Nom : _____ Date : _____ Note : _____

Attaques par hameçonnage et ingénierie sociale

Hameçonnage ciblé (spear phishing), arnaques visant les dirigeants (whaling), protocoles SPF/DKIM/DMARC, usurpation de l'expéditeur et formation des employés à la sécurité.

PRÉSENTATION DE L'APPRENTISSAGE : ATTAQUES PAR HAMEÇONNAGE

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 les attaques par hameçonnage et l'ingénierie sociale. Vous étudierez le spear phishing, le whaling, l'usurpation de domaine, les protocoles SPF/DKIM/DMARC, la sécurité des liens et la formation de sensibilisation des employés.

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/attaques-phishing/

Votre parcours d'apprentissage : atténuation de l'hameçonnage

- Identifier les arnaques courantes : hameçonnage, vishing et fenêtres pop-up de faux support technique.
- Mettre en place des procédures de vérification des transactions par un canal distinct (hors bande).
- Configurez des règles SPF, DKIM et DMARC pour bloquer les domaines usurpés.

CONSIGNES DU GUIDE SUR LES ATTAQUES PAR HAMEÇONNAGE

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 l'authentification des e-mails. Terminez par l'activité bonus Réflexion rapide.

ATTAQUES PAR HAMEÇONNAGE ET INGÉNIERIE SOCIALE (INTRODUCTION)

Les attaques par hameçonnage utilisent des messages ciblés, des arnaques de type whaling et l'usurpation de domaine pour récolter les identifiants de connexion. Sécuriser les systèmes d'une entreprise exige de déployer des règles SPF, DKIM et DMARC sur la passerelle, en plus d'étapes d'approbation par un canal distinct.

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

Point de contrôle 1 : Défi QCM

1. Qu'est-ce que le spear phishing (hameçonnage ciblé) ?

- A. Un e-mail d'hameçonnage ciblé, adapté à une personne ou une organisation précise
- B. Un e-mail de masse envoyé à des millions d'adresses aléatoires
- C. Une attaque réseau qui inonde de trafic les serveurs web
- D. Une technique d'extraction de base de données visant les fiches utilisateurs

2. Quel protocole permet à un domaine de publier dans le DNS ses adresses IP d'envoi autorisées pour lutter contre l'usurpation ?

- A. SPF
- B. DKIM
- C. DMARC
- D. HTTPS

3. Qu'est-ce qu'une attaque de whaling ?

- A. Une campagne d'hameçonnage visant spécifiquement des dirigeants d'entreprise de premier plan
- B. Une attaque par injection SQL visant les sauvegardes de base de données
- C. Le vol physique de l'équipement routeur du réseau local
- D. Une analyse automatisée par force brute de type credential stuffing

4. À quoi sert DKIM ?

- A. Ajoute une signature cryptographique aux e-mails pour vérifier l'authenticité de l'expéditeur
- B. Bloque le trafic des paquets réseau entrants au niveau du pare-feu
- C. Chiffre les volumes de stockage de la base de données au repos
- D. Analyse les pièces jointes des e-mails à la recherche de malwares connus par signature

5. Quel est le rôle de DMARC ?

- A. Indiquer aux serveurs de messagerie destinataires comment traiter les échecs des vérifications SPF/DKIM
- B. Déchiffrer les mots de passe du système à l'aide de tables arc-en-ciel précalculées
- C. Compresser les pièces jointes avant l'envoi
- D. Configurer les droits d'accès au routage réseau

Point de contrôle 2 : Défi Vrai ou Faux

6 Question 6

6. L'hameçonnage ciblé (spear phishing) repose sur des e-mails génériques envoyés en masse à des millions d'adresses aléatoires.

- ◯ Vrai
- ◯ Faux

7 Question 7

7. Les politiques DMARC peuvent demander aux serveurs de messagerie de rejeter les messages usurpés non autorisés.

- ◯ Vrai
- ◯ Faux

8 Question 8

8. La vérification SPF fonctionne en validant la signature cryptographique du corps de l'e-mail.

- ◯ Vrai
- ◯ Faux

9 Question 9

9. Les attaques de whaling ciblent des administrateurs subalternes de l'entreprise pour accéder aux fichiers de bases de données.

- ◯ Vrai
- ◯ Faux

10 Question 10

10. La vérification hors bande des demandes de paiement aide à stopper les arnaques au virement bancaire.

- ◯ 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. Cibler un employé précis avec des informations personnalisées s'appelle le _____ .
2. Falsifier un en-tête d'e-mail pour donner aux messages une apparence légitime relève du _____ de l'expéditeur.
3. La liste, dans un enregistrement DNS, des IP de serveurs de messagerie autorisés est _____ .
4. La norme de signature des e-mails qui permet de vérifier l'expéditeur est _____ .
5. Définir des politiques de rejet en cas d'échec des contrôles SPF/DKIM fait appel à _____ .
6. Une campagne d'hameçonnage visant les hauts dirigeants s'appelle le _____ .

BANQUE DE MOTS DE VOCABULAIRE

DKIM DMARC HAMEÇONNAGE HARPONNAGE SPF USURPATION VISHING WHALING

Écrivez vos réponses ici :

1.
2.
3.
4.
5.
6.

Point de contrôle 4 : Association de notions sur la sécurité

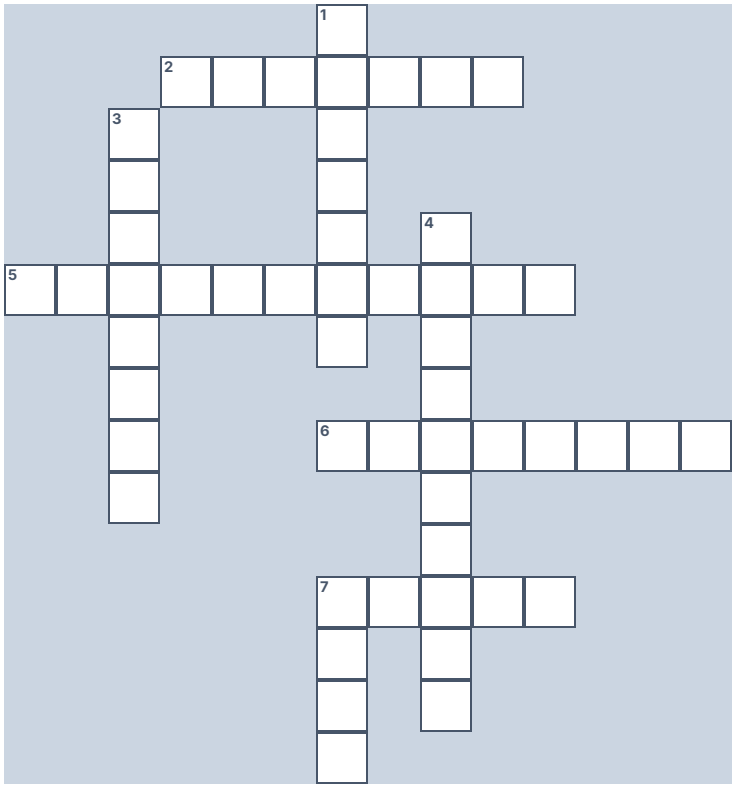
ASSOCIATION DE DÉFINITIONS

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. HAMEÇONNAGE CIBLÉ	A	Appels frauduleux par téléphone.
☐	2. USURPATION	B	Cibler les cadres dirigeants.
☐	3. SPF	C	Instructions de rejet de la politique.
☐	4. DKIM	D	Adresses IP d'expéditeurs autorisées dans le DNS.
☐	5. DMARC	E	E-mail d'ingénierie sociale.
☐	6. WHALING	F	E-mail ciblé et personnalisé.
☐	7. HAMEÇONNAGE	G	Falsification de l'adresse e-mail de l'expéditeur.
☐	8. HAMEÇONNAGE VOCAL (VISHING)	H	Signature cryptographique dans un e-mail.

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

2. Appels frauduleux par la voix. (7)

5. E-mail d'ingénierie sociale. (11)

6. Falsification de l'adresse e-mail de l'expéditeur. (8)

7. Instructions de politique de rejet. (5)

VERTICALEMENT

1. Cible les hauts dirigeants. (7)

3. IP d'expéditeurs autorisées publiées dans le DNS. (8)

4. E-mail ciblé et personnalisé (spear phishing). (10)

7. Signature cryptographique dans un e-mail. (4)

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

2 horizontal: Appels frauduleux par la voix. (7 lettres):

5 horizontal: E-mail d'ingénierie sociale. (11 lettres):

6 horizontal: Falsification de l'adresse e-mail de l'expéditeur. (8 lettres):

7 horizontal: Instructions de politique de rejet. (5 lettres):

VERTICALEMENT

1 vertical: Cible les hauts dirigeants. (7 lettres):

3 vertical: IP d'expéditeurs autorisées publiées dans le DNS. (8 lettres):

4 vertical: E-mail ciblé et personnalisé (spear phishing). (10 lettres):

7 vertical: Signature cryptographique dans un e-mail. (4 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.

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

LISTE DE MOTS DE VOCABULAIRE

HARPONNAGE SPOOFING NORMESPF DKIM DMARC WHALING
HAMECONNAGE VISHING

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. HARPONNAGE
B. SPOOFING
C. NORMESPF
D. DKIM
E. DMARC
F. WHALING
G. HAMECONNAGE
H. VISHING

	DÉFINITIONS ET CHAMPS D'ASSOCIATION
	1. Falsification de l'adresse e-mail de l'expéditeur.
	2. E-mail ciblé et personnalisé (spear phishing).
	3. Appels frauduleux par la voix.
	4. IP d'expéditeurs autorisées publiées dans le DNS.
	5. E-mail d'ingénierie sociale.
	6. Instructions de politique de rejet.
	7. Signature cryptographique dans un e-mail.
	8. Cible les hauts dirigeants.

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. **GNNOAHAEPR** _____
2. **MNFOPSER** _____
3. **ADCRM** _____
4. **NGEOMCANHAE** _____
5. **FIPGOSNO** _____
6. **IMDK** _____
7. **WNIGHLA** _____
8. **IHGVNIS** _____

Activité bonus : Réflexion rapide

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

1	Appareils qui peuvent être piratés			
2	Signes d'un e-mail d'hameçonnage			
3	Signes qu'un ordinateur est infecté			
4	Mots qui créent une fausse urgence			
5	Façons de vérifier un expéditeur			
6	Personnes à qui demander de l'aide informatique			
7	Choses que vous sauvegardez			
8	Poissons ou créatures marines que vous connaissez			
9	Entreprises dont les escrocs usurpent l'identité			
10	Bonnes habitudes de sécurité à adopter dès aujourd'hui			
11	Choses à faire après avoir cliqué sur un faux lien			
12	Choses à faire après une fuite de données			
13	Canaux où se produit l'hameçonnage			
14	Choses que vous n'envoyez jamais par e-mail			
15	Façons de protéger vos comptes			

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 : REMÉDIATION D'UNE ATTAQUE DE WHALING VISANT LA DIRECTION

👨‍💻

Scénario : Un directeur financier reçoit un e-mail très personnalisé, se présentant comme venant du PDG, qui demande un virement rapide de $50,000 pour conclure l'achat confidentiel d'un domaine.

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 : DÉPLOYER DES POLITIQUES DE PASSERELLE SPF/DKIM/DMARC

👨‍💻

Scénario : Une entreprise échoue à ses audits de sécurité parce que ses e-mails marketing sortants sont fréquemment signalés comme spam et que des pirates usurpent activement le domaine de sa marque.

Question de discussion : Mettez en place des contrôles techniques et administratifs pour vérifier l'authenticité des e-mails.

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

18 5 16 5 18 5 26 20 15 21 20 5

9 14 7 5 14 9 5 18 9 5 19 15 3 9 1 12 5

16 1 18 1 21 4 9 20 5 13 1 9 12

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'hameçonnage (phishing) ?

L'hameçonnage est une attaque d'ingénierie sociale dans laquelle des criminels envoient des messages frauduleux pour amener les utilisateurs à partager des données sensibles.

Q2: Quelle est la différence entre l'hameçonnage et le spear phishing ?

L'hameçonnage vise de larges groupes avec un contenu générique, tandis que le spear phishing vise des victimes précises à l'aide de détails personnalisés.

Q3: Qu'est-ce que le whaling ?

Le whaling est une attaque d'hameçonnage très ciblée visant des dirigeants de premier plan qui détiennent un pouvoir administratif.

Q4: Qu'est-ce que l'usurpation d'adresse e-mail (spoofing) ?

L'usurpation d'e-mail (spoofing) consiste à créer des messages avec une adresse d'expéditeur falsifiée pour amener le destinataire à faire confiance à la source.

Q5: Comment SPF empêche-t-il l'usurpation ?

Il publie dans le DNS une liste d'adresses IP autorisées à envoyer des e-mails, ce qui permet aux serveurs destinataires de vérifier la provenance du courrier. [1]

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: Qu'est-ce que DKIM ?

DomainKeys Identified Mail ajoute une signature cryptographique aux en-têtes des e-mails, prouvant qu'un domaine en a pris la responsabilité et que le message n'a pas été modifié.

Q7: Que signifie DMARC ?

Domain-based Message Authentication, Reporting, and Conformance (authentification, rapports et conformité des messages basés sur le domaine). [2]

Q8: Qu'est-ce qu'une politique DMARC ?

Une politique qui indique aux serveurs de messagerie comment traiter les messages qui échouent aux vérifications SPF/DKIM (none, quarantine ou reject). [2]

Q9: Qu'est-ce que le vishing ?

Hameçonnage vocal, où les attaquants utilisent des appels téléphoniques frauduleux pour obtenir des données administratives ou financières.

Q10: En quoi les analyseurs de liens sont-ils utiles ?

Ils analysent et réécrivent les liens des e-mails entrants pour vérifier la sécurité des pages web de destination au moment du clic.

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 fonctionne une attaque par homographe ?

Les attaquants enregistrent des noms de domaine utilisant des caractères Unicode non ASCII ressemblants pour imiter visuellement un nom de domaine légitime.

Q2: Qu'est-ce que la représentation punycode ?

Un encodage qui convertit les noms de domaine Unicode en chaînes compatibles ASCII commençant par 'xn--' pour que le DNS puisse les traiter.

Q3: Pourquoi 'p=reject' est-il le réglage DMARC le plus sûr ?

Il demande aux serveurs destinataires de rejeter, pendant la session SMTP, les messages qui échouent à DMARC (SPF/DKIM alignés), ce qui bloque l'usurpation directe. [2]

Q4: Comment les attaquants contournent-ils les règles SPF ?

En exploitant des domaines ressemblants (typosquatting) ou en utilisant des comptes compromis sur des services de messagerie tiers légitimes.

Q5: Qu'est-ce que la compromission de messagerie d'entreprise (BEC) ?

Une escroquerie visant les entreprises, dans laquelle les attaquants piratent ou usurpent des comptes de messagerie professionnels pour autoriser des paiements frauduleux.

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: Comment l'authentification multifacteur bloque-t-elle l'hameçonnage ?

Elle exige des jetons secondaires (comme des clés matérielles) qui ne peuvent pas être volés au moyen de simples pages d'accueil imitées.

Q7: Qu'est-ce qu'une page de destination de collecte d'identifiants ?

Un portail de connexion imitant l'original, conçu pour capturer en temps réel les noms d'utilisateur, les mots de passe et les codes MFA saisis.

Q8: Qu'est-ce que le détournement de sous-domaine ?

Un attaquant qui prend le contrôle d'un pointeur DNS de sous-domaine inutilisé pour héberger des pages d'hameçonnage malveillantes sous un domaine parent de confiance.

Q9: Comment fonctionne la vérification d'alignement DKIM ?

Il vérifie que le domaine de l'en-tête 'From' correspond au domaine qui a signé cryptographiquement le message dans l'en-tête DKIM.

Q10: Quel est le rôle d'une passerelle de messagerie ?

Filtrer les e-mails entrants, vérifier les liens, exécuter les pièces jointes en bac à sable et valider la conformité SPF/DKIM/DMARC.

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

L'hameçonnage et l'usurpation ont été le type de délit le plus signalé à l'IC3 du FBI en 2025, avec 191,561 plaintes. [4]

2. APERÇU SÉCURITÉ

La compromission de messagerie professionnelle (BEC) a causé plus de $3 milliards de pertes signalées à l'IC3 du FBI en 2025. [4]

3. APERÇU SÉCURITÉ

Les attaques par homographe utilisent des lettres cyrilliques ressemblantes pour reproduire visuellement, dans les navigateurs, des domaines de marque à correspondance exacte.

4. APERÇU SÉCURITÉ

Avec 'p=reject', un domaine demande aux destinataires de refuser les e-mails non conformes lors de la remise, et non de les classer comme spam. [2]

5. APERÇU SÉCURITÉ

Les attaques de whaling visant des PDG demandent souvent des paiements urgents pour des fusions confidentielles ou des achats de domaines.

6. APERÇU SÉCURITÉ

Les portails de collecte d'identifiants copient de vraies pages de connexion, si bien que les victimes saisissent leur mot de passe directement dans le formulaire de l'attaquant.

7. ZOOM SUR LA SÉCURITÉ

Les recommandations conjointes de la CISA sur le hameçonnage préconisent de former les utilisateurs, en plus de DMARC, SPF, DKIM et d'une MFA résistante au hameçonnage. [3]

8. ZOOM SUR LA SÉCURITÉ

L'évaluation SPF est limitée à 10 termes déclenchant des requêtes DNS ; dépasser cette limite renvoie un résultat 'permerror'. [1]

9. ZOOM SUR LA SÉCURITÉ

Les clés de sécurité matérielles FIDO2 offrent une protection fondée sur la cryptographie contre la collecte d'identifiants à distance.

10. APERÇU SÉCURITÉ

L'hameçonnage est l'un des moyens les plus courants par lesquels les attaquants pénètrent d'abord dans une organisation ; c'est pourquoi une formation régulière de sensibilisation est une défense efficace.

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] IETF. (2014). RFC 7208: Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, Version 1.

https://www.rfc-editor.org/rfc/rfc7208.html

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

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

[3] 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

[4] FBI Internet Crime Complaint Center. (2026). 2025 IC3 Annual Report.

https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf

[5] CISA. (n.d.). Malware, Phishing, and Ransomware.

https://www.cisa.gov/topics/cyber-threats-and-advisories/malware-phishing-and-ransomware

Corrigé : Point de contrôle 1 – Choix multiple

1 Question 1

Bonne réponse : A

NOTE PÉDAGOGIQUE

Qu'est-ce que le spear phishing (hameçonnage ciblé) ? → Un e-mail d'hameçonnage ciblé, adapté à une personne ou une organisation précise

2 Question 2

Bonne réponse : A

NOTE PÉDAGOGIQUE

SPF publie dans le DNS les hôtes d'envoi autorisés d'un domaine, afin que les destinataires puissent vérifier l'expéditeur de l'enveloppe.

3 Question 3

Bonne réponse : A

NOTE PÉDAGOGIQUE

Qu'est-ce qu'une attaque de whaling ? → Une campagne d'hameçonnage visant spécifiquement des dirigeants d'entreprise de premier plan

4 Question 4

Bonne réponse : A

NOTE PÉDAGOGIQUE

À quoi sert DKIM ? → Ajoute une signature cryptographique aux e-mails pour vérifier l'authenticité de l'expéditeur

5 Question 5

Bonne réponse : A

NOTE PÉDAGOGIQUE

Quel est le rôle de DMARC ? → Indiquer aux serveurs de messagerie destinataires comment traiter les échecs des vérifications SPF/DKIM

Corrigé : Point de contrôle 2 – Vrai ou faux

6 Question 6

Bonne réponse : Faux

NOTE PÉDAGOGIQUE

Faux : le spear phishing est adapté à des personnes précises, contrairement à l'hameçonnage de masse générique.

7 Question 7

Bonne réponse : Vrai

NOTE PÉDAGOGIQUE

Les politiques DMARC peuvent demander aux serveurs de messagerie de rejeter les messages usurpés non autorisés.

8 Question 8

Bonne réponse : Faux

NOTE PÉDAGOGIQUE

Faux : SPF compare l'IP d'envoi au DNS ; c'est DKIM qui vérifie une signature cryptographique.

9 Question 9

Bonne réponse : Faux

NOTE PÉDAGOGIQUE

Faux : le whaling cible les cadres supérieurs, qui peuvent approuver des paiements et accéder à des données sensibles.

10 Question 10

Bonne réponse : Vrai

NOTE PÉDAGOGIQUE

Vrai : confirmer les demandes de paiement par un canal distinct et connu aide à stopper la fraude au virement.

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

F 1. HAMEÇONNAGE CIBLÉ	G 2. USURPATION	D 3. SPF	H 4. DKIM
C 5. DMARC	B 6. WHALING	E 7. HAMEÇONNAGE	A 8. HAMEÇONNAGE VOCAL (VISHING)

POINT DE CONTRÔLE 3 : CORRIGÉ DES TERMES CLÉS

1 HARPONNAGE	2 USURPATION	3 SPF	4 DKIM
5 DMARC	6 WHALING		

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

1 B – SPOOFING	2 A – HARPONNAGE	3 H – VISHING	4 C – NORMESPF
5 G – HAMECONNAGE	6 E – DMARC	7 D – DKIM	8 F – WHALING

NOTES DE DISCUSSION POUR LES ENSEIGNANTS

Termes clés :
Vérifiez que les élèves savent expliquer HAMEÇONNAGE CIBLÉ, USURPATION et SPF 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.

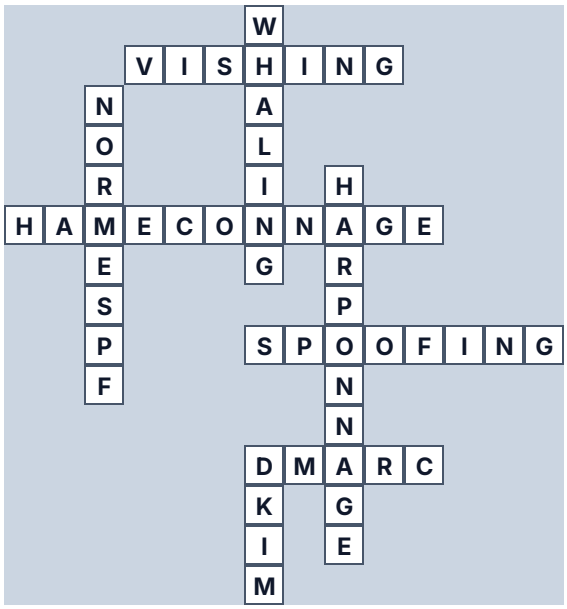
Évaluation des sources :
Faites vérifier au moins une affirmation à l'aide des sources de la fiche et discutez des raisons pour lesquelles les chiffres, les prix et les règles peuvent évoluer avec le temps.

Corrigés des jeux et notes pour l'enseignant

SOLUTION DES MOTS CACHÉS

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

SOLUTION DES MOTS CROISÉS



GUIDE DE L'ENSEIGNANT : SOLUTIONS DES MOTS CROISÉS

HORIZONTALEMENT

2 horizontal: VISHING Appels frauduleux par la voix. (7 lettres)

5 horizontal: HAMECONNAGE E-mail d'ingénierie sociale. (11 lettres)

6 horizontal: SPOOFING Falsification de l'adresse e-mail de l'expéditeur. (8 lettres)

7 horizontal: DMARC Instructions de politique de rejet. (5 lettres)

VERTICALEMENT

1 vertical: WHALING Cible les hauts dirigeants. (7 lettres)

3 vertical: NORMESPF IP d'expéditeurs autorisées publiées dans le DNS. (8 lettres)

4 vertical: HARPONNAGE E-mail ciblé et personnalisé (spear phishing). (10 lettres)

7 vertical: DKIM Signature cryptographique dans un e-mail. (4 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.	G N N O A H A E P R	HARPONNAGE	5.	F I P G O S N O	SPOOFING
2.	M N F O P S E R	NORMESPF	6.	I M D K	DKIM
3.	A D C R M	DMARC	7.	W N I G H L A	WHALING
4.	N G E O M C A N H A E	HAMECONNAGE	8.	I H G V N I S	VISHING

CORRIGÉ DU DÉFI DU CODE SECRET

"REPEREZ TOUTE INGENIERIE SOCIALE PAR AUDIT EMAIL"

Corrigé des études de cas

A Étude de cas 1 : Remédiation d'une attaque de whaling visant la direction

Corrigé de l'enseignant

CONSIGNE DE NOTATION

Les réponses des élèves doivent couvrir les points suivants :

- Analyse de scénario : un directeur financier reçoit un e-mail très personnalisé, censé provenir du PDG, qui demande un virement rapide de 50 000 $ pour conclure l'achat confidentiel d'un domaine.
- Stratégie et solution recommandées : configurer DMARC avec une politique 'p=reject' pour bloquer les domaines d'expéditeurs usurpés. Ajouter des bannières d'avertissement pour les expéditeurs externes au niveau de la passerelle et exiger une confirmation orale, hors bande, pour toutes les transactions financières.

B Étude de cas 2 : Déployer des politiques de passerelle SPF/DKIM/DMARC

Corrigé de l'enseignant

CONSIGNE DE NOTATION

Les réponses des élèves doivent couvrir les points suivants :

- Analyse de scénario : une entreprise échoue à ses audits de sécurité parce que ses e-mails marketing sortants sont souvent signalés comme spam et que des pirates usurpent activement le domaine de sa marque.
- Stratégie et solution recommandées : publiez un enregistrement TXT pour SPF indiquant les IP d'expéditeurs autorisées. Configurez des clés de signature DKIM sur les serveurs de messagerie sortants et analysez les rapports XML de retour DMARC entrants pour repérer les abus.