CYBERDEF101-Cyberedu-QUIZZ 2

1. **Cyberedu-QUIZZ-ID-2.1**

   Donner 2 exemples de données électroniques sensibles pour un étudiant :

   (a) Adresse postale (0%)
   (b) Nom et numéro de sécurité sociale (50%)
   (c) Numéro de carte bancaire (50%)
   (d) Nom de famille (0%)

2. **Cyberedu-QUIZZ-ID-2.2**

   Donner 2 exemples de données électroniques sensibles pour une université/école :

   (a) Le nom et l'origine de l'université (0%)
   (b) Les noms des professeurs (0%)
   (c) Les brevets déposés (50%)
   (d) Les épreuves d'examens à venir (non encore passés) (50%)

3. **Cyberedu-QUIZZ-ID-2.3**

   Dans un réseau, qu'est-ce qu'on entend par une zone de confiance?

   (a) Le hotspot wifi offert aux visiteurs, exemple à la gare SNCF (0%)
   (b) Le réseau interne (où sont hébergés les postes des utilisateurs et les serveurs) (100%)
   (c) Le réseau Internet (0%)
   (d) Une zone démilitarisée (DMZ) (0%)

4. **Cyberedu-QUIZZ-ID-2.4**

   Quand parle-t-on d'une authentification mutuelle entre deux entités?

   (a) Lorsque des deux entités sont administrées par la même personne (0%)
   (b) Lorsque chacune des entités doit s'authentifier vis-à-vis de l'autre (100%)
   (c) Lorsque la communication entre les deux entités est chiffrée (0%)
   (d) Lorsque les deux entités sont situées sur le même réseau (0%)

5. **Cyberedu-QUIZZ-ID-2.5**

   Dans un réseau, l'usage du BYOD peut entrainer (choisir la (ou les) proposition(s) vraie(s)) :

   (a) Une restriction du périmètre à sécuriser (0%)
   (b) La propagation de codes malveillants (50%)
   (c) La fuite de données de l'entreprise (50%)
   (d) Une meilleure sécurité du SI (0%)

6. **Cyberedu-QUIZZ-ID-2.6**

   Quel est le principe célèbre en matière de gestion de flux sur un réseau?

   (a) Tout ce qui n'est pas autorisé est interdit (100%)
   (b) Tout ce qui est autorisé n'est pas interdit (0%)
   (c) Tout ce qui est interdit est interdit (0%)

7. **Cyberedu-QUIZZ-ID-2.7**

   Un pare-feu peut être aussi bien matériel (appliance dédiée) que logiciel?

   (a) Vrai (100%)
   (b) Faux (0%)

8. **Cyberedu-QUIZZ-ID-2.8**

   Entourer la (ou les) proposition(s) vraie(s) qui peut (ou peuvent) servir de mesure de sécurisation des accès distants à un réseau :

   (a) Utiliser un serveur d'authentification centralisé comme TACACS+ (50%)
   (b) Utiliser Internet (0%)
   (c) Utiliser un protocole sécurisé tel que telnet ou ftp (0%)
   (d) Utiliser un VPN (50%)

9. **Cyberedu-QUIZZ-ID-2.9**

   Entourer la (ou les) bonne(s) mesure(s) de sécurisation de l'administration

   (a) Rendre les interfaces d'administration disponibles à tous depuis Internet (0%)

(b) Tous les administrateurs doivent utiliser le même compte pour se connecter (0%)
(c) Utiliser un réseau dédié pour l'administration (50%)
(d) Authentifier mutuellement les postes des administrateurs et les serveurs à administrer. (50%)

10. **Cyberedu-QUIZZ-ID-2.10**

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

(a) WEP (0%)
(b) WPA (0%)
(c) WPS (0%)
(d) WPA2 (100%)

11. **Cyberedu-QUIZZ-ID-2.11**

Entourer la (ou les) proposition(s) vraie(s) lors de l'usage d'un hotspot Wifi?

(a) Il peut s'agir d'un faux point d'accès ; (50%)
(b) Les autres personnes connectées peuvent voir mes communications (50%)
(c) Je suis protégé des personnes malveillantes (0%)
(d) Je suis sur un réseau de confiance, je peux désactiver mon pare-feu. (0%)

12. **Cyberedu-QUIZZ-ID-2.12**

Pourquoi vérifier l'intégrité d'un logiciel?

(a) Pour m'assurer qu'il ne contient pas de virus (0%)
(b) Pour m'assurer que le logiciel que je télécharge n'a pas été corrompu (100%)
(c) Pour m'assurer que le logiciel fonctionne bien comme promis (0%)
(d) Pour m'assurer qu'il est gratuit (0%)

13. **Cyberedu-QUIZZ-ID-2.13**

Laquelle (ou lesquelles) des expressions suivantes est (sont) vraie(s) pour un logiciel téléchargeable?

(a) toujours gratuit (0%)
(b) Peut être open source (33.33333%)
(c) Peut contenir des logiciels espions (33.33333%)
(d) Peut être un programme malveillant (33.33333%)

14. **Cyberedu-QUIZZ-ID-2.14**

Citer une bonne pratique de configuration de son antivirus

(a) Avoir un antivirus d'un éditeur connu (0%)
(b) Avoir un jour installé un antivirus (0%)
(c) Tenir son antivirus à jour (mise à jour des signatures et du moteur) (100%)
(d) Interdire l'analyse antivirale à certains répertoires ou périphériques. (0%)

15. **Cyberedu-QUIZZ-ID-2.15**

Sélectionner la (ou les) proposition(s) vraie(s) parmi les suivantes. Un antivirus:

(a) peut détecter tous les virus et programmes malveillants, y compris ceux non découverts (0%)
(b) protège de toutes les menaces (0%)
(c) ne peut détecter que les virus qui sont connus dans sa base de signatures (50%)
(d) doit être actif, et à jour pour être utile (50%)

16. **Cyberedu-QUIZZ-ID-2.16**

Choisir un (ou des) symptôme(s) potentiel(s) d'infection par un code malveillant

(a) Mon antivirus est désactivé (50%)
(b) Mon ordinateur fonctionne plus lentement (50%)
(c) J'ai plusieurs pages Web qui s'ouvrent toutes seules (0%)
(d) Des fichiers ou des répertoires sont créés automatiquement sur mon poste (0%)

17. **Cyberedu-QUIZZ-ID-2.17**

Les mises à jour logicielles servent à améliorer les logiciels et à corriger les failles de sécurité

(a) Vrai (100%)
(b) Faux (0%)

18. **Cyberedu-QUIZZ-ID-2.18**

Vous pouvez protéger la confidentialité vos données en :

(a) Les chiffrant (100%)
(b) En calculant leur empreinte de manière à vérifier leur intégrité (0%)
(c) En les envoyant vers des supports externes ou vers le Cloud (0%)
(d) En les publiant sur Internet (0%)

19. **Cyberedu-QUIZZ-ID-2.19**

Sélectionner le (ou les) moyen(s) de durcissement d'une configuration

(a) Modifier les mots de passe par défaut (33.33333%)
(b) Désinstaller les logiciels inutiles (33.33333%)
(c) Activer le mode débogage USB sur les téléphones (0%)
(d) Sécuriser le BIOS à l'aide d'un mot de passe (33.33333%)

20. **Cyberedu-QUIZZ-ID-2.20**

Sélectionner le (ou les) principes(s) à prendre en compte lors de l'attribution de privilèges utilisateurs

(a) Tout ce qui n'est pas interdit, est autorisé (0%)
(b) Moindre privilège (50%)
(c) Besoin d'en connaitre (50%)
(d) Droit administrateur pour tous (0%)

21. **Cyberedu-QUIZZ-ID-2.21**

Entourer la (ou les) mauvaise(s) pratique(s) pour les mots de passe

(a) Je crée un mot de passe très long et très complexe, dont je ne me souviens pas (25%)
(b) Ma date de naissance me sert de mot de passe (25%)
(c) Je stocke mes mots de passe en clair dans un fichier texte (25%)
(d) Mon mot de passe doit avoir au plus 7 caractères (25%)

22. **Cyberedu-QUIZZ-ID-2.22**

Entourer la (ou les) bonne(s) pratique(s) pour les mots de passe

(a) J'enregistre mes mots de passe sur chaque navigateur Internet (0%)
(b) Je crée un mot de passe long et complexe dont je peux me souvenir * facilement (50%)
(c) J'écris mon mot de passe sur un post-it que je cache sous mon clavier/PC (0%)
(d) J'utilise un porte-clés de mots de passe (50%)

23. **Cyberedu-QUIZZ-ID-2.23**

Entourer la (ou les) bonne(s) pratique(s) de navigation sur Internet

(a) Je suis victime de ransomware, je paye la rançon (0%)
(b) J'évite de communiquer avec des inconnus (100%)
(c) J'accepte toutes les demandes sur les médias sociaux (0%)
(d) Je donne mon mot de passe de messagerie à l'administrateur lorsqu'il me le demande. (0%)

24. **Cyberedu-QUIZZ-ID-2.24**

Citer deux moyens de sécurisation physique des biens/équipements

(a) Mettre les équipements sensibles dans une salle sans contrôle d'accès (0%)
(b) Attacher les équipements sensibles avec des càbles de sécurité (50%)
(c) Nommer tous les équipements de la même façon (0%)
(d) Utiliser des filtres de confidentialité pour les écrans (50%)

25. **Cyberedu-QUIZZ-ID-2.25**

Choisir l' (ou les) exemple(s) d'incidents de sécurité

(a) Le vol d'un équipement/terminal (33.33333%)
(b) La création d'un compte utilisateur pour un nouvel étudiant (0%)
(c) La présence d'un code malveillant sur un poste (33.33333%)
(d) La divulgation sur un forum des noms, prénoms, et numéros de sécurité sociale des étudiants (33.33333%)

26. **Cyberedu-QUIZZ-ID-2.26**

Choisir la (ou les) bonne(s) réaction(s) face à un incident de sécurité :

(a) Désactiver/désinstaller son antivirus (0%)
(b) Appliquer les règles/consignes reçues par exemple dans la charte informatique (50%)
(c) Chercher à identifier la cause de l'incident (50%)
(d) Désactiver son pare-feu (personnel par exemple) (0%)

27. **Cyberedu-QUIZZ-ID-2.27**

Sélectionner la (ou les) raison(s) pour laquelle (ou lesquelles) les audits de sécurité peuvent être effectués :

(a) Pour obtenir une certification ou un agrément (33.33333%)
(b) Pour trouver des faiblesses et les corriger (33.33333%)
(c) Pour évaluer le niveau de sécurité (33.33333%)
(d) Provoquer des incidents de sécurité (0%)