Nom : _____ Date : _____ Note : _____

Prévention de l'usurpation d'identité et sécurité des Guide de sécurité

Fuites d'identifiants, MFA, surveillance du dark web, alertes de gel du crédit, ingénierie sociale

PRÉSENTATION PÉDAGOGIQUE : PRÉVENTION DE L'USURPATION D'IDENTITÉ

SÉCURISÉ
CHIFFREMENT DES DONNÉES
Norme AES 256 bits

CONFORME
NORMES MONDIALES
Cadres RGPD (GDPR) et CCPA

ZERO TRUST
POLITIQUE D'ACCÈS
Authentification multifacteur

Bienvenue ! Ce dossier d'activités vous guide à travers la prévention et l'atténuation du vol d'identité. Vous étudierez les fuites d'identifiants, l'authentification multifacteur, la surveillance du dark web, les alertes de gel du crédit et la défense contre l'ingénierie sociale.

POINTS DE CONTRÔLE DE LA FICHE

- [ ] **Parties 1-4 : maîtrisez la cybersécurité et la prévention des menaces.**
- [ ] **Parties 5-7 : résolvez les mots croisés et les mots mêlés.**
- [ ] **Parties 8-9 : résolvez les études de cas et le défi de déchiffrement.**
- [ ] **Partie 10 : consultez les FAQ de base et avancées.**
- [ ] **Partie 11 : découvrez 10 faits concrets intéressants.**
- [ ] **Bonus : défi Réflexion rapide.**

Ouvrir le guide VPN.com de la cybersécurité

URL: https://www.vpn.com/fr/cybersecurite/vol-identite/

Votre parcours d'apprentissage : protection de l'identité

- Comprendre les risques d'exposition des identifiants sur les forums du dark web.
- Mettre en place l'authentification multifacteur (MFA) et des alertes de gel du crédit.
- Concevoir les défenses de sécurité de l'entreprise contre les arnaques ciblées d'ingénierie sociale.

CONSIGNES DU GUIDE SUR L'USURPATION D'IDENTITÉ

Répondez aux questions à choix multiple et vrai/faux, complétez les phrases à trous à l'aide de la banque de mots, associez les définitions et résolvez les mots croisés et les mots mêlés. Appliquez vos connaissances à la protection de l'identité. Terminez par l'activité bonus Réflexion rapide.

PRÉVENTION DE L'USURPATION D'IDENTITÉ ET SÉCURITÉ DES ACTIFS (INTRODUCTION)

L'usurpation d'identité exploite des identifiants divulgués et des connexions faibles pour détourner des comptes personnels et professionnels. La MFA, le gel du crédit, les outils de surveillance du dark web et les cadres SPF/DKIM/DMARC constituent une défense essentielle contre l'usurpation numérique.

LISEZ ATTENTIVEMENT CHAQUE POINT DE CONTRÔLE ET CHOISISSEZ OU ÉCRIVEZ LA BONNE RÉPONSE.

Point de contrôle 1 : Défi QCM

1. Quelle est la principale méthode utilisée par les usurpateurs d'identité pour voler des identifiants de connexion ?

- A. Envoyer de fausses alertes par e-mail pour amener les utilisateurs à saisir leur mot de passe sur des portails usurpés
- B. Écouter des émissions de radio près des bureaux de l'entreprise d'un utilisateur
- C. Défragmenter le disque de stockage du serveur local d'un utilisateur
- D. Déconnecter les configurations de sauvegarde réseau externes

2. Quel contrôle de sécurité offre la meilleure défense contre les fuites d'identifiants ?

- A. Authentification multifacteur à l'aide de clés matérielles
- B. Créer des mots de passe longs selon les formats par défaut du navigateur
- C. Changer de nom d'utilisateur de messagerie tous les six mois
- D. Supprimer les historiques de navigation et les cookies de suivi stockés

3. Qu'est-ce qui correspond au gel du crédit ?

- A. Verrouiller les rapports de crédit pour empêcher les voleurs d'ouvrir des prêts non autorisés
- B. Supprimer l'historique des transactions bancaires des bases de données
- C. Désactiver les lecteurs de bande magnétique des cartes bancaires sur les terminaux
- D. Chiffrer au repos les disques durs de la base de données locale

4. Pourquoi la surveillance du dark web est-elle utile ?

- A. Il alerte les utilisateurs si leurs identifiants ayant fuité apparaissent dans des bases de données illicites
- B. Il empêche les logiciels malveillants actifs de s'exécuter dans des bacs à sable virtuels
- C. Il accélère le routage du navigateur sur les réseaux virtuels
- D. Il bloque les tentatives d'injection SQL visant la base de données côté serveur

5. Que signifie l'ingénierie sociale ?

- A. Manipuler des personnes pour qu'elles révèlent volontairement des identifiants confidentiels
- B. Analyser les ports des serveurs de l'entreprise à la recherche de failles de sécurité exploitables
- C. Sauvegarder les fichiers de base de données du système sur des disques durs hors ligne
- D. Faire transiter les paquets réseau par trois nœuds onion chiffrés

Point de contrôle 2 : Défi Vrai ou Faux

6 Question 6

6. L'usurpation d'identité ne concerne que les comptes numériques en ligne, pas le courrier postal physique.

- ○ Vrai
- ○ Faux

7 Question 7

7. Imposer la MFA sur tous les comptes personnels bloque la plupart des attaques de bots par bourrage d'identifiants (credential stuffing).

- ○ Vrai
- ○ Faux

8 Question 8

8. Un gel du crédit bloque les vérifications de solvabilité mais vous empêche d'accéder à votre propre compte bancaire.

- ○ Vrai
- ○ Faux

9 Question 9

9. Les gestionnaires de mots de passe protègent contre l'hameçonnage en refusant de remplir automatiquement les mots de passe sur des domaines usurpés.

- ○ Vrai
- ○ Faux

10 Question 10

10. Les e-mails d'hameçonnage utilisent souvent un ton d'urgence pour provoquer des réactions émotionnelles et rapides.

- ○ Vrai
- ○ Faux

Point de contrôle 3 : Insertion des termes clés

Lisez chaque phrase ci-dessous et complétez le blanc avec le terme correct de la banque de mots.

1. Les usurpateurs d'identité ciblent les mots de passe personnels et les _____ des utilisateurs.

2. Alerter les utilisateurs des violations de bases de données permet de repérer les _____ touchant les comptes privés.

3. Exiger un code temporaire pour se connecter s'appelle l'authentification _____ .

4. Analyser les forums de pirates à la recherche de données volées relève de la _____ du dark web.

5. Bloquer les vérifications de crédit non autorisées nécessite un _____ .

6. Former les employés à la détection de l'hameçonnage permet de bâtir une _____ de sécurité active.

BANQUE DE MOTS DE VOCABULAIRE

DÉFENSE FUITES GEL DU CRÉDIT HAMEÇONNAGE IDENTIFIANTS MULTIFACTEUR SPOOFING SURVEILLANCE

Écrivez vos réponses ici :

1. **2.**

3. **4.**

5. **6.**

Point de contrôle 4 : Association de notions sur la sécurité

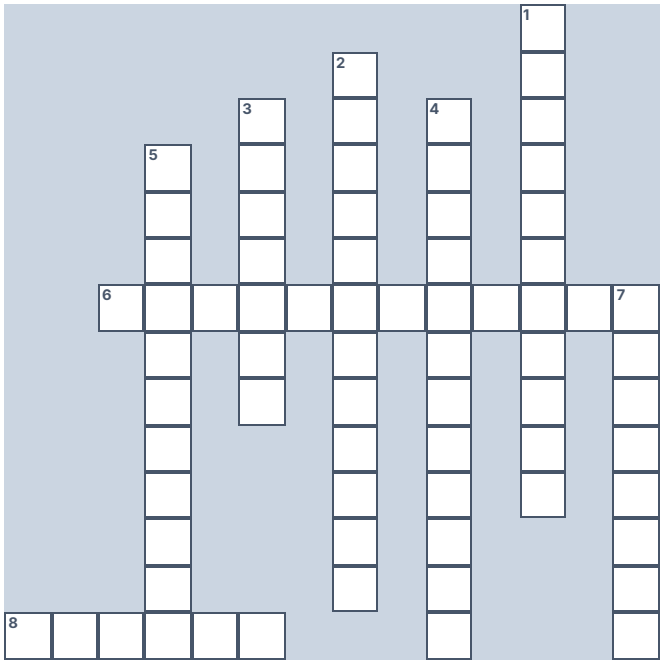
ASSOCIATION DE DÉFINITIONS

Associez chaque terme de vocabulaire à gauche à sa définition à droite en écrivant la lettre correspondante (A-H) dans la case à remplir.

☐	1. IDENTIFIANTS	A	Étape de vérification secondaire (comme des clés matérielles) protégeant les connexions aux comptes.
☐	2. FUITES	B	Créer un faux site web ou un faux e-mail pour imiter une organisation légitime.
☐	3. MFA	C	Restriction de l'accès aux dossiers de crédit pour empêcher les demandes de prêt frauduleuses.
☐	4. SURVEILLANCE	D	Exposition non autorisée de bases de données privées contenant des dossiers personnels d'utilisateurs.
☐	5. GEL	E	Formation et contrôles techniques utilisés pour se protéger contre l'usurpation d'identité.
☐	6. DÉFENSE	F	Envoyer des messages frauduleux pour amener les utilisateurs à divulguer leurs identifiants.
☐	7. USURPATION	G	Surveillance des forums en ligne et des canaux de pirates à la recherche de données d'entreprise volées.
☐	8. HAMEÇONNAGE	H	Noms d'utilisateur, mots de passe et jetons privés servant à authentifier les identités numériques.

Point de contrôle 5 : Mots croisés

Résolvez la grille de mots croisés en tapant des lettres dans les cases blanches actives. Les numéros correspondent aux définitions ci-dessous.



HORIZONTALEMENT

6. Noms d'utilisateur, mots de passe et jetons privés servant à authentifier les identités numériques. (12)

8. Exposition non autorisée de bases de données privées contenant des dossiers personnels d'utilisateurs. (6)

VERTICALEMENT

1. Envoi de messages frauduleux pour amener les utilisateurs à divulguer leurs identifiants. (11)

2. Analyse des forums en ligne et des canaux de pirates à la recherche de données d'entreprise volées. (12)

3. Formation et contrôles techniques utilisés pour se protéger contre l'usurpation d'identité. (7)

4. Étape de vérification secondaire (comme les clés matérielles) qui protège les connexions aux comptes (MFA). (12)

5. Restriction de l'accès aux dossiers de crédit pour empêcher les demandes de prêt frauduleuses. (11)

7. Création d'un faux site web ou d'un faux e-mail imitant une organisation légitime. (8)

Point de contrôle 5, variante : Définitions de mots croisés accessibles

Les utilisateurs de lecteurs d'écran et de clavier peuvent saisir les réponses des mots croisés directement dans les champs de texte ci-dessous.

HORIZONTALEMENT

6 horizontal: Noms d'utilisateur, mots de passe et jetons privés servant à authentifier les identités numériques. (12 lettres):

8 horizontal: Exposition non autorisée de bases de données privées contenant des dossiers personnels d'utilisateurs. (6 lettres):

VERTICALEMENT

1 vertical: Envoi de messages frauduleux pour amener les utilisateurs à divulguer leurs identifiants. (11 lettres):

2 vertical: Analyse des forums en ligne et des canaux de pirates à la recherche de données d'entreprise volées. (12 lettres):

3 vertical: Formation et contrôles techniques utilisés pour se protéger contre l'usurpation d'identité. (7 lettres):

4 vertical: Étape de vérification secondaire (comme les clés matérielles) qui protège les connexions aux comptes (MFA). (12 lettres):

5 vertical: Restriction de l'accès aux dossiers de crédit pour empêcher les demandes de prêt frauduleuses. (11 lettres):

7 vertical: Création d'un faux site web ou d'un faux e-mail imitant une organisation légitime. (8 lettres):

Point de contrôle 6 : Mots cachés

Trouvez les 8 termes de vocabulaire clés cachés dans la grille ci-dessous. Les mots peuvent être horizontaux, verticaux ou en diagonale.

R T U K X E J R Z X I K M X E

U M R M X U P V C T S S P V F

E F Z I I J U Q A D U Z N N D

T U B R W F R J M V R K X M Q

C I W J K L O F G N V U V F D

A T E S N E F E D X E L V O O

F E R P W G L G M M I V W N E

I S H J Q K H P J L L I W T L

T N C N C X E T W N L T N K D

L D J S O B W P X P A H C H N

U I D E N T I F I A N T S T K

M W O W O R Q R K L C N E Y C

A T I D E R C U D L E G J H A

F D H J B M T G N I F O O P S

Z H A M E C O N N A G E R R N

LISTE DE MOTS DE VOCABULAIRE

IDENTIFIANTS FUITES MULTIFACTEUR SURVEILLANCE GELDUCREDIT

DEFENSE SPOOFING HAMECONNAGE

Point de contrôle 6, variante : Association de vocabulaire accessible

Associez chacun des 8 termes de vocabulaire de la grille de mots cachés à sa définition en écrivant la lettre (A-H) dans l'espace prévu.

TERMES DE VOCABULAIRE
A. IDENTIFIANTS
B. FUITES
C. MULTIFACTEUR
D. SURVEILLANCE
E. GELDUCREDIT
F. DEFENSE
G. SPOOFING
H. HAMECONNAGE

DÉFINITIONS ET CHAMPS D'ASSOCIATION

_____ 1. Envoi de messages frauduleux pour amener les utilisateurs à divulguer leurs identifiants.

_____ 2. Noms d'utilisateur, mots de passe et jetons privés servant à authentifier les identités numériques.

_____ 3. Création d'un faux site web ou d'un faux e-mail imitant une organisation légitime.

_____ 4. Formation et contrôles techniques utilisés pour se protéger contre l'usurpation d'identité.

_____ 5. Analyse des forums en ligne et des canaux de pirates à la recherche de données d'entreprise volées.

_____ 6. Restriction de l'accès aux dossiers de crédit pour empêcher les demandes de prêt frauduleuses.

_____ 7. Exposition non autorisée de bases de données privées contenant des dossiers personnels d'utilisateurs.

_____ 8. Étape de vérification secondaire (comme les clés matérielles) qui protège les connexions aux comptes (MFA).

Point de contrôle 7 : Défi des mots mélangés

Remettez les lettres ci-dessous dans l'ordre pour découvrir des notions et termes clés de la cybersécurité. Écrivez vos réponses dans les champs prévus.

1. AIITDFNITESN
2. RUIFMEULCTAT
3. GRCELEITUDD
4. ONGIFSPO
5. TISFEU
6. EEANICLSULRV
7. DSNEEEF
8. ANEOMHCAGNE

Activité bonus : Réflexion rapide

3 RÉPONSES PAR CATÉGORIE. LE PREMIER À REMPLIR SA LISTE GAGNE.

1	Choses à faire si votre identité est usurpée			
2	Choses à ne pas partager sur les réseaux sociaux			
3	Choses que vous sauvegardez			
4	Cartes ou pièces d'identité dans votre portefeuille			
5	Documents que vous devriez protéger			
6	Choses à faire après une fuite de données			
7	Raisons de mettre à jour les logiciels			
8	Informations que veut un usurpateur d'identité			
9	Appareils qui peuvent être piratés			
10	Endroits d'où vos données peuvent fuiter			
11	Bonnes habitudes de sécurité à adopter dès aujourd'hui			
12	Signes qu'un ordinateur est infecté			
13	Façons de prouver qui vous êtes			
14	Signes d'usurpation d'identité			
15	Signaux d'alerte dans un e-mail			

Point de contrôle 8 : Études de cas sur la cybersécurité

Appliquez les notions apprises pour résoudre les scénarios réels ci-dessous.

ÉTUDE DE CAS 1 : PROTECTION CONTRE L'USURPATION D'IDENTITÉ DES DIRIGEANTS



Scénario : Un cadre dirigeant très en vue a été ciblé par des noms de domaine de typosquattage imitant son adresse e-mail personnelle afin d'escroquer des clients. Concevez un plan de protection de la marque.

Question de discussion : Analysez les risques d'usurpation de la marque et détaillez SPF/DKIM/DMARC ainsi que les contrôles d'authentification.

ÉTUDE DE CAS 2 : IDENTIFIANTS D'ENTREPRISE EXPOSÉS SUR LE DARK WEB



Scénario : Un dump de base de données sur le dark web contient plusieurs centaines d'identifiants d'entreprise appartenant aux administrateurs système d'une grande entreprise. Concevez une stratégie d'atténuation.

Question de discussion : Décrivez le processus de nettoyage des identifiants et planifiez le déploiement d'un gestionnaire de mots de passe.

Point de contrôle 9 : Déchiffrer le code

Un professionnel de la cybersécurité protège les ressources réseau contre les acteurs malveillants en ligne. Utilisez la clé de correspondance lettres-chiffres ci-dessous pour déchiffrer le message en écrivant les lettres correspondantes dans les cases vides.

CLÉ DE CHIFFREMENT LETTRE-CHIFFRE

A=1 B=2 C=3 D=4 E=5 F=6 G=7 H=8 I=9 J=10

K=11 L=12 M=13 N=14 O=15 P=16 Q=17 R=18 S=19 T=20

U=21 V=22 W=23 X=24 Y=25 Z=26

16	18	15	20	5	7	5	26		22	15	20	18	5	
9	4	5	14	20	9	20	5		14	21	13	5	18	9	17	21	5
			1	22	5	3		12	1		13	6	1				

Message déchiffré :

ASTUCE : CHAQUE NOMBRE REPRÉSENTE LA POSITION DE LA LETTRE DANS L'ALPHABET (P. EX. 1 = A, 2 = B, 26 = Z).

Point de contrôle 10 : Questions fréquentes de base sur la cybersécurité (Partie A)

Passez en revue les questions et réponses courantes sur la réduction des menaces en ligne.

Q1: Qu'est-ce que l'usurpation d'identité ?

Un délit dans lequel un attaquant vole des données personnelles (comme des mots de passe ou des numéros de sécurité sociale) pour se faire passer pour quelqu'un d'autre à des fins financières.

Q2: Quelle est la cause la plus fréquente d'usurpation d'identité ?

L'hameçonnage est l'un des principaux moyens par lesquels les voleurs obtiennent des mots de passe, en attirant les utilisateurs vers de faux sites usurpés.

Q3: Comment l'authentification multifacteur (MFA) protège-t-elle les identités ?

La MFA exige une seconde preuve (comme une clé matérielle) pour se connecter, ce qui bloque les attaquants même s'ils volent votre mot de passe.

Q4: Qu'est-ce qu'un gel du crédit ?

Un service gratuit qui empêche les agences d'évaluation du crédit de partager votre dossier de crédit, ce qui empêche les voleurs d'ouvrir de nouveaux prêts à votre nom. [2]

Q5: Qu'est-ce que la surveillance du dark web ?

Logiciel qui surveille les forums de pirates à la recherche d'adresses e-mail, de mots de passe et de données personnelles divulgués, et qui vous alerte si vos données sont exposées.

Point de contrôle 10 : Questions fréquentes de base sur la cybersécurité (Partie B)

Passez en revue les questions et réponses courantes sur la réduction des menaces en ligne.

Q6: Que signifie le credential stuffing ?

Robots automatisés qui testent des listes de mots de passe ayant fuité sur des centaines de sites web pour prendre le contrôle de comptes actifs.

Q7: Pourquoi l'usurpation d'adresse e-mail est-elle dangereuse ?

Elle permet aux attaquants de falsifier le nom de l'expéditeur dans les e-mails, de sorte que les messages d'hameçonnage semblent provenir de collègues de confiance.

Q8: Comment les gestionnaires de mots de passe empêchent-ils l'usurpation d'identité ?

Ils stockent des mots de passe complexes et uniques pour chaque compte et refusent de remplir automatiquement les identifiants sur de faux domaines d'hameçonnage.

Q9: Qu'est-ce que le harponnage (spear phishing) ?

Une attaque d'hameçonnage très ciblée, personnalisée avec le nom et les informations de la victime pour augmenter les chances de la tromper.

Q10: En quoi une alerte de crédit diffère-t-elle d'un gel de crédit ?

Une alerte demande aux prêteurs de vérifier votre identité avant d'ouvrir des comptes, alors qu'un gel bloque totalement l'accès à votre dossier de crédit. [2]

Point de contrôle 10 : Questions fréquentes avancées sur la sécurité (Partie C)

Découvrez les aspects techniques avancés des cadres de sécurité, de l'analyse des logiciels malveillants et de la conformité des données.

Q1: Comment l'échange de carte SIM (SIM swapping) mène-t-il à l'usurpation d'identité ?

Les attaquants convainquent le personnel de l'opérateur de transférer le numéro de téléphone de la victime sur une nouvelle carte SIM, détournant ainsi les codes 2FA envoyés par SMS.

Q2: Quel est le rôle de DMARC dans la prévention de l'usurpation d'identité ?

DMARC permet aux propriétaires de domaines d'empêcher les e-mails usurpés d'atteindre les boîtes de réception, ce qui bloque les faux e-mails imitant les domaines d'entreprise.

Q3: Pourquoi l'usurpation d'identité synthétique est-elle difficile à détecter ?

Les voleurs associent de vrais numéros de sécurité sociale (SSN) à de faux noms et de fausses dates de naissance pour créer de tout nouveaux profils de crédit, en contournant les alertes de fraude de base.

Q4: Comment les courtiers en données exploitent-ils les identités personnelles ?

Les courtiers en données collectent des registres publics, des comportements en ligne et des historiques d'achat pour constituer des dossiers de profils, qui peuvent fuiter ou être vendus.

Q5: Pourquoi la MFA par SMS est-elle considérée comme vulnérable ?

Le trafic SMS est vulnérable à l'interception, à l'hameçonnage et aux attaques de SIM swapping au niveau de l'opérateur.

Point de contrôle 10 : Questions fréquentes avancées sur la sécurité (Partie D)

Découvrez les aspects techniques avancés des cadres de sécurité, de l'analyse des logiciels malveillants et de la conformité des données.

Q6: Qu'est-ce qu'un verrouillage du dossier de crédit ?

Un service commercial semblable au gel du crédit, qui permet de verrouiller ou déverrouiller instantanément son dossier de crédit via une application mobile.

Q7: Comment les violations de données en entreprise alimentent-elles l'usurpation d'identité ?

Les bases de données divulguées exposent des millions d'identifiants en clair, ce qui fournit aux voleurs les données brutes nécessaires pour commettre une usurpation d'identité ciblée.

Q8: Quel est le risque de trop en partager sur les réseaux sociaux ?

Partager publiquement le nom de ses animaux, son lieu de naissance ou le nom de jeune fille de sa mère donne aux voleurs les réponses aux questions courantes de récupération de compte.

Q9: Comment les connexions biométriques protègent-elles les profils d'identité ?

La biométrie associe les connexions à des caractéristiques comme les empreintes digitales ou le visage ; conservées sur l'appareil, elles sont difficiles à voler, mais les données biométriques stockées peuvent fuiter.

Q10: Comment la Red Flags Rule lutte-t-elle contre l'usurpation d'identité ?

Une réglementation fédérale qui impose aux institutions financières d'élaborer des programmes écrits pour détecter les signaux d'alerte d'usurpation d'identité et y réagir.

Partie 11 : 10 faits et enseignements concrets sur la cybersécurité

Découvrez des faits concrets sur les failles de sécurité, les mécanismes de défense et les normes de conformité.

1. APERÇU SÉCURITÉ

IdentityTheft.gov, géré par la FTC, permet aux victimes aux États-Unis de signaler une usurpation d'identité et d'obtenir un plan de rétablissement personnalisé. [1]

2. APERÇU SÉCURITÉ

Les clés de sécurité matérielles sont une MFA résistante à l'hameçonnage, le type de MFA le plus robuste, que la CISA recommande vivement. [4]

3. APERÇU SÉCURITÉ

Les mots de passe compromis sont un point d'entrée courant des violations de données, qui alimentent ensuite l'usurpation d'identité.

4. APERÇU SÉCURITÉ

Le gel du crédit est gratuit en vertu de la loi fédérale ; il empêche les prêteurs de consulter les dossiers de crédit jusqu'à son déblocage. [2]

5. APERÇU SÉCURITÉ

DMARC permet aux propriétaires de domaines d'indiquer aux serveurs de messagerie de rejeter ou de mettre en quarantaine les e-mails usurpés qui échouent aux vérifications. [7]

6. APERÇU SÉCURITÉ

Le SIM swapping permet aux pirates de contourner l'authentification à deux facteurs par SMS sur les portails bancaires.

7. ZOOM SUR LA SÉCURITÉ

La fraude à l'identité synthétique mélange des informations réelles et fictives, ce qui la rend difficile à détecter pour les prêteurs.

8. ZOOM SUR LA SÉCURITÉ

Beaucoup de personnes réutilisent le même mot de passe pour plusieurs comptes en ligne, si bien qu'une seule fuite peut en exposer plusieurs.

9. ZOOM SUR LA SÉCURITÉ

Les courtiers en données compilent des dossiers détaillés sur un grand nombre de consommateurs, ce qui crée un risque concentré pour la vie privée.

10. APERÇU SÉCURITÉ

Se remettre d'une usurpation d'identité peut demander des mois de travail, comme contester des prélèvements et corriger des rapports de crédit.

Références techniques et sources

Le guide d'étude et les énigmes interactives sont tirés des normes internationales du NIST, de l'OWASP et de conformité en matière de protection des données.

RÉFÉRENCES ACADÉMIQUES ET PROFESSIONNELLES

[1] Federal Trade Commission. (n.d.). IdentityTheft.gov: Report identity theft and get a recovery plan.

https://www.identitytheft.gov/

[2] Federal Trade Commission. (2025). Credit Freezes and Fraud Alerts.

https://consumer.ftc.gov/articles/credit-freezes-and-fraud-alerts

[3] Federal Trade Commission. (n.d.). What To Know About Identity Theft.

https://consumer.ftc.gov/articles/what-know-about-identity-theft

[4] CISA. (n.d.). More than a Password.

https://www.cisa.gov/MFA

[5] CISA. (2023). Phishing Guidance: Stopping the Attack Cycle at Phase One.

https://www.cisa.gov/resources-tools/resources/phishing-guidance-stopping-attack-cycle-phase-one

[6] NIST. (2025). SP 800-63B-4: Digital Identity Guidelines: Authentication and Authenticator Management.

https://pages.nist.gov/800-63-4/sp800-63b.html

[7] IETF. (2015). RFC 7489: Domain-based Message Authentication, Reporting, and Conformance (DMARC).

https://www.rfc-editor.org/rfc/rfc7489.html

Corrigé : Point de contrôle 1 – Choix multiple

1 Question 1

Bonne réponse : A

NOTE PÉDAGOGIQUE

Quelle est la principale méthode utilisée par les usurpateurs d'identité pour voler des identifiants de connexion ? → Envoyer de fausses alertes par e-mail pour amener les utilisateurs à saisir leur mot de passe sur des portails usurpés

2 Question 2

Bonne réponse : A

NOTE PÉDAGOGIQUE

Quel contrôle de sécurité offre la meilleure défense contre les fuites d'identifiants ? → Authentification multifacteur à l'aide de clés matérielles

3 Question 3

Bonne réponse : A

NOTE PÉDAGOGIQUE

Qu'est-ce qui correspond au gel du crédit ? → Verrouiller les rapports de crédit pour empêcher les voleurs d'ouvrir des prêts non autorisés

4 Question 4

Bonne réponse : A

NOTE PÉDAGOGIQUE

Pourquoi la surveillance du dark web est-elle utile ? → Il alerte les utilisateurs si leurs identifiants ayant fuité apparaissent dans des bases de données illicites

5 Question 5

Bonne réponse : A

NOTE PÉDAGOGIQUE

Que signifie l'ingénierie sociale ? → Manipuler des personnes pour qu'elles révèlent volontairement des identifiants confidentiels

Corrigé : Point de contrôle 2 – Vrai ou faux

6 Question 6

Bonne réponse : Faux

NOTE PÉDAGOGIQUE

L'usurpation d'identité peut aussi commencer hors ligne, par exemple avec du courrier ou des documents volés.

7 Question 7

Bonne réponse : Vrai

NOTE PÉDAGOGIQUE

Imposer la MFA sur tous les comptes personnels bloque la plupart des attaques de bots par bourrage d'identifiants (credential stuffing).

8 Question 8

Bonne réponse : Faux

NOTE PÉDAGOGIQUE

Un gel du crédit empêche les nouvelles vérifications de crédit mais n'affecte pas vos comptes existants.

9 Question 9

Bonne réponse : Vrai

NOTE PÉDAGOGIQUE

Les gestionnaires de mots de passe protègent contre l'hameçonnage en refusant de remplir automatiquement les mots de passe sur des domaines usurpés.

10 Question 10

Bonne réponse : Vrai

NOTE PÉDAGOGIQUE

Les e-mails d'hameçonnage utilisent souvent un ton d'urgence pour provoquer des réactions émotionnelles et rapides.

Corrigés du vocabulaire et grille d'évaluation

Grille de notation de l'enseignant : attribuez 1 point par association correcte (8 points au total) et par terme en contexte (6 points au total).

POINT DE CONTRÔLE 4 : CORRIGÉ DE L'ASSOCIATION DE NOTIONS

H 1. IDENTIFIANTS	D 2. FUITES	A 3. MFA	G 4. SURVEILLANCE
C 5. GEL	E 6. DÉFENSE	B 7. USURPATION	F 8. HAMEÇONNAGE

POINT DE CONTRÔLE 3 : CORRIGÉ DES TERMES CLÉS

1 IDENTIFIANTS	2 FUITES	3 MULTIFACTEUR	4 SURVEILLANCE
5 GEL DU CRÉDIT	6 DÉFENSE		

POINT DE CONTRÔLE 6, VARIANTE : CORRIGÉ DE L'ASSOCIATION DE MOTS

1 H – HAMECONNAGE	2 A – IDENTIFIANTS	3 G – SPOOFING	4 F – DEFENSE
5 D – SURVEILLANCE	6 E – GELDUCREDIT	7 B – FUITES	8 C – MULTIFACTEUR

NOTES DE DISCUSSION POUR LES ENSEIGNANTS

Termes clés :
Vérifiez que les élèves savent expliquer IDENTIFIANTS, FUITES et MFA avec leurs propres mots et donner un exemple pour chacun.

Études de cas :
Demandez aux élèves de justifier leurs recommandations par des faits tirés de la fiche plutôt que par des suppositions.

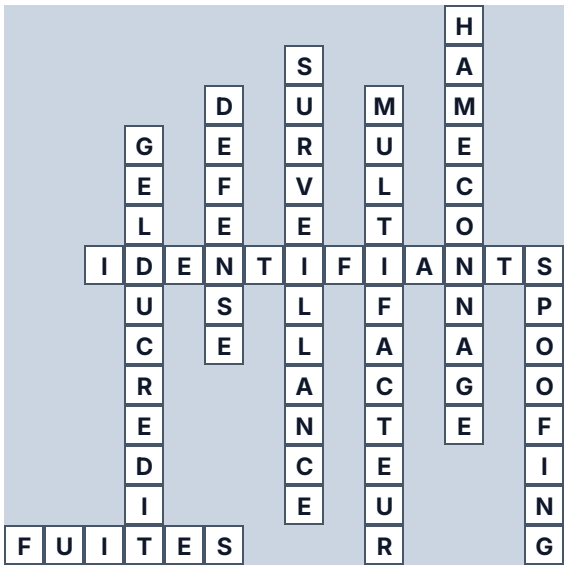
Évaluation des sources :
Faites vérifier au moins une affirmation à l'aide des sources de la fiche et discutez des raisons pour lesquelles les chiffres, les prix et les règles peuvent évoluer avec le temps.

Corrigés des jeux et notes pour l'enseignant

SOLUTION DES MOTS CACHÉS

R	T	U	K	X	E	J	R	Z	X	I	K	M	X	E
U	M	R	M	X	U	P	V	C	T	S	S	P	V	F
E	F	Z	I	I	J	U	Q	A	D	U	Z	N	N	D
T	U	B	R	W	F	R	J	M	V	R	K	X	M	Q
C	I	W	J	K	L	O	F	G	N	V	U	V	F	D
A	T	E	S	N	E	F	E	D	X	E	L	V	O	O
F	E	R	P	W	G	L	G	M	M	I	V	W	N	E
I	S	H	J	Q	K	H	P	J	L	L	I	W	T	L
T	N	C	N	C	X	E	T	W	N	L	T	N	K	D
L	D	J	S	O	B	W	P	X	P	A	H	C	H	N
U	I	D	E	N	T	I	F	I	A	N	T	S	T	K
M	W	O	W	O	R	Q	R	K	L	C	N	E	Y	C
A	T	I	D	E	R	C	U	D	L	E	G	J	H	A
F	D	H	J	B	M	T	G	N	I	F	O	O	P	S
Z	H	A	M	E	C	O	N	N	A	G	E	R	R	N

SOLUTION DES MOTS CROISÉS



GUIDE DE L'ENSEIGNANT : SOLUTIONS DES MOTS CROISÉS

HORIZONTALEMENT

6 horizontal: IDENTIFIANTS Noms d'utilisateur, mots de passe et jetons privés servant à authentifier les identités numériques. (12 lettres)

8 horizontal: FUITES Exposition non autorisée de bases de données privées contenant des dossiers personnels d'utilisateurs. (6 lettres)

VERTICALEMENT

1 vertical: HAMECONNAGE Envoi de messages frauduleux pour amener les utilisateurs à divulguer leurs identifiants. (11 lettres)

2 vertical: SURVEILLANCE Analyse des forums en ligne et des canaux de pirates à la recherche de données d'entreprise volées. (12 lettres)

3 vertical: DEFENSE Formation et contrôles techniques utilisés pour se protéger contre l'usurpation d'identité. (7 lettres)

4 vertical: MULTIFACTEUR Étape de vérification secondaire (comme les clés matérielles) qui protège les connexions aux comptes (MFA). (12 lettres)

5 vertical: GELDUCREDIT Restriction de l'accès aux dossiers de crédit pour empêcher les demandes de prêt frauduleuses. (11 lettres)

7 vertical: SPOOFING Création d'un faux site web ou d'un faux e-mail imitant une organisation légitime. (8 lettres)

Corrigé des mots mélangés et du code

Corrigé de l'activité de remise en ordre des lettres du vocabulaire et du défi du code secret.

CORRIGÉ DES MOTS MÉLANGÉS

1. AIITDFNITESN — **IDENTIFIANTS**
2. RUIFMEULCTAT — **MULTIFACTEUR**
3. GRCELEITUDD — **GELDUCREDIT**
4. ONGIFSPO — **SPOOFING**
5. TISFEU — **FUITES**
6. EEANICLSULRV — **SURVEILLANCE**
7. DSNEEEF — **DEFENSE**
8. ANEOMHCAGNE — **HAMECONNAGE**

CORRIGÉ DU DÉFI DU CODE SECRET

"PROTEGEZ VOTRE IDENTITE NUMERIQUE AVEC LA MFA"

Corrigé des études de cas

A Étude de cas 1 : Protection contre l'usurpation d'identité des dirigeants

Corrigé de l'enseignant

CONSIGNE DE NOTATION

Les réponses des élèves doivent couvrir les points suivants :

- Analyse de scénario : un membre très en vue de la direction a été ciblé par des noms de domaine en typosquatting imitant son adresse e-mail personnelle pour escroquer des clients. Concevez un plan de protection de la marque.
- Stratégie et solution recommandées : enregistrez toutes les variantes orthographiques courantes du nom du dirigeant. Déployez des protocoles d'authentification des e-mails (DMARC, DKIM, SPF) pour empêcher l'usurpation de domaine. Imposez une MFA matérielle sur toutes les connexions professionnelles des membres de la direction.

B Étude de cas 2 : Identifiants d'entreprise exposés sur le dark web

Corrigé de l'enseignant

CONSIGNE DE NOTATION

Les réponses des élèves doivent couvrir les points suivants :

- Analyse de scénario : un vidage de base de données sur le dark web contient plusieurs centaines d'identifiants d'entreprise appartenant aux administrateurs système d'une grande entreprise. Concevez une stratégie d'atténuation.
- Stratégie et solution recommandées : réinitialiser les mots de passe dans toute l'entreprise. Imposer l'utilisation d'un gestionnaire de mots de passe d'entreprise. Exiger la MFA sur tous les portails du système et mettre en place des alertes automatisées de surveillance continue du dark web.