utilisez un **algorithme de chiffrement** et une **clé de chiffrement** pour convertir les données en un code incompréhensible, appelé **texte chiffré**.

- **Algorithme de chiffrement** : Une méthode ou une procédure mathématique qui transforme les données.
- **Clé de chiffrement** : Une séquence de bits utilisée par l'algorithme pour chiffrer et déchiffrer les données.

2. **Transmission sécurisée** : Le texte chiffré peut être transmis ou stocké en toute sécurité, car même s'il est intercepté, il ne peut pas être compris sans la clé appropriée.

3. **Déchiffrement** : Lorsque les données doivent être lues par une personne autorisée, le texte chiffré est reconverti en **texte en clair** (forme originale lisible) à l'aide de l'algorithme de chiffrement et de la clé de déchiffrement.

Exemple simplifié

- **Texte en clair** : "Bonjour"
- **Algorithme de chiffrement** : Une règle qui remplace chaque lettre par une autre lettre.
- **Clé de chiffrement** : La règle spécifique, par exemple, décaler chaque lettre de 3 positions dans l'alphabet (A devient D, B devient E, etc.).
- **Texte chiffré** : "Erqmrxu"

Seule une personne avec la clé de déchiffrement (ici, la règle de décalage inverse) pourra lire le message original "Bonjour".

Pourquoi est-ce important ?

Le chiffrement des données est essentiel pour protéger les informations sensibles telles que les mots de passe, les informations bancaires et les communications privées contre les cybercriminels et les accès non autorisés.

b. Gestion des mots de passe :
- Importance des mots de passe forts et de leur renouvellement régulier.
- Présentation des gestionnaires de mots de passe (ex. **LastPass**, **Bitwarden**, **1Password**).

c. Authentification à deux facteurs (2FA) : essayons une activation de la 2FA sur un compte.

---

4. Sécurité en ligne et navigation sécurisée

- **Utilisation de réseaux Wi-Fi publics** : risques associés et solutions (ex. VPN).
- **VPN (Virtual Private Network)** :
- Un VPN est une technologie qui crée une connexion sécurisée et cryptée entre votre appareil (ordinateur, smartphone, etc.) et un serveur distant. Cette connexion permet de masquer votre adresse IP, de sécuriser vos données et d'accéder à des ressources sur le réseau privé comme si vous étiez physiquement présent à cet emplacement.

expliquer son fonctionnement de base et recommander des outils comme **NordVPN**, **ProtonVPN**, ou **OpenVPN**.
- **Navigation sécurisée** :
    - Utilisation de navigateurs sécurisés (ex. **Brave**, **Mozilla Firefox**).
    - Activation de la protection anti-phishing.
- **Extensions de sécurité** : Ces extensions sont utiles : **uBlock Origin**, **HTTPS Everywhere**, **Privacy Badger**.

---

5. Bonnes pratiques en matière de sécurité

- **Mises à jour régulières** : importance de garder les logiciels et systèmes d'exploitation à jour.
- **Courriels et phishing** : comment détecter les courriels suspects, analyser les liens et pièces jointes.
- **Utilisation sécurisée des réseaux sociaux** : paramétrage de la confidentialité, éviter de partager des informations sensibles.
- **Sécurité des appareils** : installation d'un antivirus (ex. **Windows Defender**, **Avast**, **Kaspersky**), sécurisation des appareils mobiles.
- **Sauvegarde des données** : stratégie de sauvegarde en 3-2-1 (3 copies, 2 emplacements différents, 1 copie hors site) avec des solutions comme **Google Drive**, **Dropbox**, **iCloud**, ou des disques durs externes.

---

6. Simulations et Exercices Pratiques

- **Simulation de phishing** : Des exemples d'emails frauduleux et discussion de leur détection.
- **Création de mots de passe forts** : exercice pour créer et tester des mots de passe.
- **Test d'une connexion VPN** : L'utilisation d'un VPN pour sécuriser sa connexion.

---

7. Session de Questions et Réponses

Conclusion et Conseils

- **Résumé des points clés** : importance de la vigilance, de la mise à jour des logiciels, et de la protection des comptes.
- **Ressources recommandées** : plateformes pour apprendre davantage (ex. **CyberAware**, **Cybersecurity & Infrastructure Security Agency (CISA)**).

Logiciels et outils pour la formation en cybersécurité

1. **Gestionnaires de mots de passe** : LastPass, Bitwarden, 1Password.
2. **VPN** : NordVPN, ProtonVPN, OpenVPN.
3. **Navigateurs sécurisés** : Mozilla Firefox, Brave.

4. **Antivirus** : Windows Defender, Avast, Kaspersky.
5. **Extensions de sécurité pour navigateurs** : uBlock Origin, Privacy Badger, HTTPS Everywhere.
6. **Outils de sensibilisation au phishing** : sites comme **PhishMe** ou **KnowBe4**.