aminasecurit20@gmail.com

AMINA-SECURITY INFORMATIQUEA

Centre de formation et d'expertise en informatique et cybersécurité.

www.aminasecurityinformatique.com

CYBERSECURITE

Renforcer sa sécurité numérique : les bonnes pratiques pour une protection efficace en ligne

ETS ASI

INTRODUCTION

Dans un monde de plus en plus connecté, la cybersécurité devient un enjeu majeur aussi bien pour les particuliers, les entreprises, les administrations que les étudiants. Les cyberattaques se multiplient et touchent désormais tous les secteurs.

Cette conférence a pour objectif de sensibiliser le public aux risques numériques actuels et de présenter des solutions simples, pratiques et accessibles pour mieux se protéger au quotidien.

Présenter par: Ing Oumar Hissein Hassan

ETS ASI

PROGRAMME DE LA CONFÉRENCE

- ✔ Comprendre les menaces numériques actuelles
- ✔ Adopter les bons réflexes face aux cyberattaques
- ✔ Protéger ses comptes et ses données personnelles
- ✔ Sensibilisation à la cybersécurité pour tous

Présenter par: Ing Oumar Hissein Hassan

ETS ASI

POURQUOI PARLER DE CYBERSÉCURITÉ ?

Parler de cybersécurité est devenu essentiel parce qu'une grande partie de nos activités dépend aujourd'hui du numérique : téléphones, banques, réseaux sociaux, administrations, hôpitaux, entreprises, transports, etc. Quand ces systèmes sont attaqués ou mal protégés, les conséquences peuvent être très concrètes.

ETS ASI

LES PRINCIPALES MENACES NUMÉRIQUES

Le phishing (Hameçonnage)

Technique de fraude où un attaquant se fait passer pour une personne ou une organisation de confiance (banque, réseau social, administration) afin de tromper la victime et lui voler des informations sensibles comme des mots de passe, numéros bancaires ou codes secrets. Cela se fait souvent par e-mail, SMS ou faux sites web.

Les logiciels malveillants (Malwares)

Programmes informatiques conçus pour nuire à un appareil, voler des données ou prendre le contrôle d'un système. Les malwares incluent les virus, chevaux de Troie, ransomwares et logiciels espions.

Le piratage des comptes et mots de passe

Action consistant à accéder illégalement au compte d'une personne en découvrant, volant ou devinant son mot de passe. Les pirates utilisent parfois des logiciels, des fuites de données ou des techniques de manipulation pour récupérer ces informations.

Les réseaux Wi-Fi publics non sécurisés

Réseaux Internet accessibles au public (cafés, hôtels, aéroports, etc.) qui ne sont pas suffisamment protégés. Des cybercriminels peuvent intercepter les données échangées sur ces réseaux, comme les mots de passe ou informations personnelles.

ETS ASI

LE PHISHING (HAMEÇONNAGE)

Technique de fraude où un attaquant se fait passer pour une personne ou une organisation de confiance (banque, réseau social, administration) afin de tromper la victime et lui voler des informations sensibles comme des mots de passe, numéros bancaires ou codes secrets. Cela se fait souvent par e-mail, SMS ou faux sites web.

Mots de passe,

Informations bancaires,

Données personnelles.

Les cybercriminels utilisent :

- de faux emails,
- de faux SMS,
- de faux liens,
- ou de faux sites web.

ETS ASI

LES LOGICIELS MALVEILLANTS (MALWARES)

Sont des logiciels conçus pour :

- voler des données,
- espionner les utilisateurs,
- bloquer les systèmes,
- endommager les appareils.

Types fréquents :

- Virus
- Spywares
- Trojans
- Ransomwares

ETS ASI

LE LIEN MALVEILLANT

✓ http://exemple.com/cadeau-gratuit ✓ https://2024-program.xyz/airtelrewards.html

✓ Clique ici pour aller sur Google

- ❑ Atteinte à la réputation en ligne
- ❑ Perte de données
- ❑ Propagation de malwares
- ❑ Compromission de la sécurité en ligne
- ❑ Vol d'informations sensibles

ETS ASI

SE PROTÉGER DES LIENS MALVEILLANTS

Un lien malveillant est un lien frauduleux créé par des cybercriminels pour tromper l'utilisateur afin de :

- voler des informations personnelles,
- pirater un compte,
- ou installer un logiciel malveillant sur un appareil.

SCAMDOC

A presentation is a formal talk, often delivered in front of an audience, aimed at conveying information, persuading others, or sharing insights on a particular topic.

VIRUSTOTAL

A presentation is a formal talk, often delivered in front of an audience, aimed at conveying information, persuading others, or sharing insights on a particular topic.

GOOGLE SAFE BROWSING

A presentation is a formal talk, often delivered in front of an audience, aimed at conveying information, persuading others, or sharing insights on a particular topic.

URLVOID

A presentation is a formal talk, often delivered in front of an audience, aimed at conveying information, persuading others, or sharing insights on a particular topic.

CHECKSHORTURL

A presentation is a formal talk, often delivered in front of an audience, aimed at conveying information, persuading others, or sharing insights on a particular topic.

TABLEAU DE BORD DE GOUVERNANCE
CYBERSÉCURITÉ : CADRE STRATÉGIQUE

SAUVEGARDES RÉGULIÈRES (DISQUES & CLOUD)

Sauvegardes chiffrées hebdomadaires.

Statut: **Conforme.**

GESTION DES VERSIONS LOGICIELS

Processus d'application des correctifs critique.

Statut: **Conforme.**

DÉPLOIEMENT ANTIVIRUS D'ENTREPRISE

Surveillance et mises à jour en temps réel.

Statut: **Conforme.**

AUTHENTIFICATION MULTI-FACTEURS (MFA)

Déploiement MFA obligatoire sur tous les comptes.

Statut: **Conforme.**

GESTION DES ACCÈS ET PRIVILÈGES

Principe du moindre privilège appliqué.

Statut: **Conforme.**

PROTÉGER LES DONNÉES PERSONNELLES

Conformité à la protection des données.

Statut: **Conforme.**

ÉVITER LIENS ET FICHIERS SUSPECTS

Analyse automatisée et formation continue.

Statut: **Conforme.**

RECONNAÎTRE EXTENSIONS DE FICHIERS DOUTEUSES

Contrôle des types de fichiers et blocage.

Statut: **Conforme.**

VÉRIFIER L'ORIGINE DES MESSAGES (PHISHING)

Authentification de l'expéditeur et alertes.

Statut: **Conforme.**

SÉCURISATION DES RÉSEAUX ET WIFI

Réseaux d'entreprise et invités sécurisés.

Statut: **Conforme.**

TÉLÉCHARGER VIA SOURCES OFFICIELLES

Utilisation de sources vérifiées et signées.

Statut: **Conforme.**

STRATÉGIE DES MOTS DE PASSE

Exigences de complexité et rotation.

Statut: **Conforme.**

SURVEILLANCE DES INCIDENTS (SOC)

Surveillance 24/7 et triage des alertes.

Statut: **En cours.**

PLAN DE RÉPONSE AUX INCIDENTS (IRP)

Contain → Eradicate → Recover

Plan testé et prêt à l'emploi.

Statut: **Conforme.**

FORMATION ET SENSIBILISATION (CULTURE)

Tremion modules

Phish test résultas

Statut: **Conforme.**

GOUVERNANCE ET CULTURE CYBERSÉCURITÉ

Responsabilités et KPI de sécurité définis.

Statut: **Conforme.**

ETS ASI

MERCI POUR VOTRE SUIVI ATTENTIF

+235 66221695 WWW.AMINASECURITYINFORMATIQUE.COM N'DJAMENA-TCHAD