



CYBER SECURITY

"COMPRENDRE LA SÉCURITÉ : PROTÉGER VOS ACTIFS"

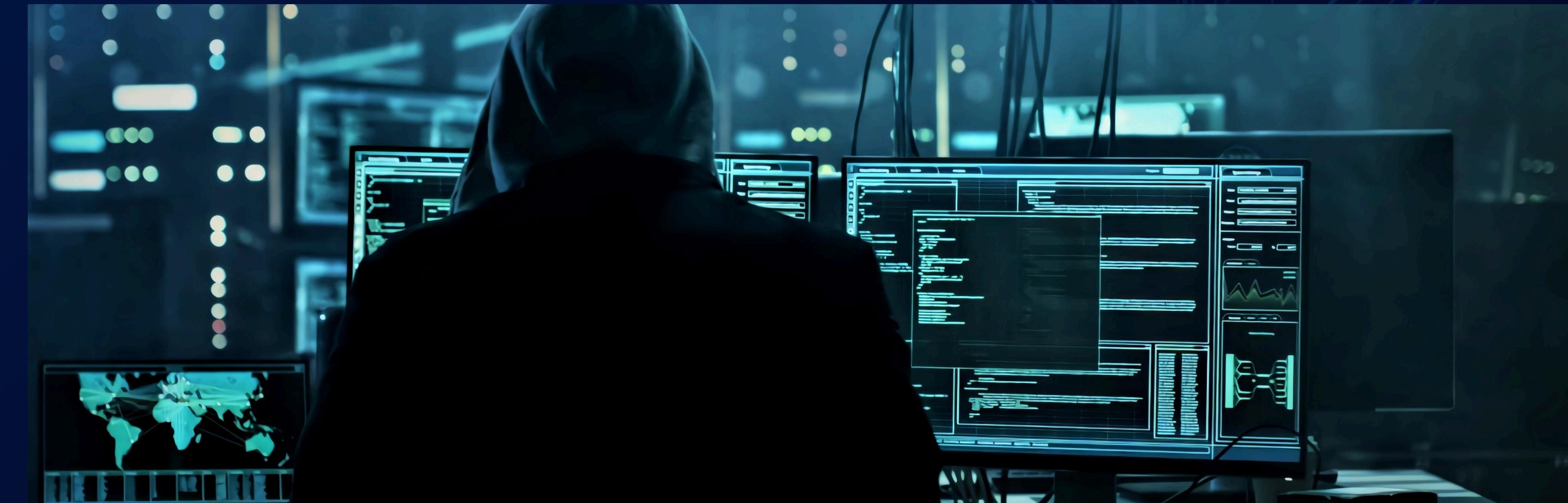
La sécurité informatique est un aspect critique de notre monde numérique en constante évolution. Avec la prolifération des menaces en ligne telles que les logiciels malveillants, les attaques par hameçonnage et les violations de données, la protection de nos informations sensibles est plus importante que jamais.



OBJECTIF

01

Cette présentation vise à approfondir la compréhension de la sécurité informatique et à fournir des conseils pratiques pour protéger efficacement vos données sensibles. Nous aborderons divers sujets, notamment les menaces courantes, les meilleures pratiques de sécurité, la conformité aux réglementations et la gestion des incidents.





TYPES DE MENACES

Cyber menaces :

- Les logiciels malveillants, tels que les virus, les vers et les chevaux de Troie, qui peuvent infecter les systèmes et causer des dommages.
- Les attaques de phishing, qui utilisent des e-mails ou des messages trompeurs pour inciter les utilisateurs à divulguer des informations personnelles ou à installer des logiciels malveillants.
- Les attaques par déni de service (DDoS), qui visent à perturber les services en ligne en submergeant un serveur de demandes.



TYPES DE MENACES

Menaces Physiques :

- Le vol d'ordinateurs ou de dispositifs mobiles contenant des données sensibles.
- L'accès non autorisé aux locaux, pouvant entraîner le vol ou la compromission de matériel informatique.



TYPES DE MENACES

Autres Menaces :

- Les fuites de données causées par des erreurs humaines ou des défauts de sécurité.
- Les vulnérabilités des logiciels et des systèmes qui peuvent être exploitées par des attaquants pour accéder à des informations sensibles.

MESURES DE CYBERSÉCURITÉ :

01

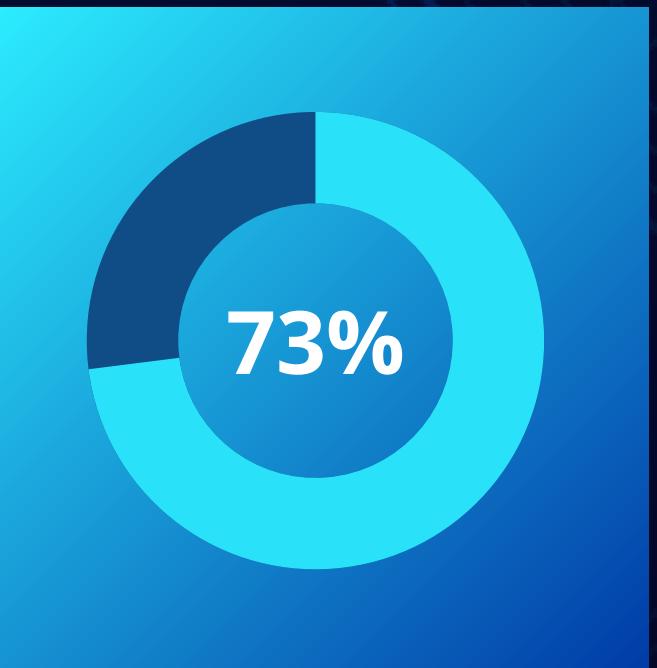
- Utilisation de logiciels antivirus et antimalware pour détecter et supprimer les menaces potentielles.

02

- Configuration de pare-feux pour contrôler le trafic réseau entrant et sortant et bloquer les activités suspectes.

03

- Utilisation de l'authentification à deux facteurs pour renforcer la sécurité des comptes en ligne.



MESURES DE SÉCURITÉ PHYSIQUE :

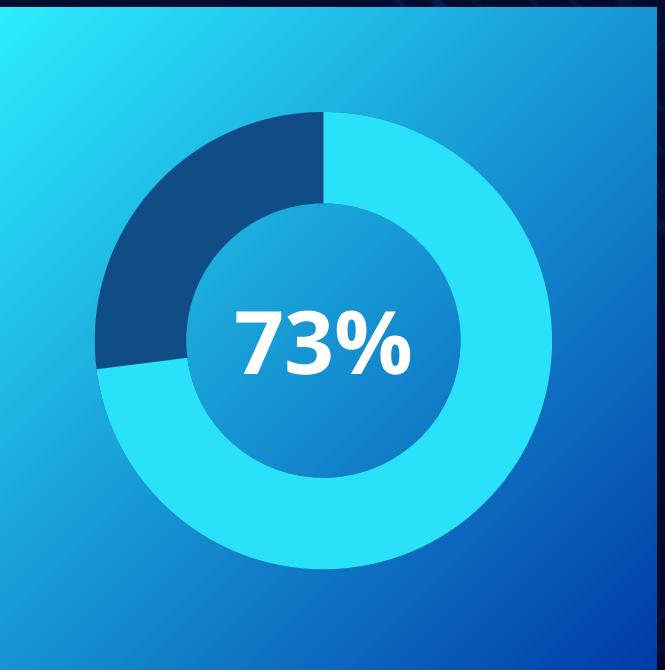
01

- Installation de systèmes de vidéosurveillance pour surveiller les locaux et dissuader les intrusions.



02

- Utilisation de serrures électroniques et de badges d'accès pour limiter l'accès aux zones sensibles.



03

- Mise en place de procédures de sauvegarde régulières pour protéger les données contre la perte ou la corruption.



AUTRES MESURES :

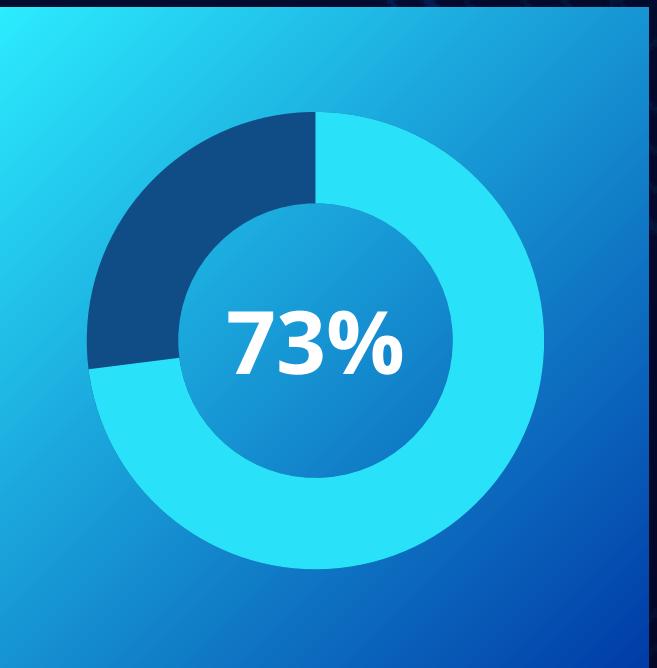
01

- Sensibilisation des utilisateurs aux bonnes pratiques de sécurité, telles que la création de mots de passe forts et la vigilance face aux attaques de phishing.

02

- Mise à jour régulière des logiciels et des systèmes pour corriger les vulnérabilités connues et renforcer la sécurité.

-> Ces mesures de sécurité couvrent à la fois les aspects cybersécuritaires et physiques, offrant ainsi une protection complète contre les menaces potentielles. Dites-moi quand vous êtes prêt pour la prochaine diapositive !





CONCLUSION

La sécurité informatique est une composante essentielle de toute organisation moderne.

En adoptant une approche proactive en matière de sécurité informatique, en investissant dans la formation des employés et en mettant en place des plans de réponse aux incidents, nous pouvons renforcer la résilience de nos organisations face aux menaces émergentes.

THANK
YOU

Home

Video

About Us

Contact

