Phishing
ou hameçonnage

Le phishing est une technique de fraude visant à obtenir des informations sensibles telles que des noms d'utilisateur, des mots de passe et des détails de carte de crédit en se faisant passer pour une entité de confiance dans une communication électronique.

Cryptographie

La cryptographie est la pratique et l'étude des techniques permettant de sécuriser la communication en présence de tiers, en chiffrant les informations pour qu'elles ne soient lisibles que par les destinataires autorisés.

Facteurs d'authentification

la connaissance, la possession ou encore les caractéristiques biométriques.

Ransomware

Un ransomware est un type de malware qui chiffre les fichiers de la victime et exige une rançon pour fournir la clé de déchiffrement.

RGPD

Le RGPD est un règlement de l'Union européenne sur la protection des données et la vie privée de tous les individus au sein de l'UE et de l'Espace économique européen (EEE).

Quels sont les signes d'une infection par malware ?

Ralentissement du système, pop-ups indésirables, programmes inconnus qui s'exécutent, comportements inhabituels du système, et accès non autorisé à des fichiers.

Que faire en cas de réception d'un email de phishing ?

Ne pas cliquer sur les liens ou ouvrir les pièces jointes, signaler l'email comme phishing à l'administrateur système, et supprimer l'email.

Quelles sont les étapes de réponse à un incident de sécurité ?

Identification, confinement, éradication, récupération, et leçons apprises.

## Attaque par Déni de Service (DDoS)

Une attaque par déni de service distribué (DDoS) est une attaque dans laquelle plusieurs systèmes compromis sont utilisés pour cibler un seul système, provoquant une surcharge de trafic et rendant le service inaccessible.

## Attaque de l'Homme du Milieu (Man In The Middle)

Une attaque MITM se produit lorsqu'un attaquant intercepte et éventuellement modifie les communications entre deux parties sans qu'elles en soient conscientes.

Cross-Site Scripting (XSS)

Une attaque XSS injecte des scripts malveillants dans les pages web vues par d'autres utilisateurs, souvent via des entrées utilisateur non sécurisées.

Injection SQL

Une injection SQL est une technique d'attaque qui exploite des failles dans une application web pour exécuter des commandes SQL malveillantes sur la base de données de l'application.

Cheval de Troie (Trojan)

Un cheval de Troie est un type de malware qui se déguise en logiciel légitime pour inciter les utilisateurs à l'installer, permettant ensuite à l'attaquant d'accéder au système infecté.

Malware

Le malware est un terme général désignant tout logiciel conçu pour endommager, perturber ou obtenir un accès non autorisé à un système informatique. Les types de malwares incluent les virus, les chevaux de Troie, les vers et les ransomwares.

## Botnet

Un botnet est un réseau de machines infectées par un malware et contrôlées par un attaquant pour exécuter des tâches automatisées, souvent à des fins malveillantes comme les attaques DDoS.

## Zero-Day Attack

Une attaque Zero-Day exploite une vulnérabilité logicielle inconnue du fabricant ou non corrigée, rendant difficile la défense contre ce type d'attaque.

Attaque par Brute Force

Une attaque par force brute tente de deviner les identifiants de connexion en essayant toutes les combinaisons possibles jusqu'à trouver la bonne.

Social Engineering

Le social engineering est une technique d'attaque qui manipule les individus pour qu'ils divulguent des informations confidentielles, souvent par la tromperie ou la persuasion. (Voir attaque du président)

L'usage d'outils pour obtenir les clés Wifi et accéder au réseau Wifi du voisin est il légal ?

C'est illégal.
cela peut tomber sous le coup des lois suivantes :
Vigipirate, Godfrain, Hadopi, Patriot Act.

Quelle est la technologie la plus appropriée pour sécuriser son accès Wifi ?

~~WEP~~
~~WPA~~
~~WPS~~
WPA2

Lorsque la clé utilisée pour transformer un texte en clair en texte illisible est la même pour rendre, le texte illisible en texte en clair, on parle de ?

Chiffrement symétrique

Lorsque pour envoyer un message privé à Bob, Alice utilise la clé publique de Bob pour rendre « illisible » le « texte en clair », et que Bob utilise sa clé privée pour transformer le texte «illisible » en « texte en clair », on parle de ?

Chiffrement Asymétrique

DMZ (Demilitarized Zone)

Une DMZ est une zone physique ou logique dans un réseau qui sépare le réseau interne d'une organisation du réseau externe (Internet). Elle contient des ressources accessibles publiquement tout en limitant les risques pour le réseau interne.

Parmi les quatres propositions suivantes, quel est le mot de passe le plus robuste ?

password12345678

monreveloetaitturquoise

QXiL-2Bq3-6u22

HiP@sswd38

QXiL-2Bq3-6u22

Régulièrement, je navigue sur des sites Internet sécurisés (HTTPS). Grâce à cette sécurité, je peux sans risque, utiliser les mêmes identifiants et mots de passe pour tous ces sites.

FAUX

Pour corriger les failles de sécurité dans mon logiciel favori, il faut

Télécharger la nouvelle version du logiciel sur le site de l'éditeur

Lorsque je suis en déplacement, en me connectant aux réseaux WiFi disponibles, je peux surfer sur Internet sans crainte

NON

Un attaquant peut accéder librement aux appareils non sécurisés présents sur le même réseau.
Un attaquant peut utiliser une attaque de type Man In The Middle.

La messagerie est aujourd'hui un moyen de communication sûr. Grâce à l'anti-spam, je peux ouvrir sans crainte tous les emails que je reçois

FAUX

Exemple : hameçonnage, malware en pièce jointe ...

Un agent du service informatique me contacte depuis son téléphone mobile pour m'informer qu'un virus a été détecté sur mon ordinateur. Pour supprimer le virus, le technicien a besoin de mon mot de passe. Que faites-vous ?

Je refuse de communiquer mon mot de passe à qui que ce soit !

Vous êtes victime d'un ransomware (rançongiciel), quel est votre premier réflexe ?

Déconnecter votre ordinateur du réseau

Grâce à la législation qui protège mes données personnelles, comme le RGPD, je peux utiliser les réseaux sociaux sans crainte car je garde le contrôle de mes données

FAUX

La messagerie est aujourd'hui un moyen de communication sûr. Grâce à l'anti-spam, je peux ouvrir sans crainte tous les emails que je reçois

FAUX

Exemple : hameçonnage, malware en pièce jointe ...