Cartes Défis

Pour les cartes 1 à 7 possibilité d'indiquer la liste des malwares suivante : Virus, phishing, botnet, cheval de troie, déni de service (DOS), spyware, ransomware

CARTE D1 :

"Je suis une attaque qui rend un service indisponible et qui empêche les utilisateurs légitimes de l'utiliser" (Réponse : DOS)

CARTE D2 :

"Je suis un programme qui chiffre les fichiers et demande une rançon pour les déchiffrer." (Réponse : Ransomware)

CARTE D3 :

"Je suis un programme qui enregistre les frappes du clavier, la webcam, le micro …" (Réponse : Spyware)

CARTE D4 :

"Je suis un réseau de robots informatiques contenant des programmes malveillants qui communiquent entre eux par Internet pour exécuter des tâches." (Réponse : Botnet)

CARTE D5 :

"Je suis un programme qui s'attache à un autre pour modifier ou altérer son fonctionnement." (Réponse : Virus)

CARTE D6 :

"Je suis un programme qui permet à un attaquant de prendre le contrôle de l'ordinateur cible." (Réponse : Cheval de Troie)

CARTE D7 :

"Je suis un message qui ressemble à un mail légitime et qui vous demande d'entrer vos informations personnelles, vos identifiants de connexion et/ou vos coordonnées bancaires à la suite d'une erreur sur un de vos comptes bancaires. (Réponse : Phishing)

CARTE D8 :

Quelles est la différence entre les sauvegardes "différentielles" et les sauvegardes "entières" ?
(Réponse : Les sauvegardes différentielles vont comparer les changements entre la dernière sauvegarde et l'état actuel du document et enregistreront les changements par version (sauvegarde plus rapide). Les sauvegardes "entières" synchroniseront à chaque fois toutes les données sans faire de comparatif entre les données sources et celles sauvegardées (sauvegarde plus longue).)

CARTE D9 : Défi pour tous les joueurs (5 indices à donner le plus vite possible, 3 pts par indices)

Quels sont les éléments pouvant indiquer qu'il s'agit probablement d'un mail de phishing ?
Réponse :
- Les courriels malveillants sont souvent envoyés à destination d'un grand nombre de cibles, ils ne sont pas ou peu personnalisés
- Le message évoque un dossier, une facture, un thème qui ne vous parle pas
- L'expéditeur vous est inconnu (ne fait pas partie de votre liste de contacts)
- Le niveau de langage du courriel est médiocre
- Il contient un lien dont la destination est douteuse

CARTE D10 :

Qu'est-ce que le "social engineering" ?
(Réponse : L'influence interpersonnelle afin d'obtenir des informations sensibles en matière de sécurité)

CARTE D11 :

Ai-je besoin d'un antivirus pour mon smartphone ?
A- Non, le smartphone ne peut pas être attaqué
B- Non, le plus important est que les applications proviennent d'une source digne de confiance, et de ne pas prêter son portable
C- Oui, c'est tout aussi important que sur PC
(Réponse : B)

CARTE D12 :

La sécurité des données augmente …
A- si tous les collaborateurs communiquent leurs mots de passe au responsable informatique
B- si tous les collaborateurs n'ont pas les mêmes droits d'accès
C- si tous les collaborateurs savent où les données sont stockées
(Réponse : B)

CARTE D13 : Défi pour tous les joueurs (4 réponses à donner le plus vite possible, 2 pts par réponse)

Je suis salarié(e) et possède un post de travail dans mon entreprise -Que puis-je faire pour éviter tout vol d'information à mon insu ?

Réponses :

- Verrouiller ma session lors de pause et à la fin de la journée de travail
- Accompagner les visiteurs dans leurs déplacements
- Être discret lors de mes déplacements
- Maintenir mon matériel à jour

CARTE D14 :

Que signifie l'acronyme DIC en sécurité de l'information ?

Disponibilité, Intégrité, Confidentialité

CARTE D15 :

Qu'est-ce qui repose sur le principe d'authentification ?
A- Le contrôle d'accès
B- le contrôle de mandat
C- Le contrôle des identités
(Réponse : A)

CARTE D16 :

Quels facteurs utilise-t-on pour prouver son identité ?
A- les facteurs d'identification
B- les facteurs d'autorisation
C- les facteurs d'authentification
D- les facteurs de consultation
(Réponse : C)

CARTE D17 :

Comment nomme-t-on un mécanisme d'authentification qui met en œuvre plusieurs facteurs d'authentifications ?
A- Authentification forte
B- Authentification simple
C- Authentification robuste
(Réponse A)

CARTE D18 :

Parmi les propositions suivantes, quelle est la mesure de renforcement d'authentification la plus sûre ?
A- Envoi d'un SMS
B- Question secrète
C- Saisie de votre code postal
(Réponse : A, c'est une authentification forte)

CARTE D19 :

Pour quelle(s) raison(s) ce mot de passe ne peut être considéré comme suffisamment sécurisé : "Ma_fiLlE_SapPelLE_CeCiLe" ? (Réponse complète = 3 pts, réponse incomplète et/ou incorrecte = 0 pts)
A- Il est trop court
B- il se réfère à un mot du dictionnaire
C- Le jeu de caractères est insuffisamment varié
D- Un élément de logique ou un rapport psycho-social est présent
(Réponse B et D)

CARTE D20 :

Pour quelle raison ce mot de passe ne peut être considéré comme suffisamment sécurisé : "8T@b6" ?
A- Il est trop court
B- il se réfère à un mot du dictionnaire
C- Le jeu de caractères est insuffisamment varié
D- Un élément de logique ou un rapport psycho-social est présent
(Réponse A)

CARTE D21 :

Puis-je me connecter sans risques avec mes identifiants auprès d'un site internet commençant par "http" ?
(Réponse : Non, lors d'une authentification auprès d'un service via un navigateur internet, il est primordial que ce soit par le protocole HTTPS)

CARTE D22 : Défi pour tous les joueurs (3 réponses à donner le plus vite possible, 2 pts par réponse)

Donnez des méthodes mnémotechniques pour créer un mot de passe.
Réponse : Phrase de passe / Méthode phonétique / Méthode des premières lettres

CARTE D23 :

Quelle bonne pratique peut permettre d'identifier un message frauduleux ?
A- Créer des adresses électroniques différentes en fonction de vos usages
B- Utiliser un mot de passe robuste
C- Ne pas utiliser sa machine personnelle pour des usages professionnels
(Réponse : A)

CARTE D24 : Défi pour tous les joueurs (5 réponses à donner le plus vite possible, 2 pts par réponse)

Citer des recommandations devant être suivies pour préserver la sécurité de ses données.
Réponses :

- Ne pas prêter son matériel
- Créer différents comptes avec des droits différents
- Effectuer des sauvegardes régulières
- Respecter les systèmes d'authentification
- Activer le verrouillage automatique sur les matériels

CARTE D25 :

Je suis salarié(e) dans une entreprise, quels sont les risques associés à l'utilisation d'un compte administrateur pour travailler au quotidien ? (2 réponses, 1 point par bonne réponse)
Réponse :

- Répandre une contamination sur le réseau de l'entreprise
- Installer des programmes malveillants

CARTE D26 :

Quel compte permet d'utiliser le système avec l'accès le plus restreint ? (2 points)
A- Compte administrateur
B- Compte invité
C- Compte utilisateur
(Réponse : B, il permet d'utiliser le système, mais ne permet pas de conserver ses données d'une session à une autre, il ne dispose d'aucun privilège)

CARTE D27 : Défi pour tous les joueurs (3 réponses à donner le plus vite possible, 2 pts par réponse)

Quels sont les principes associés à la séparation des usages ?
Réponses :

- Utiliser des mots de passe différents pour chaque site/application
- Utiliser des comptes avec des droits différents
- Utiliser plusieurs comptes de messagerie électronique (professionnel/personnel)

CARTE D28 :

La BYOD consiste à ...
A- Faire du télétravail
B- Rapporter du travail à la maison
C- Utiliser son ordinateur professionnel pour une activité personnelle
D- Travailler avec son ordinateur personnel
(Réponse : D)

CARTE D29 :

Comment sont désignés les chercheurs qui identifient des failles et les exploitent pour leur propre intérêt ?
(Réponse : Black hats)

CARTE D :30

Vrai ou Faux, Installer un deuxième antivirus permet de renforcer la sécurité de son matériel ?
(Réponse : Faux, cette pratique est déconseillée, car les logiciels de sécurité de même type, peuvent présenter des incompatibilités.)

CARTE D31 :

Qu'est-ce qu'une faille 0-day ?
A- Une faille inconnue de son éditeur
B- Une vulnérabilité virtuellement impossible à exploiter
C- Une faille découverte avant la sortie du logiciel
D- Une faille découverte le jour de la sortie du logiciel
(Réponse : A)