Générer un « bon » mot de passe

Questionnaire d'entraînement et de vérification de la théorie

Nom, prénom :	**Date :**
Classe ou groupe :	**Points obtenus :** _____ / 71

Consignes : répondez d'après la théorie « Générer un "bon" mot de passe ». Cochez ou complétez, selon la question. Le nombre de points est indiqué entre parenthèses, pour un total de 71 points.

Source de la théorie : sectioninformatique.ch, « Générer un "bon" mot de passe » (Orif, domaine informatique).

1. Pourquoi parler des mots de passe ?

4 pts

1. D'après la théorie, d'où viennent la majorité des cyberattaques réussies ? *(1 pt)*

- ☐ A. De pannes de réseau
- ☐ B. De mots de passe faibles ou volés
- ☐ C. De câbles défectueux
- ☐ D. D'écrans mal protégés

2. En moyenne, environ combien de comptes possède un utilisateur ? *(1 pt)*

- ☐ A. 10
- ☐ B. 25
- ☐ C. 80
- ☐ D. 500

3. Citez deux raisons pour lesquelles la gestion des mots de passe est devenue difficile et risquée. *(2 pts)*

2. Le rôle d'un mot de passe

5 pts

4. Complétez la phrase. *(3 pts)*

Un mot de passe est une _____ de sécurité, un _____ personnel et un moyen d'_____.

5. Citez deux cas dans lesquels un mot de passe devient inutile. *(2 pts)*

3. Les erreurs courantes

15 pts

6. Vrai ou faux ? *(4 pts)*

Affirmation	Vrai	Faux
Une date de naissance est un bon mot de passe, car elle est facile à retenir.	☐	☐
« bonjour123 » est un mot de passe solide, car il contient des chiffres.	☐	☐
Réutiliser le même mot de passe sur plusieurs sites est une erreur courante.	☐	☐
Envoyer son mot de passe par e-mail ou par message est acceptable.	☐	☐

7. Complétez la phrase. *(3 pts)*

les _____, les fuites de _____ et les _____ humaines.

Exercice 1 – Identifier les mauvais mots de passe *(8 pts)*

Quels mots de passe sont problématiques ? Pourquoi ? Chaque mot de passe est utilisé pour un seul compte, sauf indication contraire.

Mot de passe	Problématique ?	Pourquoi ?
`azerty`	☐ Oui ☐ Non	
`Lucas2014`	☐ Oui ☐ Non	
`Tuile-Bateau-Orage-Fenouil`	☐ Oui ☐ Non	
`bonjour123`	☐ Oui ☐ Non	
`Rx4$nB81!wLq`	☐ Oui ☐ Non	
`Mamie1948!`	☐ Oui ☐ Non	
`MesVoisinsCultiventDesCourgettesGeantes`	☐ Oui ☐ Non	
`Zr8!pF29$gQ!` (utilisé pour la messagerie, la banque et les réseaux sociaux)	☐ Oui ☐ Non	

4. Ce qui fait un mot de passe fort

15 pts

8. Selon la méthode classique, un mot de passe fort compte au minimum : *(1 pt)*

- ☐ A. 6 à 8 caractères
- ☐ B. 8 à 10 caractères
- ☐ C. 12 à 16 caractères
- ☐ D. 32 caractères

9. Complétez la phrase. *(2 pts)*

La méthode classique mélange des majuscules, des minuscules, des _____ et des _____.

10. Vrai ou faux ? *(1 pt)*

Affirmation	Vrai	Faux
Un mot de passe long est plus important qu'un mot de passe complexe.	☐	☐

11. Donnez deux avantages de la méthode des phrases secrètes (méthode recommandée). *(2 pts)*

12. Associez chaque exemple à la méthode utilisée. Écrivez la lettre : A = méthode classique, B = phrase secrète, C = quatre mots aléatoires. *(3 pts)*

Exemple	Lettre
Cactus-Soleil-Horloge-Melon	
Zr8!pF29$gQ!	
HierJaiMangé3CrêpesAuCitron	

Exercice 2 – Créer une phrase secrète *(4 pts)*

Invente une phrase de 5 à 7 mots, unique et facile à retenir. N'écris pas un mot de passe que tu utilises réellement.

Ma phrase :

Nombre de caractères : _____

Pourquoi est-ce un bon choix ? (deux arguments)

Exercice 3 – Long ou complexe ? *(2 pts)*

Comparez A = « P@ss1! » et B = « Cactus-Soleil-Horloge-Melon ». Lequel est le plus solide ? Justifiez en citant le principe vu dans la théorie.

5. Les gestionnaires de mots de passe

8 pts

13. Citez deux raisons d'utiliser un gestionnaire de mots de passe. *(2 pts)*

14. Avec un gestionnaire, combien de mots de passe faut-il retenir ? *(1 pt)*

- ☐ A. Aucun
- ☐ B. Un seul : le mot de passe maître
- ☐ C. Un par site
- ☐ D. Cinq

15. Reliez chaque fonction à sa description. Écrivez la lettre : A = prévient si un mot de passe apparaît dans une fuite, B = rend les mots de passe illisibles sans le mot de passe maître, C = remplit les champs de connexion, D = retrouve ses mots de passe sur plusieurs appareils. *(4 pts)*

Fonction	Lettre
Synchronisation multi-supports	
Autofill (remplissage automatique)	
Alerte en cas de fuite de données	
Stockage chiffré	

16. Lequel de ces gestionnaires cités dans la théorie stocke les données en local ? *(1 pt)*

- ☐ A. Bitwarden
- ☐ B. ProtonPass
- ☐ C. 1Password
- ☐ D. KeePass

6. L'authentification à deux facteurs (2FA)

7 pts

17. Que signifie 2FA et à quoi sert-elle ? *(2 pts)*

18. Citez trois formes de deuxième facteur. *(3 pts)*

19. Quelle forme de 2FA la théorie recommande-t-elle ? *(1 pt)*

- ☐ A. Le code reçu par SMS
- ☐ B. L'application d'authentification
- ☐ C. La clé de sécurité physique (clé USB)
- ☐ D. Aucune : le mot de passe suffit

20. Vrai ou faux ? *(1 pt)*

Affirmation	Vrai	Faux
Même si un mot de passe est volé, le 2FA bloque la majorité des attaques.	☐	☐

7. Le phishing : reconnaître les pièges

9 pts

21. Citez trois signes d'un e-mail ou d'un message frauduleux. *(3 pts)*

Exercice 4 – Analyser un e-mail suspect *(6 pts)*

De : securite@mabanque-verification.example
Objet : URGENT – Votre compte sera supprimé dans 24 h !

Bonjour cher cliente,

Nous avons détecté une activité suspecte sur votre compte. Sans confirmation de vos informations, votre compte sera supprimé dans 24 heures.

Cliquez sur le lien ci-dessous et saisissez votre mot de passe actuel : http://mabanque-securite.example/connexion

Ouvrez aussi la pièce jointe « Facture_urgente.zip ».

Merci de votre compréhention.

Le service sécurité

a) Relevez au moins quatre signes qui montrent que ce message est frauduleux. *(4 pts)*

b) Que faites-vous concrètement avec ce message ? *(2 pts)*

8. Synthèse

8 pts

22. Léa utilise le même mot de passe, « Lea2010! », pour sa messagerie, sa banque en ligne et ses réseaux sociaux. a) Quel risque court-elle ? b) Quels conseils lui donnez-vous (deux au moins) ? *(3 pts)*

23. Complétez les cinq points à retenir. *(5 pts)*

La _____ est plus importante que la complexité.

Ne jamais utiliser le _____ mot de passe partout.

Un gestionnaire de mots de passe = un seul mot de passe _____.

Activer le _____ (authentification à deux facteurs).

Se méfier des e-mails _____.

Corrigé

Réservé au formateur – total : 71 points

1. Pourquoi parler des mots de passe ?

4 pts

N°	Réponse attendue	Points
Q1	B. De mots de passe faibles ou volés	1
Q2	C. 80	1
Q3	La multiplication des comptes (environ 80 en moyenne). La réutilisation du même mot de passe partout. 1 point par raison cohérente avec la théorie (mots de passe faibles ou volés acceptés).	2

2. Le rôle d'un mot de passe

5 pts

N°	Réponse attendue	Points
Q4	1) barrière 2) secret 3) authentification	3
Q5	Il est facile à deviner, réutilisé, divulgué ou stocké sans protection. 2 au choix, 1 point chacun.	2

3. Les erreurs courantes

15 pts

N°	Réponse attendue	Points
Q6	1) Faux : information personnelle, facile à deviner. 2) Faux : mot simple, exploité par les dictionnaires. 3) Vrai. 4) Faux : c'est une divulgation du mot de passe.	4
Q7	1) dictionnaires 2) données 3) habitudes	3
Ex. 1	**azerty :** Oui. Suite de touches du clavier et mot simple : présent dans les dictionnaires des pirates. **Lucas2014 :** Oui. Prénom (d'enfant) et année : informations personnelles faciles à deviner ; court. **Tuile-Bateau-Orage-Fenouil :** Non. Quatre mots aléatoires : long et facile à retenir. **bonjour123 :** Oui. Mot simple suivi de chiffres prévisibles : exploité par les dictionnaires. **Rx4$nB81!wLq :** Non. 12 caractères, mélange de majuscules, minuscules, chiffres et symboles, aucun mot du dictionnaire. **Mamie1948! :** Oui. Surnom et année de naissance : informations personnelles ; seulement 10 caractères. **MesVoisinsCultiventDesCourgettesGeantes :** Non. Phrase secrète longue et facile à retenir. **Zr8!pF29$gQ! :** Oui. Fort en lui-même, mais réutilisé : un seul vol ou une seule fuite expose tous les comptes.	8

4. Ce qui fait un mot de passe fort

15 pts

N°	Réponse attendue	Points
Q8	C. 12 à 16 caractères	1
Q9	1) chiffres 2) symboles	2
Q10	Vrai : c'est le point pédagogique de la théorie.	1
Q11	Plus longue donc plus sécurisée. Facile à retenir. Pas besoin de symboles compliqués. 2 au choix, 1 point chacun.	2
Q12	Cactus-Soleil-Horloge-Melon → C ; Zr8!pF29$gQ! → A ; HierJaiMangé3CrêpesAuCitron → B	3
Ex. 2	1 point : la phrase compte 5 à 7 mots. 1 point : elle est longue (12 caractères ou plus). 1 point : elle est unique et sans information personnelle. 1 point : deux arguments cohérents (longue, facile à retenir, sans symboles compliqués).	4
Ex. 3	B est le plus solide. Principe : la longueur compte plus que la complexité (6 caractères pour A, 27 pour B). 1 point pour le choix, 1 point pour la justification.	2

5. Les gestionnaires de mots de passe

8 pts

N°	Réponse attendue	Points
Q13	Il génère automatiquement des mots de passe forts. Il stocke tous les mots de passe en sécurité. Un seul mot de passe maître à retenir. 2 au choix, 1 point chacun.	2
Q14	B. Un seul : le mot de passe maître	1
Q15	Synchronisation multi-supports → D ; Autofill (remplissage automatique) → C ; Alerte en cas de fuite de données → A ; Stockage chiffré → B	4
Q16	D. KeePass	1

6. L'authentification à deux facteurs (2FA)

7 pts

N°	Réponse attendue	Points
Q17	Authentification à deux facteurs (1 point). C'est une deuxième vérification, en plus du mot de passe (1 point).	2
Q18	Code reçu par SMS. Application d'authentification. Clé de sécurité physique (clé USB). 1 point par forme.	3

N°	Réponse attendue	Points
Q19	B. L'application d'authentification	1
Q20	Vrai.	1

7. Le phishing : reconnaître les pièges

9 pts

N°	Réponse attendue	Points
Q21	Urgence, faux liens très ressemblants, fautes d'orthographe, demande de mot de passe ou d'informations personnelles, pièces jointes douteuses. 3 au choix, 1 point chacun.	3
Ex. 4	a) Signes à relever (1 point chacun, 4 minimum) : urgence (« supprimé dans 24 h ») ; adresse et lien qui imitent la banque (faux lien) ; fautes (« cher cliente », « compréhention ») ; demande du mot de passe actuel ; pièce jointe douteuse (fichier .zip). b) Ne pas cliquer sur le lien, ne pas ouvrir la pièce jointe, ne rien saisir (1 point). Aller manuellement sur le site officiel de la banque pour vérifier (1 point).	6

8. Synthèse

8 pts

N°	Réponse attendue	Points
Q22	a) Le mot de passe est réutilisé : une seule fuite ou un seul vol expose tous ses comptes (1 point). Il est aussi basé sur un prénom et une année. b) Un mot de passe unique par compte, long (phrase secrète ou quatre mots), un gestionnaire de mots de passe, activer le 2FA (2 au choix, 1 point chacun).	3
Q23	1) longueur 2) même 3) maître 4) 2FA 5) suspects	5