Nom : _____ Date : _____ Note : _____

Arnaques en ligne et ingénierie sociale Guide de protection

Hameçonnage (phishing) par e-mail, domaines usurpés, vishing, arnaques au support technique, vérification hors bande, fraude au président (BEC)

PRÉSENTATION DE L'APPRENTISSAGE : ARNAQUES EN LIGNE

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 défense contre les arnaques en ligne. Vous étudierez les faux sites d'hameçonnage, les tactiques d'ingénierie sociale, les arnaques au faux support technique, les vecteurs de fraude au virement et les méthodes de vérification des paiements.

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/arnaques-en-ligne/

Votre parcours d'apprentissage : protection contre les arnaques en ligne

- Identifier les signes courants des arnaques au support technique et des domaines de typosquatting.
- Mettre en œuvre des protocoles de vérification des e-mails (SPF, DKIM, DMARC) contre l'usurpation.
- Mettre en place une vérification des transactions hors bande pour prévenir la fraude au virement en entreprise.

CONSIGNES DU GUIDE SUR LES ARNAQUES EN LIGNE

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 contre les arnaques en ligne. Terminez par l'activité bonus Réflexion rapide.

PROTECTION CONTRE LES ARNAQUES EN LIGNE ET L'INGÉNIERIE SOCIALE (INTRODUCTION)

Les arnaques en ligne exploitent le comportement humain par l'hameçonnage (phishing), les fenêtres de faux support, le vishing et la fraude au virement. Imposer une vérification des transactions par un canal distinct et des règles de domaine SPF/DKIM/DMARC aide à bloquer les vecteurs d'ingénierie sociale dès la passerelle.

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

Point de contrôle 1 : Défi QCM

1. Quel est le principal indice d'une arnaque au support technique ?

- A. Une fenêtre surgissante affirmant que votre système est infecté et exigeant que vous appeliez un numéro de téléphone
- B. Une mise à jour de sécurité automatique téléchargée depuis un dépôt officiel
- C. Un gestionnaire de mots de passe qui refuse de remplir les identifiants sur un domaine d'entreprise
- D. Une sauvegarde de fichiers en arrière-plan sur un disque externe

2. Quelle technique utilise des domaines d'expéditeur usurpés pour voler des coordonnées bancaires ?

- A. Hameçonnage par e-mail
- B. Analyse de ports
- C. Injection en mémoire
- D. Effacement cryptographique

3. Qu'est-ce qui correspond à une fraude au virement bancaire ?

- A. Amener des victimes, par ingénierie sociale, à envoyer de l'argent sur de faux comptes d'entreprise
- B. Chiffrer les bases de données du système à l'aide de charges utiles de rançongiciel
- C. Interroger des bases de données au moyen de commandes d'injection SQL
- D. Sauvegarder les fichiers système sur des disques de stockage hors ligne

4. Pourquoi les escrocs créent-ils de faux sites marchands ?

- A. Voler les données de carte de crédit et les identifiants de paiement des acheteurs
- B. Héberger les tables de base de données d'analyse de logiciels malveillants en bac à sable
- C. Pour accélérer la livraison des commandes en ligne
- D. Pour tester gratuitement de nouveaux designs de site web

5. Que signifie le vishing ?

- A. Escroqueries d'hameçonnage vocal par téléphone pour voler des identifiants
- B. Analyser les réseaux locaux à la recherche d'appareils non sécurisés
- C. Restaurer les bases de données système après une intrusion non autorisée
- D. Exécuter du code non fiable dans des conteneurs virtuels sécurisés

Point de contrôle 2 : Défi Vrai ou Faux

6 Question 6

6. Les arnaques par hameçonnage ne visent que les utilisateurs finaux, jamais les dirigeants ciblés par le whaling.

- ○ Vrai
- ○ Faux

7 Question 7

7. Les domaines usurpés utilisent souvent de légères fautes de frappe (comme amaz0n.com) pour imiter des marques de confiance.

- ○ Vrai
- ○ Faux

8 Question 8

8. Les arnaques au faux support technique peuvent être résolues en accordant un accès à distance à l'appelant.

- ○ Vrai
- ○ Faux

9 Question 9

9. L'ingénierie sociale exploite la psychologie humaine, comme la peur et l'urgence, pour contourner les règles de sécurité.

- ○ Vrai
- ○ Faux

10 Question 10

10. Les demandes de virement doivent toujours être vérifiées par un canal de communication distinct (hors bande).

- ○ 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 e-mails frauduleux qui piègent les utilisateurs relèvent de l' _____ .
2. Une adresse web qui imite une marque de confiance est un domaine _____ .
3. Les arnaques vocales visant les coordonnées bancaires s'appellent le _____ .
4. Une fenêtre surgissante qui exige de l'argent pour supprimer un virus est une _____ au faux support technique.
5. Confirmer une demande de paiement nécessite une _____ hors bande.
6. Rediriger des transactions d'entreprise vers les comptes de voleurs relève de la fraude au _____ .

BANQUE DE MOTS DE VOCABULAIRE

ARNAQUE HAMEÇONNAGE SMISHING USURPÉ VÉRIFICATION VIREMENT VISHING WHALING

Écrivez vos réponses ici :

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

Point de contrôle 4 : Association de notions sur la sécurité

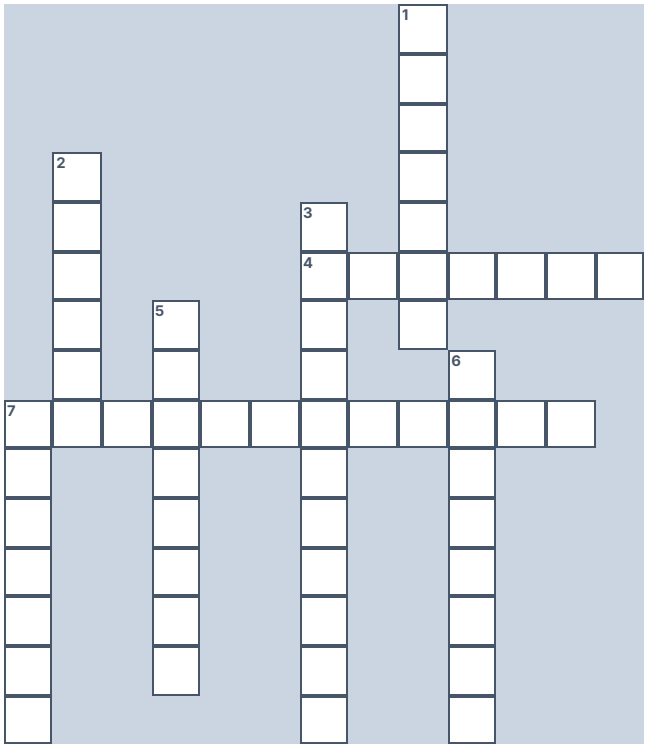
ASSOCIATION DE DÉFINITIONS

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	A	Détournement frauduleux de transactions bancaires vers des comptes criminels.
☐	2. USURPÉ	B	Escroquerie conçue pour dérober de l'argent ou des identifiants d'accès aux victimes.
☐	3. HAMEÇONNAGE VOCAL (VISHING)	C	Envoyer des SMS frauduleux pour voler les identifiants de comptes mobiles.
☐	4. ARNAQUE	D	Appels vocaux frauduleux conçus pour voler des identifiants et des informations de compte.
☐	5. VÉRIFICATION	E	Attaques d'hameçonnage ciblées visant à voler les identifiants des cadres dirigeants.
☐	6. VIREMENT	F	Adresse d'expéditeur d'e-mail ou de site web imitée pour paraître légitime.
☐	7. WHALING	G	Campagnes d'e-mails frauduleux conçues pour voler des identifiants de connexion et des mots de passe.
☐	8. SMISHING	H	Confirmer les détails d'un paiement par un autre moyen de contact de confiance.

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

4. Stratagème frauduleux visant à soutirer de l'argent ou des identifiants aux victimes. (7)

7. Confirmation des informations de paiement par un moyen de contact secondaire de confiance. (12)

VERTICALEMENT

1. Attaques d'hameçonnage ciblées visant à voler les identifiants des hauts dirigeants. (7)

2. Se dit d'un expéditeur d'e-mail ou d'une adresse de site imités pour paraître légitimes. (6)

3. Campagnes d'e-mails frauduleux visant à voler identifiants de connexion et mots de passe. (11)

5. Envoi de SMS frauduleux pour voler les identifiants de comptes mobiles. (8)

6. Détournement frauduleux de transactions bancaires vers des comptes criminels. (8)

7. Appels vocaux frauduleux visant à voler des identifiants et des informations de compte. (7)

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

4 horizontal: Stratagème frauduleux visant à soutirer de l'argent ou des identifiants aux victimes. (7 lettres):

7 horizontal: Confirmation des informations de paiement par un moyen de contact secondaire de confiance. (12 lettres):

VERTICALEMENT

1 vertical: Attaques d'hameçonnage ciblées visant à voler les identifiants des hauts dirigeants. (7 lettres):

2 vertical: Se dit d'un expéditeur d'e-mail ou d'une adresse de site imités pour paraître légitimes. (6 lettres):

3 vertical: Campagnes d'e-mails frauduleux visant à voler identifiants de connexion et mots de passe. (11 lettres):

5 vertical: Envoi de SMS frauduleux pour voler les identifiants de comptes mobiles. (8 lettres):

6 vertical: Détournement frauduleux de transactions bancaires vers des comptes criminels. (8 lettres):

7 vertical: Appels vocaux frauduleux visant à voler des identifiants et des informations de compte. (7 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.

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

LISTE DE MOTS DE VOCABULAIRE

HAMECONNAGE, USURPE, VISHING, WHALING, ARNAQUE, SMISHING, VERIFICATION, VIREMENT

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. HAMECONNAGE
B. USURPE
C. VISHING
D. ARNAQUE
E. VERIFICATION
F. VIREMENT
G. WHALING
H. SMISHING

	DÉFINITIONS ET CHAMPS D'ASSOCIATION
	1. Se dit d'un expéditeur d'e-mail ou d'une adresse de site imités pour paraître légitimes.
	2. Confirmation des informations de paiement par un moyen de contact secondaire de confiance.
	3. Détournement frauduleux de transactions bancaires vers des comptes criminels.
	4. Envoi de SMS frauduleux pour voler les identifiants de comptes mobiles.
	5. Attaques d'hameçonnage ciblées visant à voler les identifiants des hauts dirigeants.
	6. Appels vocaux frauduleux visant à voler des identifiants et des informations de compte.
	7. Campagnes d'e-mails frauduleux visant à voler identifiants de connexion et mots de passe.
	8. Stratagème frauduleux visant à soutirer de l'argent ou des identifiants aux victimes.

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. CNGAONHAMEE
2. VSGNIHI
3. VEACOTRINFII
4. GHILNWA
5. RUEUPS
6. UNQAAER
7. VTMENIER
8. SMHGSNII

Activité bonus : Réflexion rapide

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

1	Appareils qui peuvent être piratés			
2	Phrases souvent utilisées par les escrocs			
3	Moyens de paiement que demandent les escrocs			
4	Types d'arnaques en ligne			
5	Offres trop belles pour être vraies			
6	Endroits où signaler une arnaque			
7	Mots liés à la cybersécurité			
8	Personnes que vous pouvez avertir des arnaques			
9	Choses que vous sauvegardez			
10	Signaux d'alerte dans un e-mail			
11	Signes qu'un ordinateur est infecté			
12	Façons de vérifier une boutique en ligne			
13	Façons de protéger vos comptes			
14	Choses à faire si vous vous êtes fait arnaquer			
15	Choses à faire après une fuite de données			

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 : PRÉVENTION DES ESCROQUERIES AU VIREMENT EN ENTREPRISE

👷

Scénario : Un service financier reçoit un e-mail urgent provenant de l'adresse usurpée d'un fournisseur, qui demande que les futurs virements de factures soient dirigés vers un nouveau numéro de compte.

Question de discussion : Décrivez la politique de vérification contre la fraude au virement et précisez les blocages fondés sur l'authentification des e-mails.

ÉTUDE DE CAS 2 : INCIDENT DE WHALING VISANT UN DIRIGEANT

👷

Scénario : Un dirigeant a cliqué sur un lien d'hameçonnage prétendant contenir un document confidentiel de réunion du conseil d'administration, et a saisi ses principaux identifiants d'entreprise sur un portail usurpé.

Question de discussion : Détaillez les étapes de réponse à l'incident et expliquez comment auditer les connexions des dirigeants.

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		12	5		16	8	9	19	8	9	14	7
							7	18	1	3	5		1		12	1		
						22	5	18	9	6	9	3	1	20	9	15	14	

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 qu'une arnaque en ligne ?

Une escroquerie qui utilise des canaux numériques pour amener les victimes à envoyer de l'argent ou à divulguer leurs identifiants personnels.

Q2: Quel est le principal indice d'un e-mail d'hameçonnage ?

Un message qui invoque l'urgence (comme la suspension d'un compte) et vous dirige vers un lien qui ne correspond pas au domaine officiel.

Q3: Qu'est-ce que le typosquatting ?

Enregistrement de domaines reprenant des fautes de frappe courantes de marques populaires (comme amaz0n.com) pour héberger de faux sites d'hameçonnage.

Q4: Qu'est-ce qu'une arnaque au faux support technique ?

Une fenêtre surgissante affirmant que votre PC est infecté et vous invitant à appeler un numéro et à payer un faux logiciel de nettoyage ou des services d'accès à distance. [1]

Q5: Qu'est-ce que le vishing ?

Attaques par hameçonnage utilisant des appels téléphoniques pour pousser les victimes à divulguer leurs coordonnées bancaires ou leurs identifiants de connexion.

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 la fraude électronique (wire fraud) ?

Redirection de transactions de paiement vers des comptes frauduleux en se faisant passer pour des fournisseurs ou des dirigeants.

Q7: Qu'est-ce que le whaling ?

Une forme très ciblée de harponnage (spear phishing) qui vise directement des cibles de grande valeur, comme les dirigeants d'entreprise.

Q8: Qu'est-ce que le smishing ?

SMS frauduleux envoyés sur des appareils mobiles, contenant des liens vers de faux portails ou de prétendues mises à jour de suivi de colis.

Q9: Pourquoi la vérification hors bande est-elle essentielle ?

Elle confirme les détails de la transaction par un canal de communication distinct (comme un appel téléphonique), en évitant les fils d'e-mails compromis.

Q10: Comment fonctionne une arnaque au faux séquestre (escrow) ?

Les escrocs créent un faux site de séquestre (escrow) en affirmant que les fonds sont conservés en toute sécurité, puis volent le virement de l'acheteur.

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 les escrocs utilisent-ils la compromission de messagerie professionnelle (BEC) pour commettre une fraude au virement ?

Ils piratent le compte e-mail d'un employé légitime, surveillent les échanges sur les factures et envoient des coordonnées de facturation modifiées avec des comptes bancaires frauduleux.

Q2: Quel est le risque des attaques par homographes IDN dans les arnaques en ligne ?

Utilisation de caractères non ASCII identiques en apparence à des lettres normales (par ex. le 'a' cyrillique) pour enregistrer des domaines frauduleux imitant de vraies marques.

Q3: Pourquoi l'examen des en-têtes d'e-mail est-il important pour détecter les arnaques ?

Ils révèlent l'IP réelle du serveur d'origine et le résultat de la validation SPF/DKIM, ce qui montre si le domaine de l'expéditeur est falsifié.

Q4: Comment les escrocs au faux support technique exploitent-ils les logiciels de bureau à distance ?

Ils utilisent des outils comme AnyDesk ou TeamViewer pour se connecter à l'appareil de la victime, y installer un logiciel malveillant et voler les mots de passe enregistrés.

Q5: Quel est l'objectif des arnaques aux frais payés d'avance ?

Pousser les victimes à payer d'avance des frais de dossier en échange d'une importante récompense financière qui n'existe pas.

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 les escrocs utilisent-ils le profilage sur les réseaux sociaux pour l'hameçonnage ciblé ?

Ils compilent les organigrammes des entreprises et les noms des employés pour rédiger des e-mails de harponnage (spear-phishing) convaincants.

Q7: Pourquoi les fausses boutiques en ligne proposent-elles de fortes remises ?

Pour pousser les acheteurs à saisir les données de leur carte bancaire, afin de capturer ces informations pour les réutiliser ou les revendre sur des forums de carding.

Q8: Comment les enregistrements DMARC bloquent-ils les arnaques par hameçonnage ?

DMARC permet aux propriétaires de domaines de demander aux destinataires de mettre en quarantaine ou de rejeter les messages qui échouent aux vérifications SPF et DKIM alignées, ce qui bloque l'usurpation directe. [5]

Q9: Quelle est la menace des portails de collecte d'identifiants ?

Pages d'arrivée usurpées conçues pour ressembler exactement à Microsoft 365 ou Google Workspace, qui volent les identifiants au moment où ils sont saisis.

Q10: Comment les équipes de sécurité signalent-elles et neutralisent-elles les domaines frauduleux ?

En transmettant les preuves de fraude à l'adresse e-mail de signalement d'abus du bureau d'enregistrement, à l'hébergeur et au registre Google Safe Browsing.

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. [2]

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. [2]

3. APERÇU SÉCURITÉ

Les domaines de typosquatting ne diffèrent des vrais noms de marque que d'un ou deux caractères, si bien qu'un coup d'œil rapide peut ne pas les repérer.

4. APERÇU SÉCURITÉ

Les arnaques au faux support technique ont causé plus de $2.1 milliards de pertes signalées à l'IC3 du FBI en 2025. [2]

5. APERÇU SÉCURITÉ

Les attaques par homographe paraissent identiques dans la barre d'adresse du navigateur, sauf si celui-ci affiche le punycode.

6. APERÇU SÉCURITÉ

Les arnaques par SMS (smishing) utilisent des messages courts et urgents contenant des liens, ce qui laisse aux victimes peu d'éléments pour repérer la fraude.

7. ZOOM SUR LA SÉCURITÉ

Les attaques de whaling ciblent les e-mails des dirigeants, car ceux-ci contrôlent l'accès à d'importants virements bancaires.

8. ZOOM SUR LA SÉCURITÉ

Vérifier les changements de coordonnées de paiement en appelant un numéro de téléphone connu et enregistré est une défense clé contre la fraude au virement de type BEC.

9. ZOOM SUR LA SÉCURITÉ

Les faux sites de séquestre (escrow) sont une arnaque courante sur les places de marché en ligne : ils ressemblent à un service de paiement sûr mais volent le virement de l'acheteur.

10. APERÇU SÉCURITÉ

Google Safe Browsing avertit les utilisateurs avant qu'ils n'ouvrent des sites signalés pour hameçonnage ou logiciels malveillants.

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.). How To Spot, Avoid, and Report Tech Support Scams.

https://consumer.ftc.gov/articles/how-spot-avoid-and-report-tech-support-scams

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

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

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

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

[5] 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

Quel est le principal indice d'une arnaque au support technique ? → Une fenêtre surgissante affirmant que votre système est infecté et exigeant que vous appeliez un numéro de téléphone

2 Question 2

Bonne réponse : A

NOTE PÉDAGOGIQUE

Quelle technique utilise des domaines d'expéditeur usurpés pour voler des coordonnées bancaires ? → Hameçonnage par e-mail

3 Question 3

Bonne réponse : A

NOTE PÉDAGOGIQUE

Qu'est-ce qui correspond à une fraude au virement bancaire ? → Amener des victimes, par ingénierie sociale, à envoyer de l'argent sur de faux comptes d'entreprise

4 Question 4

Bonne réponse : A

NOTE PÉDAGOGIQUE

Pourquoi les escrocs créent-ils de faux sites marchands ? → Voler les données de carte de crédit et les identifiants de paiement des acheteurs

5 Question 5

Bonne réponse : A

NOTE PÉDAGOGIQUE

Que signifie le vishing ? → Escroqueries d'hameçonnage vocal par téléphone pour voler des identifiants

Corrigé : Point de contrôle 2 – Vrai ou faux

6 Question 6

Bonne réponse : Faux

NOTE PÉDAGOGIQUE

Faux : l'hameçonnage cible aussi les dirigeants ; le whaling est un hameçonnage visant les cadres supérieurs.

7 Question 7

Bonne réponse : Vrai

NOTE PÉDAGOGIQUE

Les domaines usurpés utilisent souvent de légères fautes de frappe (comme amaz0n.com) pour imiter des marques de confiance.

8 Question 8

Bonne réponse : Faux

NOTE PÉDAGOGIQUE

Faux : donner un accès à distance à un faux support technique lui permet d'installer des logiciels malveillants et de voler des données.

9 Question 9

Bonne réponse : Vrai

NOTE PÉDAGOGIQUE

L'ingénierie sociale exploite la psychologie humaine, comme la peur et l'urgence, pour contourner les règles de sécurité.

10 Question 10

Bonne réponse : Vrai

NOTE PÉDAGOGIQUE

Les demandes de virement doivent toujours être vérifiées par un canal de communication distinct (hors bande).

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

G 1. HAMEÇONNAGE	F 2. USURPÉ	D 3. HAMEÇONNAGE VOCAL (VISHING)	B 4. ARNAQUE
H 5. VÉRIFICATION	A 6. VIREMENT	E 7. WHALING	C 8. SMISHING

POINT DE CONTRÔLE 3 : CORRIGÉ DES TERMES CLÉS

1 HAMEÇONNAGE	2 USURPÉ	3 VISHING	4 ARNAQUE
5 VÉRIFICATION	6 VIREMENT		

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

1 B – USURPE	2 E – VERIFICATION	3 F – VIREMENT	4 H – SMISHING
5 G – WHALING	6 C – VISHING	7 A – HAMECONNAGE	8 D – ARNAQUE

NOTES DE DISCUSSION POUR LES ENSEIGNANTS

Termes clés :
Vérifiez que les élèves savent expliquer HAMEÇONNAGE, USURPÉ et HAMEÇONNAGE VOCAL (VISHING) 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.

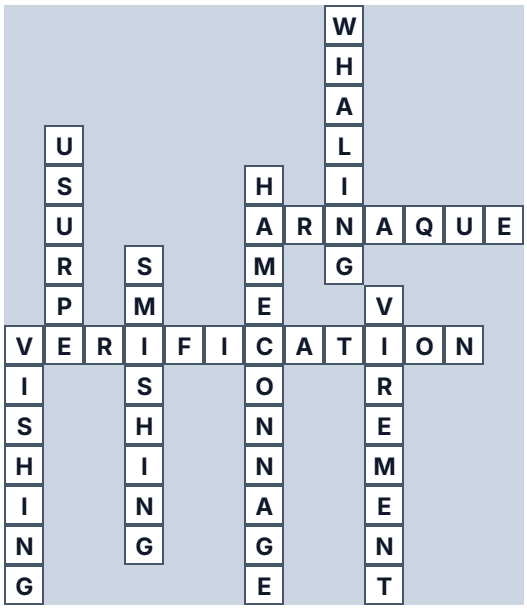
Évaluation des sources :
Faites vérifier au moins une affirmation à l'aide des sources de la fiche et discutez des raisons pour lesquelles les chiffres, les prix et les règles peuvent évoluer avec le temps.

Corrigés des jeux et notes pour l'enseignant

SOLUTION DES MOTS CACHÉS

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

SOLUTION DES MOTS CROISÉS



GUIDE DE L'ENSEIGNANT : SOLUTIONS DES MOTS CROISÉS

HORIZONTALEMENT

4 horizontal: ARNAQUE Stratagème frauduleux visant à soutirer de l'argent ou des identifiants aux victimes. (7 lettres)

7 horizontal: VERIFICATION Confirmation des informations de paiement par un moyen de contact secondaire de confiance. (12 lettres)

VERTICALEMENT

1 vertical: WHALING Attaques d'hameçonnage ciblées visant à voler les identifiants des hauts dirigeants. (7 lettres)

2 vertical: USURPE Se dit d'un expéditeur d'e-mail ou d'une adresse de site imités pour paraître légitimes. (6 lettres)

3 vertical: HAMECONNAGE Campagnes d'e-mails frauduleux visant à voler identifiants de connexion et mots de passe. (11 lettres)

5 vertical: SMISHING Envoi de SMS frauduleux pour voler les identifiants de comptes mobiles. (8 lettres)

6 vertical: VIREMENT Détournement frauduleux de transactions bancaires vers des comptes criminels. (8 lettres)

7 vertical: VISHING Appels vocaux frauduleux visant à voler des identifiants et des informations de compte. (7 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. CNGAONHAMEE — **HAMECONNAGE**
2. VSGNIHI — **VISHING**
3. VEACOTRINFII — **VERIFICATION**
4. GHILNWA — **WHALING**
5. RUEUPS — **USURPE**
6. UNQAAER — **ARNAQUE**
7. VTMENIER — **VIREMENT**
8. SMHGSNII — **SMISHING**

CORRIGÉ DU DÉFI DU CODE SECRET

"REPEREZ LE PHISHING GRACE A LA VERIFICATION"

Corrigé des études de cas

A Étude de cas 1 : Prévention des escroqueries au virement en entreprise

Corrigé de l'enseignant

CONSIGNE DE NOTATION

Les réponses des élèves doivent couvrir les points suivants :

- Analyse de scénario : un service financier reçoit un e-mail urgent provenant de l'adresse usurpée d'un fournisseur, demandant que les futurs virements de factures soient dirigés vers un nouveau numéro de compte bancaire.
- Stratégie et solution recommandées : imposez une politique de double autorisation pour tous les paiements. Mettez en place une vérification hors bande à l'aide d'un numéro de téléphone préenregistré et bloquez à la passerelle les e-mails provenant de domaines usurpés.

B Étude de cas 2 : Incident de whaling visant un dirigeant

Corrigé de l'enseignant

CONSIGNE DE NOTATION

Les réponses des élèves doivent couvrir les points suivants :

- Analyse de scénario : un dirigeant a cliqué sur un lien d'hameçonnage prétendant contenir un document sécurisé de conseil d'administration et a saisi ses identifiants professionnels principaux sur un portail usurpé.
- Stratégie et solution recommandées : isolez l'appareil du dirigeant. Réinitialisez tous les jetons de session et identifiants de l'entreprise. Examinez les journaux d'accès à la recherche de sorties de données et mettez en place une MFA matérielle sur toutes les connexions.