@Ecole Normale Supérieure Setif

CONFÉRENCE CYBERSECURITÉ

LE 09 Mai 2024

Sécurité en ligne : Protégez vous !

Apprenez à sécuriser vos données, à prévenir les cyberattaques et à se protéger des menaces numériques.

PRÉSENTÉE PAR: DR.BOUNOUNI MAHDI

1. Importance de protéger notre présence en ligne

1. **Importance des Réseaux Sociaux**
   - ✓ Les réseaux sociaux ne sont plus simplement un moyen de rester en contact avec des amis et des proches
   - ✓ ils sont devenus une extension de notre identité personnelle et professionnelle. nous partageons des informations,
   - ✓ nous engageons dans des discussions et nous connectons avec des communautés à travers diverses plateformes telles que Facebook, Twitter, Instagram, et LinkedIn
2. **Pourquoi la Cybersécurité ?**
   - ✓ la cybersécurité devient cruciale. Elle sert à protéger nos informations personnelles contre les accès non autorisés
   - ✓ préserver notre vie privée
   - ✓ défendre nos comptes contre les cyberattaques, qui sont de plus en plus fréquentes et sophistiquées

1. Importance de protéger notre présence en ligne

1. Pourquoi la Cybersécurité ?

- ✓ Protéger vos données personnelles est vital pour éviter l'usurpation d'identité et les fraudes financières.
- ✓ Une sécurité renforcée est essentielle pour maintenir la confiance et assurer une expérience utilisateur sécurisée et positive sur les réseaux sociaux.
- ✓ Cas d'étude: En 2021, un compte Facebook compromis a été utilisé pour orchestrer une campagne de phishing, entraînant des pertes financières significatives pour les utilisateurs dupés.

2. Menaces Courantes sur les Réseaux Sociaux

1. **Hameçonnage (Phishing)**

- ✓ "Les attaquants utilisent des emails et des messages semblant légitimes pour subtiliser des informations confidentielles."
- ✓ "Exemple réel: En 2022, des attaquants ont envoyé des emails de phishing très crédibles à des utilisateurs de LinkedIn pour recueillir illicitement leurs informations de connexion.«

1. **Malware**

- ✓ "Les malwares, incluant virus et ransomwares, sont souvent masqués dans des fichiers ou des liens apparemment inoffensifs."
- ✓ "Exemple réel: Une vidéo malicieuse diffusée sur Facebook a conduit à l'infection de milliers d'ordinateurs avec un ransomware qui exigeait une rançon pour déchiffrer les fichiers."

2. Menaces Courantes sur les Réseaux Sociaux

1. Arnaques

- ✓ "Les réseaux sociaux abritent diverses escroqueries, telles que fausses annonces et concours trompeurs."
- ✓ "Exemple réel: Sur Instagram, une arnaque répandue promettait un iPhone gratuit en échange de détails bancaires pour participer à un faux concours."

1. Ingénierie sociale

- ✓ Manipulation psychologique des personnes en les incitant à divulguer des informations confidentielles ou à effectuer des actions qui peuvent compromettre leur sécurité.
- ✓ Attaquants créant des profils fictifs et établissant des relations de confiance pour obtenir des informations sensibles ou influencer les comportements

2. Menaces Courantes sur les Réseaux Sociaux

1. **Usurpation d'identité (Identity theft)**

- ✓ Utilisation par des cybercriminels d'informations personnelles volées pour usurper l'identité de quelqu'un sur les réseaux sociaux, souvent pour commettre des fraudes ou propager des arnaques
- ✓ Création de faux profils utilisant les photos et les détails personnels d'une personne réelle pour tromper ses amis ou sa famille

1. **Fake news et désinformation**

- ✓ Diffusion délibérée de fausses informations ou de contenus trompeurs destinés à manipuler l'opinion publique ou à créer de la confusion.
- ✓ Partage viral de fausses informations concernant des événements actuels qui peuvent influencer les opinions ou provoquer des réactions sociales

2. Menaces Courantes sur les Réseaux Sociaux

1. **Scamming via des applications tierces**

- ✓ Arnaques réalisées à travers des applications qui se connectent à des plateformes de réseaux sociaux, souvent en promettant des fonctionnalités attrayantes pour inciter les utilisateurs à partager des informations personnelles
- ✓ Applications offrant de voir qui a visité votre profil mais qui, en réalité, volent vos données d'identification.

1. **Account hijacking (Détournement de compte)**

- ✓ Accès non autorisé et contrôle d'un compte de réseau social, souvent utilisé pour envoyer des spams ou des messages malveillants.
- ✓ Pirates informatiques qui prennent le contrôle d'un compte Twitter populaire pour diffuser des liens malveillants ou pour mener des campagnes de désinformation

3. Importance des Mots de Passe Forts

1. **Introduction :**
   - ✓ "Un mot de passe fort est votre première ligne de défense contre les accès non autorisés à vos comptes personnels et professionnels."
2. **Statistiques :**
   - ✓ "Selon une étude récente, plus de 80% des violations de données impliquent des mots de passe faibles ou compromis."
3. **Importance :**
   - ✓ "Un mot de passe fort et unique pour chaque compte aide à prévenir le vol d'identité."
   - ✓ "Les mots de passe complexes réduisent le risque d'attaques de force brute et de devinettes."Account hijacking (Détournement de compte)

3. Importance des Mots de Passe Forts

1. Comment Construire un Mot de Passe Sécurisé

- ✓ **Longueur :** "Optez pour des mots de passe d'au moins 12 caractères."
- ✓ **Complexité :** "Utilisez une combinaison de lettres majuscules et minuscules, de chiffres et de symboles."
- ✓ **Unicité :** "Chaque compte devrait avoir un mot de passe unique pour éviter la propagation de dommages en cas de fuite d'un mot de passe.
- ✓ **Exemple :** Évitez "password123" ou "123456", optez plutôt pour quelque chose comme "B@n@n@_M0nK3y!23".
- ✓ **Exemple :** Modifiez vos mots de passe tous les 3 à 6 mois, même si vous n'avez pas de raison apparente de le faire.

2. Ce Qu'il Faut Éviter

- ✓ **Simplicité :** "Évitez les mots de passe basés sur des informations personnelles facilement accessibles, comme les anniversaires, noms de famille ou animaux de compagnie."
- ✓ **Réutilisation :** "Ne recyclez pas les mêmes mots de passe sur plusieurs sites."
- ✓ **Prévisibilité :** "Évitez les suites de chiffres ou de lettres simples, comme '123456' ou 'abcdef'."

3. Utilisation de Gestionnaires de Mots de Passe

1. **Qu'est-ce qu'un gestionnaire de mots de passe ?**
   - ✓ "Un outil qui stocke, génère, et gère vos mots de passe pour tous vos comptes en ligne de manière sécurisée."
2. **Avantages :**
   - ✓ "Crée automatiquement des mots de passe forts et uniques pour chaque compte."
   - ✓ "Vous n'avez besoin de vous souvenir que d'un seul mot de passe maître."
   - ✓ "Synchronisation sécurisée des mots de passe sur différents appareils."
3. **Exemples populaires :**
   - ✓ LastPass, Dashlane, 1Password.

3. Activation de l'Authentification à Deux Facteurs

1. **Définition :**
   - ✓ "L'authentification à deux facteurs (2FA) ajoute une étape supplémentaire de vérification lors de l'accès à vos comptes, en plus de votre mot de passe."
2. **Comment ça fonctionne :**
   - ✓ "Après avoir entré votre mot de passe, un code de vérification vous est envoyé par SMS, email, ou via une application d'authentification."
   - ✓ "Ce code doit être entré pour accéder à votre compte, assurant que seuls les utilisateurs autorisés puissent accéder."
3. **Avantages :**
   - ✓ "Significativement réduit le risque de compromission de compte, même si votre mot de passe est volé."
   - ✓ "Recommandé par les experts en sécurité pour tous les comptes importants, comme les emails, les banques en ligne, et les réseaux sociaux."

4. Conseils pour Sécuriser les Smartphones et Tablettes

- **Mises à Jour Régulières :** Assurez-vous que votre système d'exploitation et toutes les applications sont constamment mis à jour pour bénéficier des derniers correctifs de sécurité.
- **Verrouillage de l'Écran :** Utilisez des méthodes de verrouillage sécurisées tels que les codes PIN, les empreintes digitales ou la reconnaissance faciale pour empêcher l'accès non autorisé à votre appareil.
- **Applications Fiables :** Téléchargez uniquement des applications à partir de sources officielles telles que Google Play Store (Android) ou App Store (iOS). Évitez les applications provenant de sources non vérifiées.
- **Réseau Wi-Fi Sécurisé :** Évitez de vous connecter à des réseaux Wi-Fi publics non sécurisés. Utilisez un réseau privé virtuel (VPN) pour chiffrer votre connexion lorsque vous utilisez des réseaux Wi-Fi publics.
- **Antivirus et Sécurité :** Installez une application antivirus fiable pour détecter et éliminer les logiciels malveillants.

4. Conseils pour Sécuriser les Smartphones et Tablettes

Gestion des Autorisations d'Application

- **Examen des Autorisations :** Avant d'installer une application, examinez attentivement les autorisations demandées. Ne donnez que les autorisations nécessaires à chaque application.
- **Révoquer les Autorisations Inutiles :** Dans les paramètres de votre appareil, vous pouvez révoquer les autorisations d'application, limitant ainsi l'accès à certaines données sensibles.
- **Contrôle des Paramètres de Confidentialité :** Utilisez les paramètres de confidentialité de votre appareil pour contrôler l'accès aux photos, à la localisation, aux contacts, etc.
- **Utilisation des Contôles Parentaux :** Si votre appareil est partagé avec des membres de la famille, utilisez les contrôles parentaux pour gérer l'accès des applications et du contenu.

5. Conseils pour Éviter les Sites Web Malveillants

1. **Vérification de l'URL :** Avant de cliquer sur un lien, assurez-vous de vérifier l'URL. Les sites malveillants peuvent utiliser des URL trompeuses ou similaires à celles de sites légitimes.
2. **Utilisation de Connexions Sécurisées :** Privilégiez les sites Web qui utilisent le protocole HTTPS, indiqué par un cadenas dans la barre d'adresse. Cela garantit une communication chiffrée entre votre navigateur et le site.
3. **Méfiance envers les Pop-ups :** Évitez de cliquer sur des fenêtres pop-up suspectes. Ces pop-ups peuvent être des tentatives de phishing ou contenir des liens malveillants.
4. **Logiciel de Sécurité :** Installez un logiciel de sécurité fiable qui peut détecter et bloquer les sites Web malveillants.
5. **Vérification des Avis :** Avant d'effectuer des transactions en ligne ou de fournir des informations sensibles, vérifiez les avis et la réputation du site.
6. **Correctifs de Sécurité :** Les mises à jour du navigateur incluent souvent des correctifs de sécurité qui comblent les vulnérabilités, protégeant ainsi contre les attaques en ligne.

5. Conseils pour Éviter les Sites Web Malveillants

1. Extensions de Navigateur pour la Sécurité

- ✓ **AdBlock Plus :** Bloque les publicités intrusives et potentiellement malveillantes.
- ✓ **HTTPS Everywhere :** Force les connexions sécurisées en redirigeant automatiquement vers la version HTTPS d'un site lorsque disponible.
- ✓ **NoScript :** Permet de contrôler les scripts exécutés sur les pages web, réduisant les risques d'attaques basées sur des scripts.
- ✓ **Password Manager :** Une extension de gestionnaire de mots de passe, comme LastPass ou 1Password, peut renforcer la sécurité des identifiants en ligne.
- ✓ **Privacy Badger :** Bloque les trackers et autres outils de suivi sur les sites Web, renforçant la confidentialité en ligne.