Sécurité numérique et protection des données

Présenté par :

- *HOUDAIFA FEKIHI*
- *MOHAMED BOGHANEM*

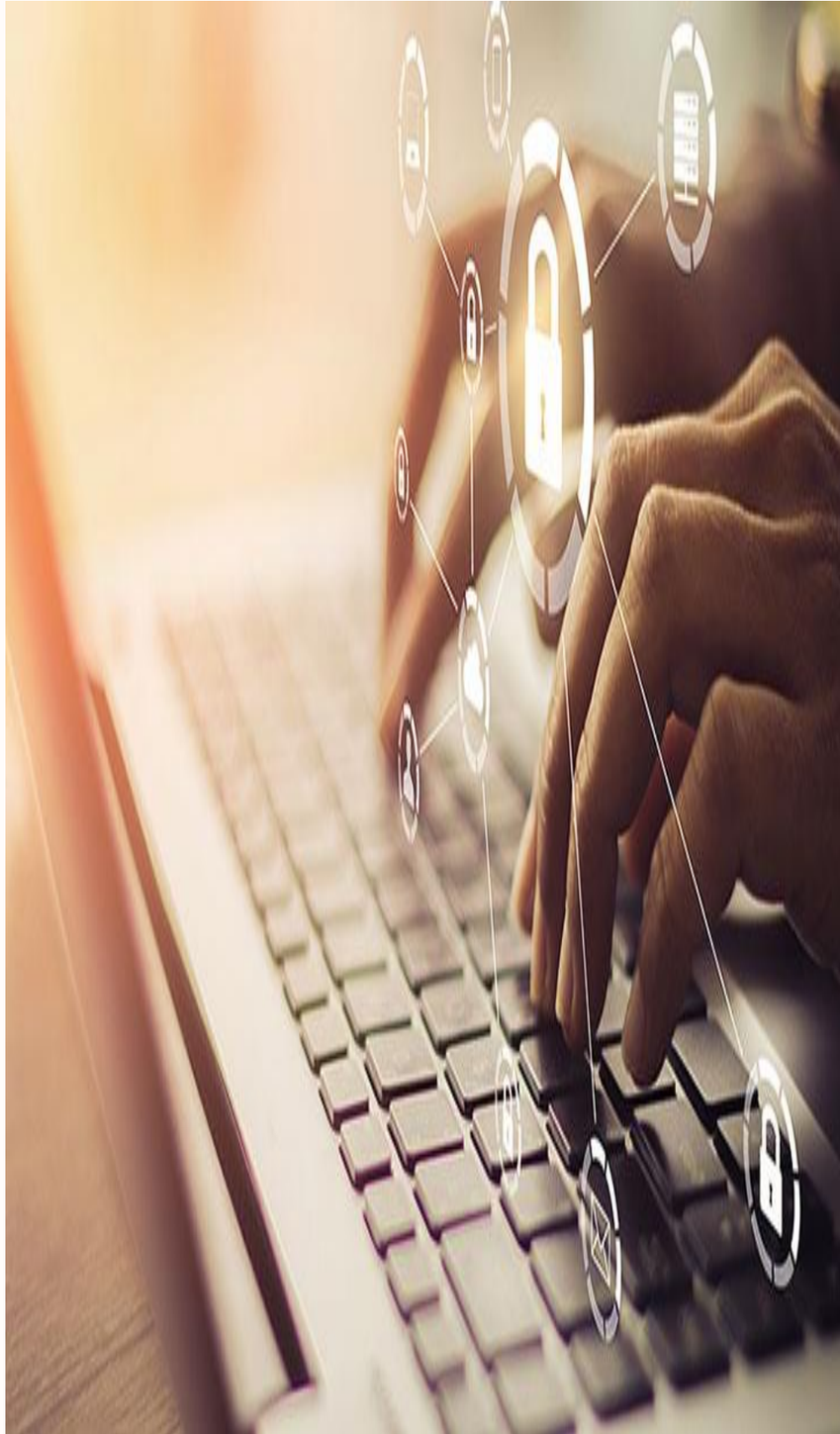
Encadré par :

- **YAHYANI ISSAM**

Introduction :

Aujourd’hui, nous utilisons Internet pour presque tout : communiquer, travailler, étudier...
Mais cela nous expose à des risques : vol de données, virus, piratage.
Il est donc très important de comprendre la sécurité numérique.
La sécurité numérique concerne tout le monde, pas seulement les experts en informatique.

- Sécurité numérique et protection des données
- Comprendre les cyberattaques courantes
- Le pouvoir des mots de passe robustes
- Le rôle des logiciels antivirus
- Conseils de sécurité pour les appareils mobiles
- Meilleures pratiques en matière de sécurité informatique
- Habitudes de navigation sécurisées
- Conclusion : Rester vigilant à l'ère du numérique



Sécurité numérique et protection des données

La sécurité numérique est essentielle en 2024 face à la recrudescence des menaces cybernétiques. Les fuites de données causent de graves dommages financiers et de confidentialité. Les cyberattaques augmentent dans le monde entier chaque année, exigeant une protection plus forte de la part des particuliers et des entreprises.

Comprendre les cyberattaques courantes

Attaques de phishing

Les faux e-mails incitent les victimes à voler des identifiants. Vérifiez attentivement les détails de l'expéditeur.

Types de logiciels malveillants

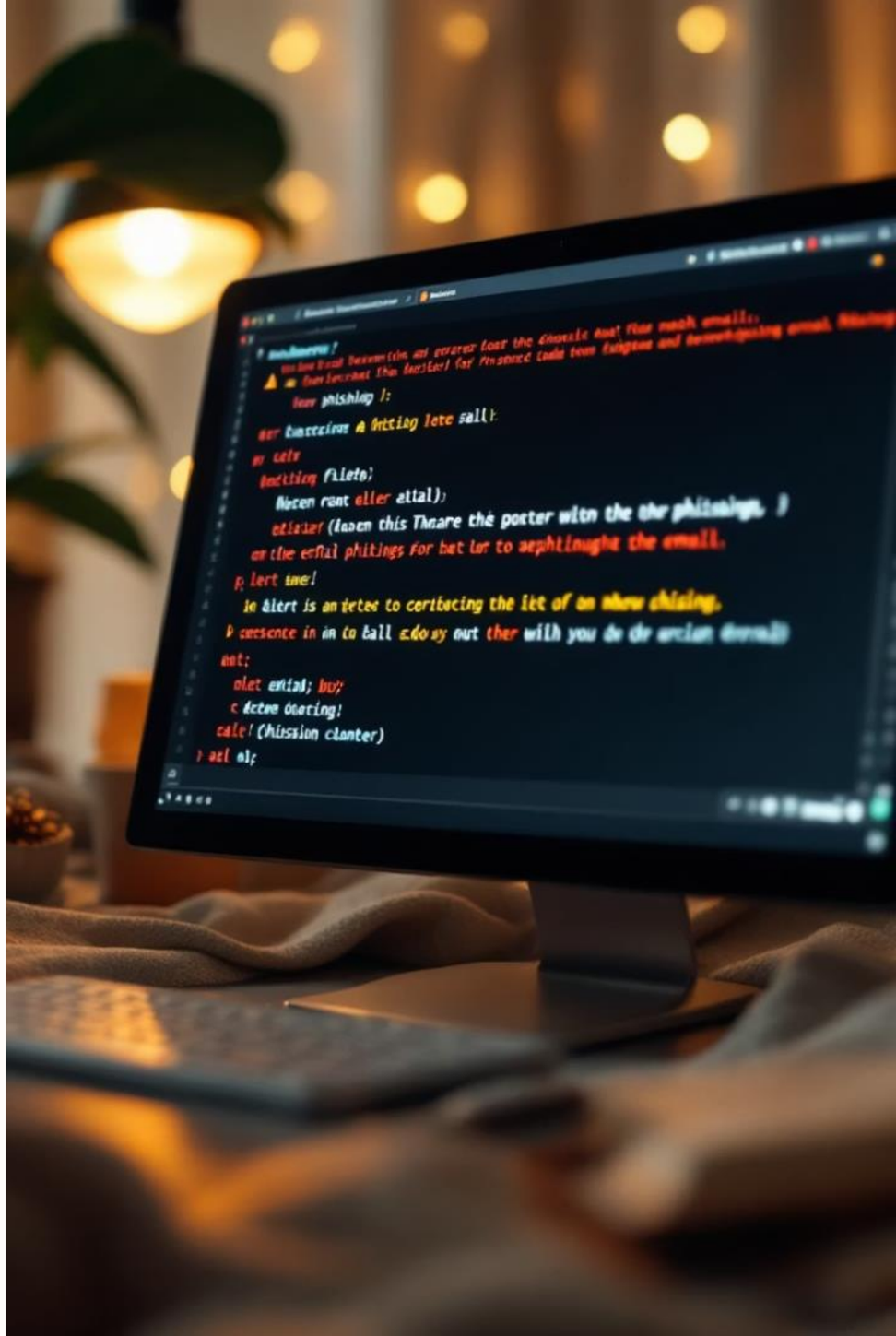
Les virus, vers et chevaux de Troie infectent via les téléchargements ou les liens.

Rançongiciels

Verrouille les fichiers contre une rançon ; prévenez-les avec des sauvegardes et en cliquant avec prudence.

Attaques DDoS

Surcharge les serveurs pour perturber les services ; les grandes entreprises sont des cibles courantes.



Le pouvoir des mots de passe robustes

Solidité du mot de passe

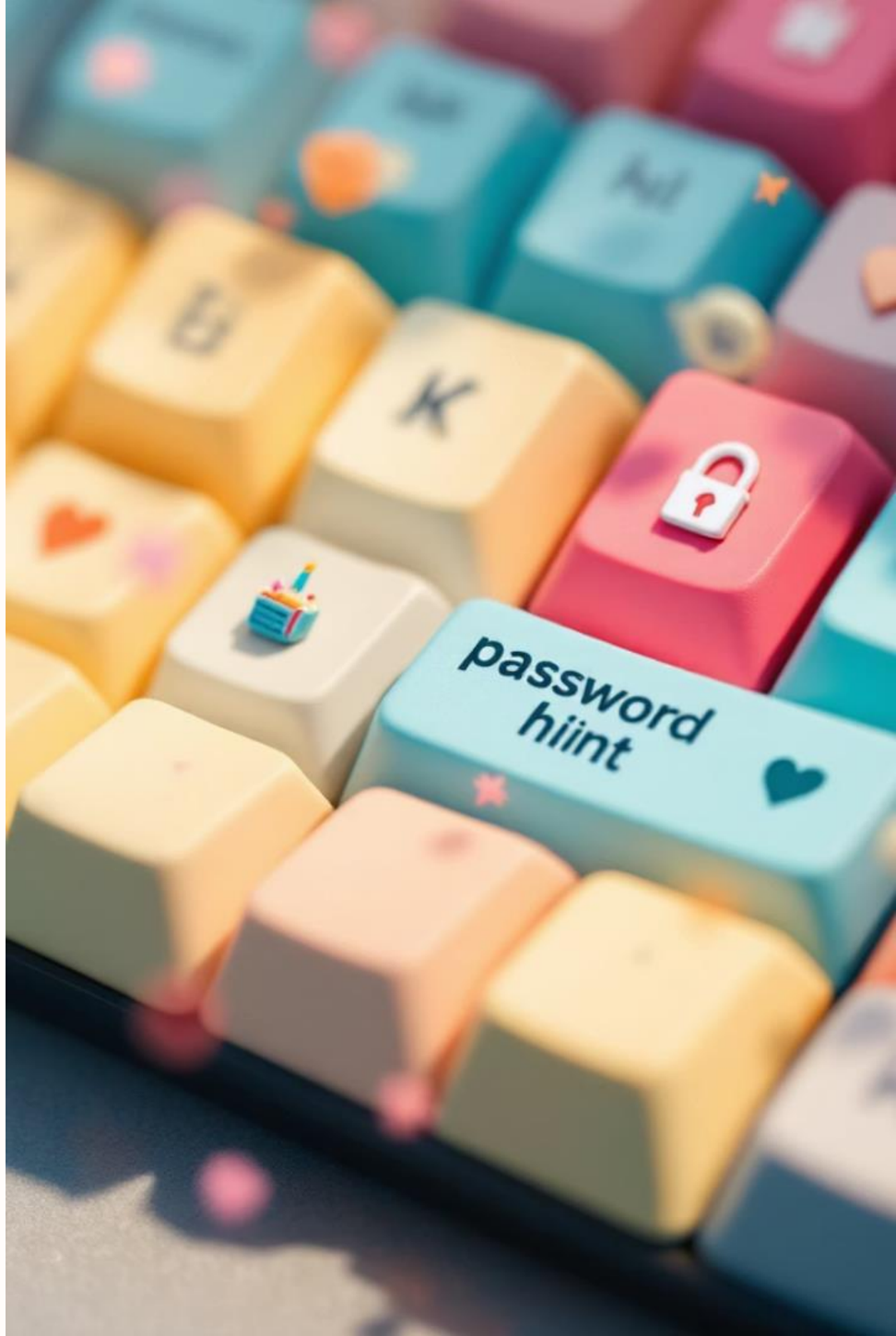
Utilisez des mots de passe longs, complexes et uniques pour chaque compte.

Gestionnaires de mots de de passe

Stockez et générez de manière sécurisée les mots de passe, simplifiant ainsi leur gestion.

Authentification à plusieurs facteurs

Ajoute des couches de vérification supplémentaires au-delà des mots de passe.



Le rôle des logiciels antivirus

Fonctionnalités de protection

Détecte les logiciels malveillants, bloque les menaces et analyse les fichiers en continu.

Types d'analyse

- En temps réel pour une détection instantanée des menaces
- Programmée pour des vérifications approfondies du système

Choix du logiciel

Recherchez les mises à jour, un faible impact sur le système et une couverture complète.

Conseils de sécurité pour les appareils mobiles

Accès sécurisé

Utilisez des codes d'accès, la biométrie et le chiffrement.

Vérification des applications

Examinez les autorisations et installez uniquement à partir de sources de confiance.

Wi-Fi public

Utilisez des VPN pour sécuriser les connexions sur les réseaux ouverts.

Effacement à distance

Activez-le pour effacer l'appareil s'il est perdu ou volé.

Meilleures pratiques en matière de sécurité informatique

Mises à jour de logiciels

Mettez régulièrement à jour le système d'exploitation et les applications pour les correctifs de sécurité.

Utilisation du pare-feu

Configurez les pare-feux pour surveiller et bloquer le trafic non autorisé.

Vigilance dans les e-mails

Évitez de cliquer sur des liens et des pièces jointes suspects.

Sauvegardes de données

Effectuez régulièrement des sauvegardes pour prévenir la perte de données.

Habitudes de navigation sécurisées

1

Repérer les sites de hameçonnage

Vérifiez attentivement les URL et évitez les domaines suspects.

2

Utiliser HTTPS

Assurez-vous que les connexions aux sites Web sont sécurisées et chiffrées.

3

Effacer l'historique

Supprimez régulièrement l'historique de navigation et les cookies.

4

Gérer les extensions

N'installez que des extensions de navigateur vérifiées.

Conclusion : Rester vigilant à l'ère du numérique

Mesures clés

Des mots de passe robustes, un antivirus, des mises à jour et une navigation sécurisée protègent les données.

Sensibilisation continue continue

Restez informé avec les actualités sur la sécurité et les menaces émergentes.

Ressources

Utilisez des sites Web de cybersécurité de confiance pour obtenir des conseils et des alertes.

Appel à l'action

Adoptez des habitudes proactives pour sécuriser votre vie numérique.

Conclusion :

- N'oublions pas que la sensibilisation est tout aussi cruciale. Il est essentiel de former vos collaborateurs et vos proches aux risques numériques et aux bonnes pratiques de sécurité. Cela renforce non seulement la protection de vos données, mais aussi celle de vos environnements professionnels et personnels.

- Merci pour votre attention. Je suis à votre disposition pour répondre à vos questions.