

Sensibilisation à l'hygiène informatique et à la cybersécurité

Dans un monde de plus en plus connecté, la cybersécurité est devenue un enjeu crucial. Cette présentation vous guidera à travers les concepts clés de l'hygiène informatique et de la cybersécurité en France, vous préparant ainsi à relever les défis du numérique.

Sommaire

1

Organisations en charge de la cybersécurité

Découvrez les acteurs clés qui protègent notre espace numérique en numérique en France.

2

Types de vulnérabilités

Explorez les failles courantes qui menacent notre sécurité en ligne.

3

Exemple de cyberattaque

Analysez un cas concret pour mieux comprendre les risques réels.

CYBERSECURITY INFOGRAPHIC



10, French Cybersecurity Organizations

Supérieur logo no français Cybersecurity Organizations = continue partnerships



Organisations en charge de la cybersécurité en France

La France dispose d'un écosystème robuste d'organisations dédiées à la cybersécurité. Chacune joue un rôle crucial dans la protection de notre espace numérique national.

ANSSI et CNIL : Piliers de la cybersécurité française

ANSSI

- Assure la sécurité des systèmes d'information critiques
- Émet des recommandations et normes de sécurité
- Intervient lors d'incidents majeurs pour garantir la résilience

CNIL

- Veille au respect du RGPD
- Contrôle les pratiques de cybersécurité des entreprises
- Sensibilise le public aux enjeux de la protection des données



CERT-FR et EBIOS : Experts en intervention et analyse



CERT-FR

Détecte, analyse et répond aux incidents de sécurité informatique.



EBIOS

Fournit une méthode d'analyse des risques cyber pour les organisations.



Collaboration

EBIOS travaillent avec l'ANSSI pour renforcer la cybersécurité nationale française.

Types de vulnérabilités

1

Fuite d'informations

Interception ou exfiltration des données sensibles

2

Attaques de type "Man-in-the-Middle"

Interception de données lors d'un transport de paquet

3

Vulnérabilités applicatives

Logiciel non mit à jour

4

Vulnérabilités humaines

Manipulation pour fournir des informations ou exécuté des actions

Types de vulnérabilités

1

Absence de chiffrement ou utilisation de protocoles faibles

Utilisation de protocole non sécurisé

2

Attaques par déni de service (DDoS)

Surcharge d'un serveur ou d'un réseau

3

Exploitation des failles DNS

Manipulations des serveurs DNS

4

Vulnérabilités des périphériques connectés

Appareil connecté peu sécurisé

Types de vulnérabilités

1

Typosquatting

Des noms de domaines proches de ceux de sites légitimes

2

Absence de segmentation des réseaux

Réseau non segmenté

3

Mauvaise gestion des accès et droits utilisateurs

Mauvaise attribution des droits

4

Faibles dans les réseaux Wi-Fi

Manque de précautions sur l'infrastructure réseau

Types de vulnérabilités

1

Utilisation de périphériques amovibles non sécurisés

clés USB ou disques durs infectés

2


Vulnérabilités des VPN mal configurés

Mal sécurisation d'un VPN

Exemple de cyberattaque




Merci d'avoir écouté



ATTESTATION DE SUIVI

L'équipe SecNumacadémie atteste que **shemseddine mammad** a suivi avec succès les cours des quatre modules de MOOC et obtenu les scores suivants aux évaluations

MODULES	DATE DE L'ÉVALUATION	SCORE
PANORAMA DE LA SSI	16/11/2024	84.0%
SÉCURITÉ DE L'AUTHENTIFICATION	16/11/2024	94.0%
SÉCURITÉ SUR INTERNET	16/11/2024	90.0%
SÉCURITÉ DU POSTE DE TRAVAIL ET NOMADISME	16/11/2024	86.0%



Fait le 16 Novembre 2024
L'équipe SecNumacadémie

www.secnumacademie.gouv.fr