LIVRET DE JEUX

CYBER4GOOD

CYBER4GOOD, UNE NOUVELLE PHILOSOPHIE POUR LA CYBERSÉCURITÉ

CYBER4GOOD résulte d'une conviction : la cybersécurité est vitale pour que la société française d'aujourd'hui et de demain puisse bénéficier d'un monde numérique sûr et épanouissant. Elle mobilise tous les acteurs de l'écosystème autour du bien commun, en mettant notre culture Tech et notre passion pour l'innovation au service des grands enjeux actuels

La cybersécurité permet d'oeuvrer pour que chaque individu, entreprise et organisation puisse bénéficier pleinement des technologiques et des innovations offertes par le numérique.
Diverse et inclusive, elle concourt à l'émergence d'avenirs positifs.

Ce livret entre dans cette initiative. L'objectif : vous faire découvrir les différentes cyberattaques et comment vous en prémunir !

SOMMAIRE

GRILLE 1

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

Accès
Adresse
Avatar
Blog
Chat
Communication
Confidentialité
Connexion
Cryptage
Données
Envoi
Filtrer
Forum
Gestion
ligne
Messagerie
Navigateur
Partage
Pixel
Pixel
Recherche
Réseautage
Réseaux
Sécurité
Site
Souris
Streaming
Technologie
Téléchargement
Webcam

LE MOT CACHÉ EST : **SCAM**

QU'EST-CE QUE **LE SCAM**

Le SCAM est une forme d'escroquerie visant à tromper, manipuler ou piéger des individus dans le but de leur extorquer de l'argent, des informations personnelles ou d'autres biens de valeur. Les scams sont souvent réalisés par des escrocs qui utilisent diverses méthodes pour se donner une apparence de légitimité ou pour exploiter la crédulité des victimes.

ALORS COMMENT ÇA **FONCTIONNE ?**

Les escrocs ciblent des personnes vulnérables, crédules, ou qui pourraient être plus susceptibles de tomber dans le piège. Ils utilisent diverses sources d'informations, telles que les réseaux sociaux, les forums en ligne, les bases de données de clients piratées, ou simplement des listes de contacts volées pour trouver des cibles potentielles.

QUE PEUX-TU PERDRE EN ÉTANT VICTIME DE **SCAM** ?

Si tu es victime de SCAM tu peux perdre différents biens ou ressources en fonction du type d'arnaque et des informations qu'elles ont divulguées aux escrocs.
Voici quelques pertes courantes:

- **argent** : au travers de loteries, achats fictifs.
- **informations personnelles** : numéros de sécurité sociale , identifiants bancaires ...
- **Réputation**: en impliquant d'autres personnes de ton entourage à participer à l'arnaque

SCAM

BONNES PRATIQUES

- **Soyez vigilants face aux demandes d'argent** : méfiez-vous des demandes d'argent inattendues, en particulier si elles proviennent de personnes ou d'organisations que vous ne connaissez pas. Ne partagez jamais d'informations financières sensibles avec des personnes non vérifiées.

- **Vérifiez l'identité des contacts** : avant de partager des informations personnelles ou de répondre à des demandes, assurez-vous de vérifier l'identité de la personne ou de l'organisation en question. Ne cliquez pas sur des liens et ne rappelez pas des numéros de téléphone douteux.

- **Méfiez-vous des offres trop belles pour être vraies** : Si une offre semble trop alléchante, il est probablement trop risqué de poursuivre. Soyez sceptiques face aux promesses de gains rapides, de prix inattendus ou de remises importantes.

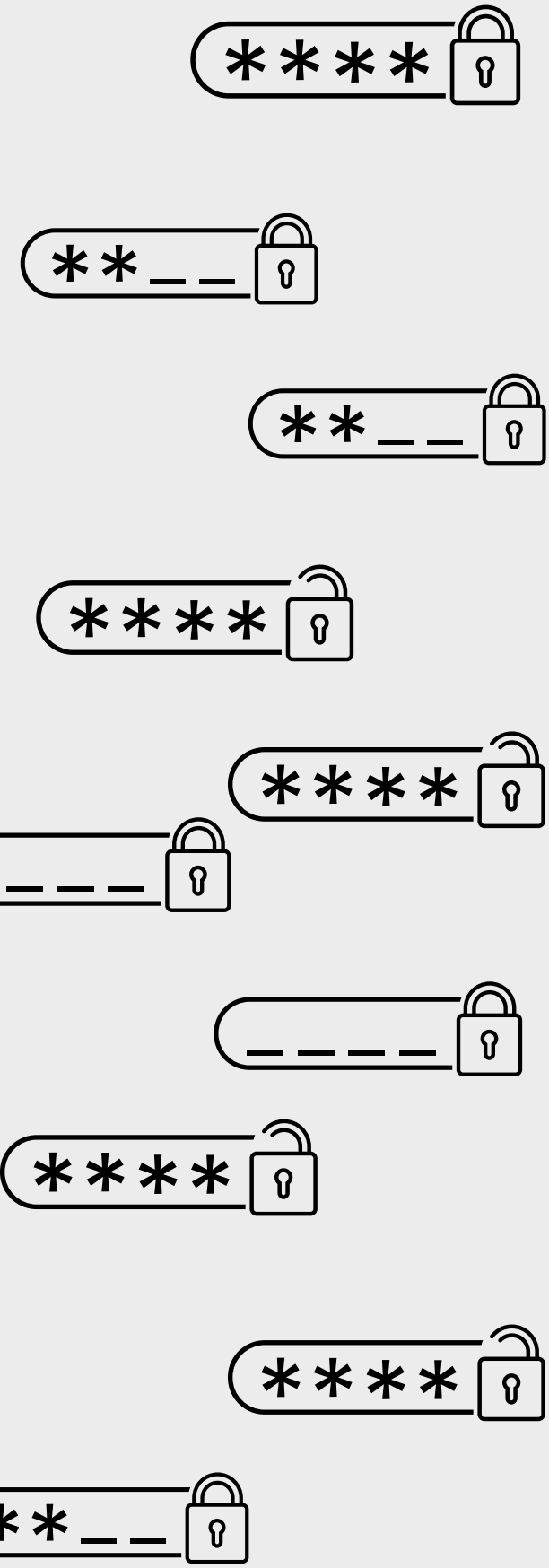
GRILLE 2

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

Animation
App
Avatar
Balayage
Batterie
Blog
Clé
Clic
Écran
Envoi
Forum
Interaction
Ligne
Logiciel
Mémoire
Messagerie
Modem
Navigateur
Numérique
Photo
Pixel
Puce
Recherche
Réseau
Robot
Scanner
Sécurité
Streaming
Système
Technologie
Télécommande
Téléviseur
Virus

__ __ __ __ __ __ __ __ __ __

LE MOT CACHÉ EST : **PASSPHRASE**



QU'EST-CE QU'UNE **PASSPHRASE ?**

Une passphrase est une forme de mot de passe utilisé pour renforcer la sécurité des comptes, des systèmes informatiques ou des données sensibles. Contrairement aux mots de passe traditionnels, qui sont généralement courts et constitués d'une combinaison de lettres, de chiffres et de symboles, une passphrase est composée d'une séquence de mots ou de caractères alphanumériques, formant une phrase ou une expression significative.

POURQUOI UTILISER UNE **PASSPHRASE** ?

Les passphrases sont généralement plus longues que les mots de passe traditionnels, ce qui les rend plus complexes et difficiles à deviner ou à craquer par les pirates.
Contrairement aux mots de passe simples, les passphrases incluent souvent des mots mémorables mais moins évidents, rendant les attaques de dictionnaire moins efficaces.
Les passphrases basées sur des mots significatifs peuvent être plus faciles à mémoriser que des mots de passe aléatoires, ce qui réduit le risque d'oublier votre mot de passe.

EXEMPLE DE **PASSPHRASE**

La phrase « **Je crée un mot de passe super sécurisé ! Plus de 12 caractères et 4 types différents !** » permet de créer le mot de passe « **Jcumdpss!Pd12ce4td!** »

PASSPHRASE

BONNES PRATIQUES

- **Optez pour une passphrase d'au moins16 caractères** : plus elle est longue, plus elle sera sécurisée.
- **Utilisez des mots significatifs** : Choisissez des mots mémorables, mais évitez d'utiliser des mots évidents, tels que "motdepasse" ou "abcdef".
- **Combinaison de mots** : Sélectionnez plusieurs mots distincts et non liés entre eux pour former votre passphrase. Vous pouvez utiliser des mots en français, en anglais ou dans une autre langue que vous maîtrisez.
- **Mélangez des chiffres et des caractères spéciaux** : par exemple, remplacez certaines lettres par des chiffres ou utilisez des caractères spéciaux tels que !, @, #, etc.
- **Ne pas utiliser des informations personnelles** : Évitez d'inclure des informations personnelles évidentes, comme votre nom, votre date de naissance, ou d'autres informations faciles à trouver.

pn

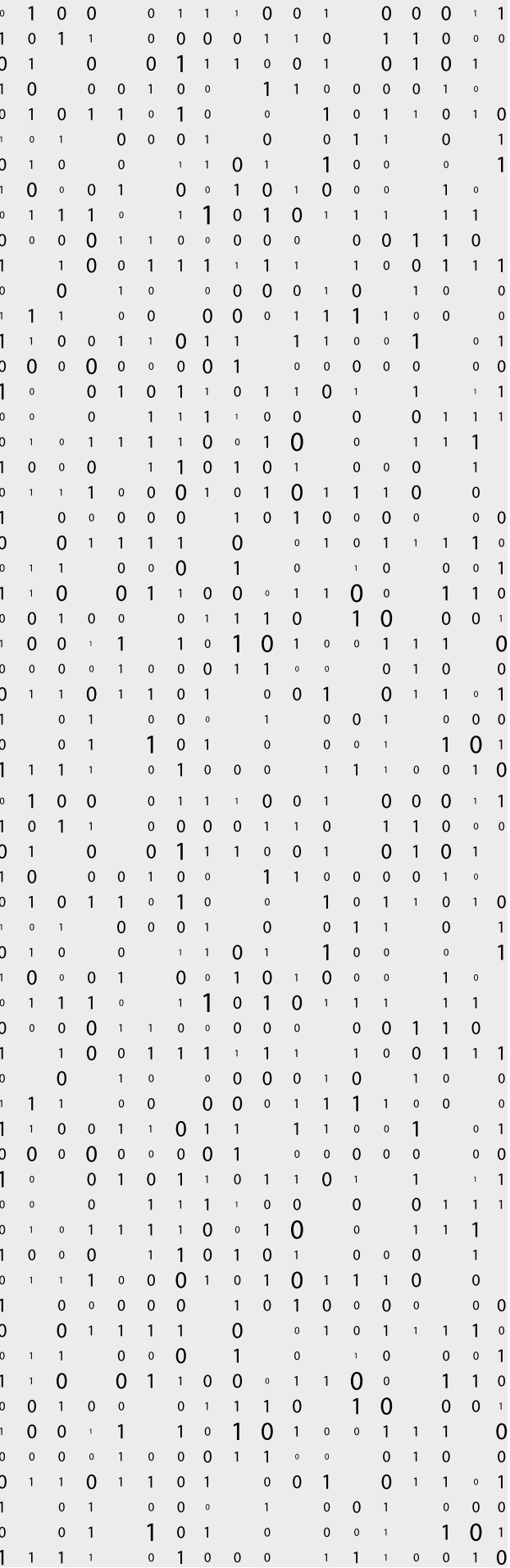
GRILLE 3

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

adresse
analyse
Animation
audio
Batterie
Blogueur
Cloud
Coller
Commentaire
Connecter
Copier
Envoi
Fichier
Format
Forum
Mémoire
Modem
Navigateur
Partager
Pixel
Puce
Rechercher
reseau
Sécurité
Site
Souris
Streaming
systeme
Système
Téléphone

_ _ _ _ _ _

LE MOT CACHÉ EST : **PIRATE**



QU'EST-CE QU'UN **PIRATE ?**

Un pirate est une personne qui s'engage dans des activités malveillantes sur les systèmes informatiques des particuliers, ou organisations. Les pirates sont également connus sous le nom de "hackers" et ont généralement des connaissances avancées en informatique qu'ils utilisent pour accéder à des informations, des données ou des systèmes auxquels ils n'ont pas légalement le droit d'accéder.

QUELS SONT LEURS **OBJECTIFS ?**

Les pirates ont pour objectif de voler des informations personnelles sensibles, de réaliser des escroqueries financières en ligne, d'utiliser des techniques pour obtenir des informations confidentielles, de cibler les comptes bancaires et d'effectuer des fraudes à l'assurance sociale. Ils peuvent également chercher à vous escroquer en se faisant passer pour des amis ou des partenaires potentiels.

COMMENT S'Y PRENNENT-ILS ?

Les pirates utilisent différentes méthodes pour accéder illégalement aux systèmes informatiques parmi lesquelles :

- La manipulation psychologique : pour convaincre les utilisateurs de divulguer des informations sensibles ou d'accorder un accès non autorisé à leurs systèmes
- Logiciels malveillants : Les pirates créent et distribuent des logiciels malveillants tels que les virus, les vers et les chevaux de Troie pour infecter les systèmes et voler des informations.

PIRATE

BONNES PRATIQUES

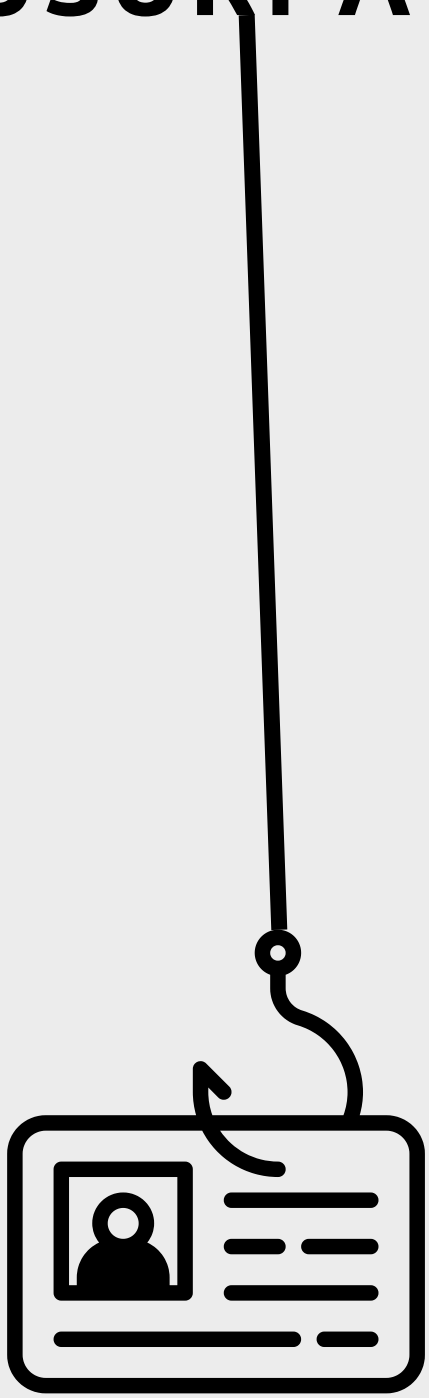
- **Mettez à jour régulièrement vos logiciels** : les mises à jour corrigent souvent les vulnérabilités connues.
- **Utilisez des mots de passe forts** : choisissez des mots de passe uniques, longs et complexes pour chaque compte en ligne.
- **Activez l'authentification à deux facteurs (2FA)** : lorsque cela est possible, activez l'authentification à deux facteurs pour vos comptes en ligne. Cela ajoute une couche de sécurité supplémentaire en demandant un second code de vérification lors de la connexion.
- **Soyez prudent avec les liens et les pièces jointes** : Méfiez-vous des liens et des pièces jointes provenant de sources inconnues ou suspectes, car ils pourraient contenir des logiciels malveillants. N'ouvrez pas de pièces jointes à moins d'être sûr de leur provenance.
- **Installez un logiciel antivirus** et antimalware sur votre ordinateur

GRILLE 4

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

activités
analyse
audit
conformité
digital
Données
Droits
exposition
générique
hackeur
incident
internet
intrusion
logiciel
menace
mesures
nuisible
numerique
Personnelles
port
programme
Risque
scam
Sécurité
Sous
virus
vulnerabilités

LE MOT CACHÉ EST : **USURPATION**



QU'EST-CE QUE **L'USURPATION ?**

L'usurpation mis pour **usurpation d'identité** également appelée vol d'identité, est une forme de fraude dans laquelle une personne se fait passer pour quelqu'un d'autre en utilisant ses informations personnelles, telles que son nom, son numéro de sécurité sociale, son numéro de carte de crédit ou d'autres données confidentielles.
L'objectif de l'usurpation d'identité est généralement de commettre des activités criminelles, financières ou frauduleuses au nom de la victime ; à utiliser sans votre accord, des informations permettant de vous identifier.

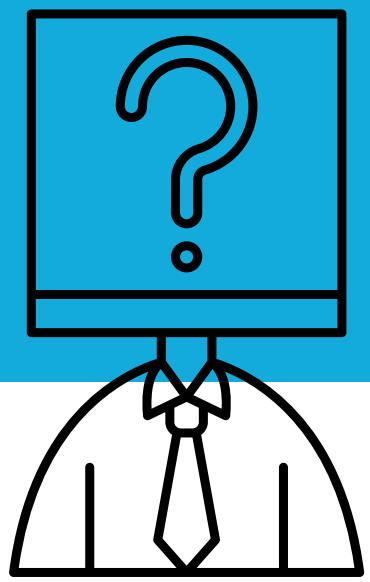
COMMENT ?

Les méthodes courantes utilisées par les usurpateurs d'identité comprennent le vol de portefeuille, le vol de courrier, le piratage informatique, le phishing (hameçonnage) et le vol de données provenant de sources non sécurisées. Une fois en possession des informations personnelles de la victime, l'usurpateur peut ouvrir des comptes bancaires, demander des prêts, effectuer des achats ou même commettre des crimes en utilisant l'identité de la victime.

QUELLES CONSÉQUENCES?

L'usurpation d'identité peut avoir des conséquences graves pour la victime telles que des problèmes financiers, des pertes de réputation et des problèmes juridiques.

USURPATION



BONNES PRATIQUES

- Choisissez un mot de passe complexe en alternant les majuscules et minuscules, les chiffres, etc.
- N'utilisez pas un mot de passe unique sur tous tes comptes, alternez-les en fonction des sites
- Ne partagez pas vos mots de passe
- Vérifiez bien l’expéditeur avant d’envoyer des informations par mail
- Évitez d'inscrire votre adresse mail principale sur des sites dont vous n’êtes pas certain de la fiabilité
- Soyez attentif à vos relevés de compte bancaire
- Détruisez tout papier comportant des informations personnelles avant de le jeter

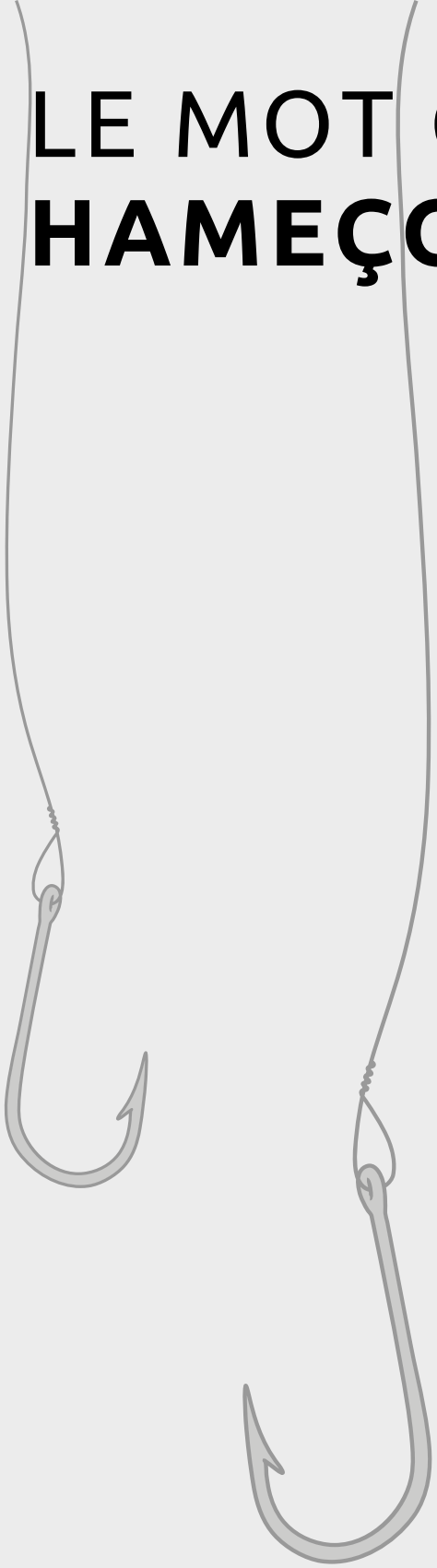
GRILLE 5

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

Anonymat
Attaque
Cyber
Cyberattaque
défense
documenter
Enquête
entrée
Escamotage
Escroc
Espionnage
Fraude
Fuite
guide
Hackeur
hôte
Identité
images
Infiltrer
Informations
mail
Navigateur
Risque
Sûreté
Victime
Violation
Virus

__ __ __ __ __ __ __ __ __ __ __

LE MOT CACHÉ EST : **HAMEÇONNAGE**



QU'EST-CE QUE **L'HAMEÇONNAGE**

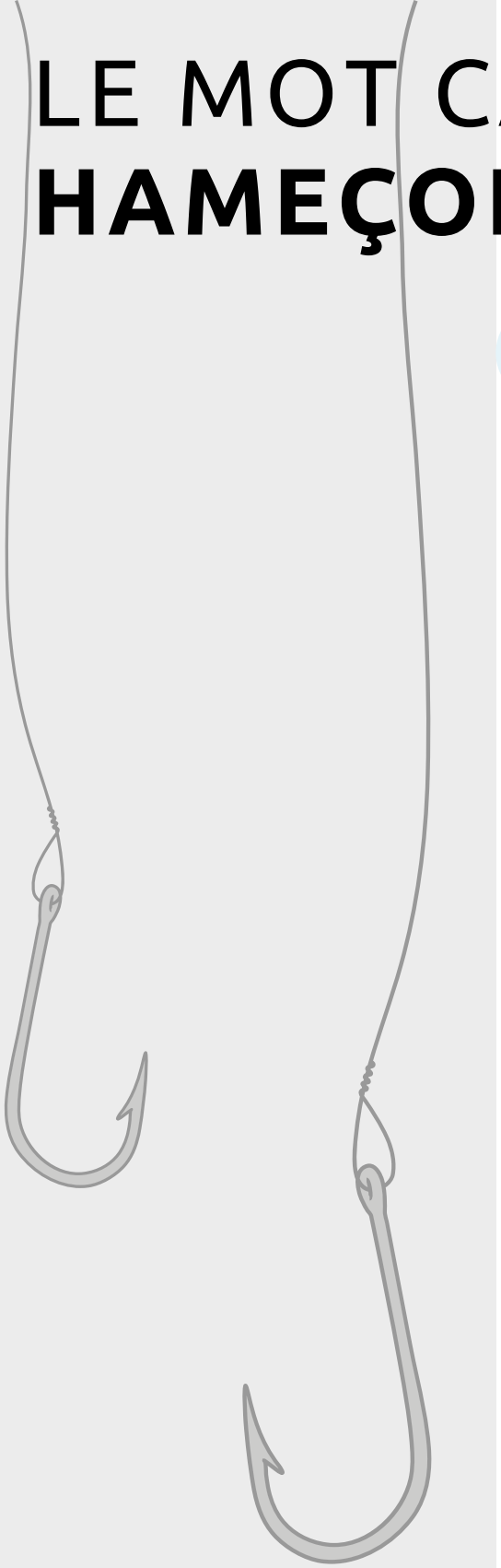
Le hameçonnage également connu sous le nom de "**phishing**" en anglais, est une technique d'escroquerie utilisée par des cybercriminels pour tromper les individus et les inciter à divulguer des informations personnelles sensibles, telles que des mots de passe, des numéros de carte de crédit, des numéros de sécurité sociale, etc. Cette technique repose sur la création de fausses communications qui semblent provenir d'entités légitimes, telles que des banques, des entreprises ou des organismes gouvernementaux.

ALORS COMMENT ÇA **FONCTIONNE ?**

Les cybercriminels envoient des e-mails ou des lettres postales informant les victimes qu'elle ont gagné un prix ou une loterie. Pour réclamer leur gain, elles doivent fournir leurs informations personnelles ou envoyer de l'argent pour couvrir les frais administratifs. En réalité, il n'y a pas de loterie ou de prix, et les fraudeurs cherchent simplement à escroquer de l'argent.

Ils peuvent aussi envoyer aux victimes des mails et des messages en se faisant passer pour un organisme de confiance tels que les impôts ou l'assurance maladie dans lesquels ils demandent généralement de cliquer urgemment sur un lien ou de télécharger une pièce jointe contenant des informations.

LE MOT CACHÉ EST : **HAMEÇONNAGE**



QU’EST-CE QU'IL SE PASSE SI VOUS CLIQUEZ SUR **LE LIEN OU TÉLÉCHARGER LA PIÈCE-JOINTE ?**

- Vous pourriez être redirigés vers un faux site ressemblant à un site légitime sur lequel il vous sera demandé de renseigner vos informations de connexion; ces dernières seront par la suite récupérées par les pirates à des fins malveillantes.
- Des logiciels malveillants pourraient être téléchargés et installés sur votre appareil sans votre consentement.
- Votre compte en ligne pourrait être compromis et utilisé pour des activités malveillantes.
- Vos fichiers et données pourraient être bloqués par un logiciel malveillant, exigeant une rançon pour les récupérer.
- Vous pourriez être victime d'usurpation d'identité ou de vol d'informations personnelles.
- Votre ordinateur, tablette ou téléphone pourrait être endommagé et vos données pourraient être supprimées.
- Vous pourriez devenir la cible de messages malveillants envoyés à vos contacts.
- Votre vie privée et votre sécurité en ligne pourraient être gravement compromises.

HAMEÇONNAGE

BONNES PRATIQUES

- **Soyez vigilants envers les e-mails** : Ne cliquez pas sur les liens et n'ouvrez pas les pièces jointes d'e-mails provenant d'expéditeurs inconnus ou suspects. Vérifiez également l'adresse e-mail de l'expéditeur pour vous assurer qu'elle est légitime.

- **Ne partagez pas d'informations sensibles** : Ne fournissez jamais de mots de passe, de numéros de carte de crédit, de numéros de sécurité sociale ou d'autres informations personnelles par e-mail ou par téléphone, à moins d'être sûr de l'identité de la personne avec laquelle vous communiquez.

- **Faites preuve de prudence avec les appels téléphoniques** : Ne donnez jamais d'informations personnelles à des personnes qui vous appellent de manière inattendue, surtout si elles prétendent être des représentants d'organisations officielles.

- **Lorsque vous recevez un lien par sms ou par mail** rendez-vous directement sur le site de l'organisme pour vérifier les informations demandées.

HAMEÇONNAGE

BONNES PRATIQUES

- **Méfiez-vous des liens suspects** : Ne cliquez pas sur les liens provenant d'emails, de messages ou de sites web suspects. Vérifiez toujours l'URL avant de cliquer, et si vous avez des doutes, accédez directement au site en saisissant l'adresse dans la barre d'URL du navigateur.

- **Vérifiez l'adresse email de l'expéditeur** : Soyez attentif à l'adresse email de l'expéditeur. Les cybercriminels utilisent souvent des adresses similaires à celles d'entreprises légitimes, mais avec de légères différences dans l'orthographe ou la structure.

- **Méfiez-vous des offres trop belles pour être vraies** : Soyez sceptique envers les offres ou les cadeaux gratuits qui vous sont proposés, car cela peut être une technique de hameçonnage pour vous attirer.

- **N'ayez pas peur de demander de l'aide** : Si vous avez des doutes concernant un e-mail, un appel téléphonique ou un site web, n'hésitez pas à demander l'avis d'un proche ou d'un ami avant de prendre des mesures.

GRILLE 6

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

Archives
Articles
Balise
Blog
Blogroll
Clic
Cloud
Connexion
Déconnexion
Domaine
Enregistrer
Forum
Galerie
Hacked
Hébergement
Héros
Hyperlien
Inscription
Liens
Ligne
Logo
Navigateur
Page
Piratage
Portfolio
Serveur
Site
Table
Texte
Web

__ __ __ __ __ __ __ __ __ __

LE MOT CACHÉ EST : **DÉFACEMENT**

QU'EST-CE QUE **LE DÉFACEMENT**

Le Défacement également appelé défiguration, est un acte malveillant qui consiste à altérer ou à modifier le contenu d'un site web sans l'autorisation du propriétaire .

ALORS COMMENT ÇA **FONCTIONNE ?**

Le pirate effectue une recherche pour identifier des failles de sécurité dans le site web . Une fois à l'intérieur du système, le pirate modifie son contenu ; cela peut consister à remplacer la page d'accueil par un message, à ajouter des images ou des vidéos, ou à modifier tout autre élément du site. Après avoir effectué les modifications, le pirate publie le défacement pour que les visiteurs du site web puissent le voir. Le défacement peut contenir des messages politiques, des revendications, des images choquantes, des fichiers téléchargeables, des liens ou d'autres contenus malveillants

QUELLES CONSÉQUENCES POURRAIENT AVOIR UN SITE DÉFIGURÉ SUR VOUS ?

Un site défiguré pourrait afficher de fausses informations ou des messages trompeurs, vous pourriez être induit en erreur ou prendre des décisions basées sur des informations incorrectes. Dans certains cas, le défacement peut être utilisé pour distribuer des logiciels malveillants aux visiteurs du site, ce qui peut entraîner des infections sur vos appareils.

DÉFACEMENT

BONNES PRATIQUES

- **Vérifiez l'URL** : Avant de cliquer sur un lien ou de saisir l'adresse d'un site web, assurez-vous de vérifier l'URL pour vous assurer qu'il correspond bien au site que vous souhaitez visiter. Méfiez-vous des URL étranges ou contenant des erreurs d'orthographe.

- **Utilisez des sites Web sécurisés** : Privilégiez les sites web qui utilisent le protocole HTTPS, car ils offrent une connexion sécurisée entre votre navigateur et internet.

- **Soyez conscients des signaux d'alerte** : Si un site web semble avoir un contenu étrange, ou s'il affiche des messages d'erreur inhabituels, quittez-le immédiatement.

- **Évitez de cliquer sur des liens raccourcis** (ex : bit.ly) qui masquent la véritable URL du site web.

- **Méfiez-vous des sites web** qui demandent des informations sensibles dès la page d'accueil.

GRILLE 7

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

Agresseur	Attentif	Bluetooth
Capgemini	Casque	Contexte
Culture	Cybersecurite	Dossier
Espace	Insultes	Manuscrite
Menaces	Mobilite	Mots
Options	Prevention	Provocations
Psychologique	Rapports	Taille
Tolerance	Troll	Victime
Webcam		

___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___

LE MOT CACHÉ EST : **CYBERHARCÈLEMENT**

QU'EST CE QUE LE **CYBERHARCÈLEMENT ?**

Le Cyberharcèlement est toute intimidation ou menace d'une personne au travers d'internet ou des réseaux sociaux. Cela peut inclure l'envoi de messages méchants, la diffusion de rumeurs blessantes, ou la création de faux profils pour harceler quelqu'un en ligne

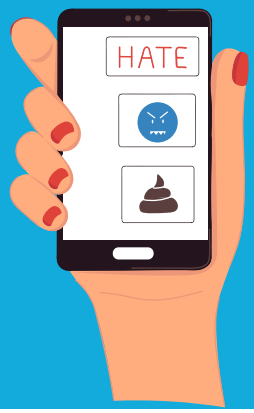
ALORS COMMENT ÇA **FONCTIONNE ?**

Le cyberharceleur identifie une personne comme cible potentielle. Cela peut se produire sur les réseaux sociaux, les forums en ligne, ou même par le biais d'e-mails non sollicités. Il peut créer de faux profils en utilisant des photos et des informations personnelles volées, pour se faire passer pour quelqu'un d'autre ou pour se cacher derrière l'anonymat. Le cyberharceleur peut propager de fausses informations ou des rumeurs blessantes sur la personne ciblée, dans le but de la discréditer ou de ternir sa réputation.

Dans certains cas, le cyberharceleur peut partager des photos ou des vidéos intimes ou humiliantes de la victime sans son consentement, cherchant à la ridiculiser ou à la déshonorer. Le cyberharceleur peut utiliser des tactiques de manipulation émotionnelle pour créer de la peur, de la détresse, de l'anxiété ou de la confusion chez la victime, l'amenant à se sentir vulnérable et isolée.

Le harcèlement peut impliquer plusieurs cyberharceleurs travaillant ensemble pour cibler la même personne, intensifiant ainsi la pression et les conséquences néfastes .

CYBERHARCÈLEMENT



BONNES PRATIQUES

- Configurer les paramètres de confidentialité sur les réseaux sociaux et autres plateformes en ligne pour contrôler qui peut vos informations .

- Soyez prudents lors de l'utilisation de sites de jeux en ligne et évitez de donner des informations personnelles pour jouer.

- Soyez prudents lors de l'utilisation de sites de rencontre en ligne et ne partagez pas d'informations personnelles trop rapidement.

- N'acceptez pas les demandes d'amitié ou de connexion de personnes inconnues sur les réseaux sociaux.

- Soyez prudents lors de la publication de photos ou d'informations personnelles sur les réseaux sociaux.

GRILLE 8

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

Aide
Aligné
Annuler
Coller
Colonnes
Copier
Couper
Document
Éditeur
Fenêtre
Fermer
Format
Gras
Guide
Image
Insertion
Italique
Justifié
Numéro
Outil
Ouvrir
Page
Paragraphe
Police
Souligné
Style
Tableau
Texte
Traitement
Zoom

LE MOT CACHÉ EST : **RANCONGIÇIEL**

QU'EST-CE QU'UN **RANÇONGICIEL ?**

Un rançongiciel est un programme malveillant dont le but est d'obtenir de la victime le paiement d'une rançon .

ALORS COMMENT ÇA **FONCTIONNE ?**

Lors d'une attaque par rançongiciel le pirate met l'ordinateur ou le système d'information de la victime hors d'état de fonctionner de manière réversible.
La machine peut être infectée après l'ouverture d'une pièce jointe, ou après avoir cliqué sur un lien malveillant reçu dans des courriels, ou parfois simplement en naviguant sur des sites compromis, ou encore suite à une intrusion sur le système. Dans la majorité des cas, les cybercriminels exploitent des vulnérabilités connues dans les logiciels, mais dont les correctifs n'ont pas été mis à jour par les victimes.

DANS QUEL **BUT ?**

L'objectif principal de ce type d'attaque est d'extorquer de l'argent à la victime en échange de la promesse (pas toujours tenue) de retrouver l'accès aux données corrompues. Certaines attaques visent parfois simplement à endommager le système de la victime pour lui faire subir des pertes d'exploitation et porter atteinte à son image.

RANÇONGICIEL

BONNES PRATIQUES

- Appliquez de manière régulière et systématique vos mises à jour.
- Utilisez des connexions Wi-Fi sécurisées que vous connaissez et évitez les réseaux Wi-Fi publics (Gares , centre commerciaux ...)
- Fais régulièrement des sauvegardes .
- Évitez de télécharger des applications ou des logiciels à partir de sources inconnues.
- Éteignez vos ordinateurs lorsque vous ne vous en servez pas.
- N'ouvrez pas les pièces jointes de courriels qui semblent suspects, même s'ils proviennent d'expéditeurs connus.
- Ne partagez jamais vos informations de connexion

pn

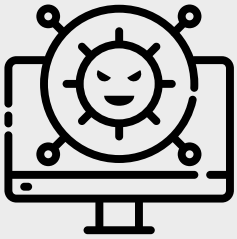
GRILLE 9

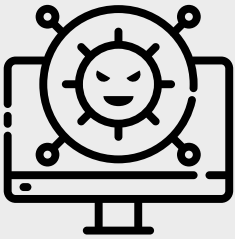
M A C R E G A T R A P L W A N
R L T É L É T R A V A I L E G
É A U T O M A T I Q U E I A I
I N T E R A C T I O N K D R S
É T I L A É R P R I V É E R E
P U B L I Q U E M E M Y G Ê D
I P W F E A L O C A P A A T Y
X T K E E H T T R R N U G E M
E G O S B S P R A A A N O R E
L I É B Y M E A L C A N B C D
O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

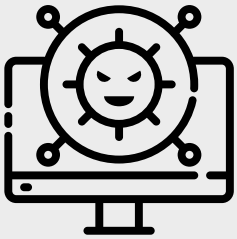
Analyse
Apprentissage
Arrêter
Automatique
Clé
Cloud
Couper
Débogage
Démarrer
Design
Ecran
Ecran
Interaction
Lien
Modem
Mots
Outil
Panne
Partager
Pixel
Privée
publique
Réalité
Réseau
Robot
Supervision
Tactile
Télétravail
Webmaster

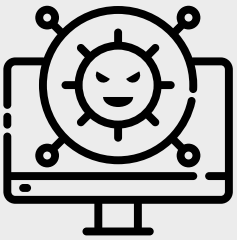
__ __ __ __ __ __ __

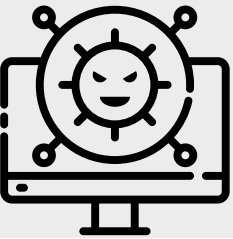
LE MOT CACHÉ EST : **MALWARE**











QU'EST-CE QU'UN **MALWARE ?**

Un Malware également connu sous le nom de logiciel malveillant, est un type de logiciel développé dans le but de nuire à un système informatique, voler des données, ou causer des dommages à un utilisateur ou à une organisation.

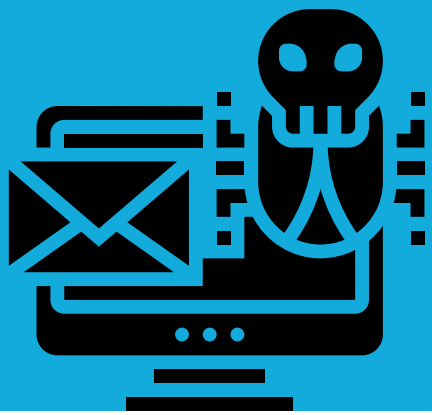
ALORS COMMENT ÇA **FONCTIONNE ?**

Les pirates utilisent différentes méthodes pour distribuer les malwares aux victimes potentielles. Cela peut inclure l'envoi d'e-mails de phishing avec des liens ou des pièces jointes infectés, la diffusion de publicités malveillantes sur des sites web, ou l'injection de code malveillant dans des sites web défigurés.
Lorsque la victime clique sur un lien malveillant, télécharge un fichier infecté ou interagit avec du contenu malveillant, le malware est activé et infecte son appareil .

DANS QUEL **BUT ?**

Certains malwares sont conçus pour surveiller discrètement les activités de l'utilisateur, en enregistrant les frappes au clavier, en prenant des captures d'écran, en activant la webcam ou en capturant des informations sur la navigation en ligne. Les données collectées peuvent être utilisées à des fins d'espionnage ou de chantage.

MALWARE



BONNES PRATIQUES

- **Méfiez-vous des clés USB inconnues** : N'insère pas de périphériques inconnus dans ton ordinateur.

- **Évitez les sources non fiables** : Ne téléchargez pas de logiciels, d'applications ou de fichiers depuis des sources non fiables. Privilégiez les téléchargements depuis les sites officiels et les boutiques d'applications reconnues.

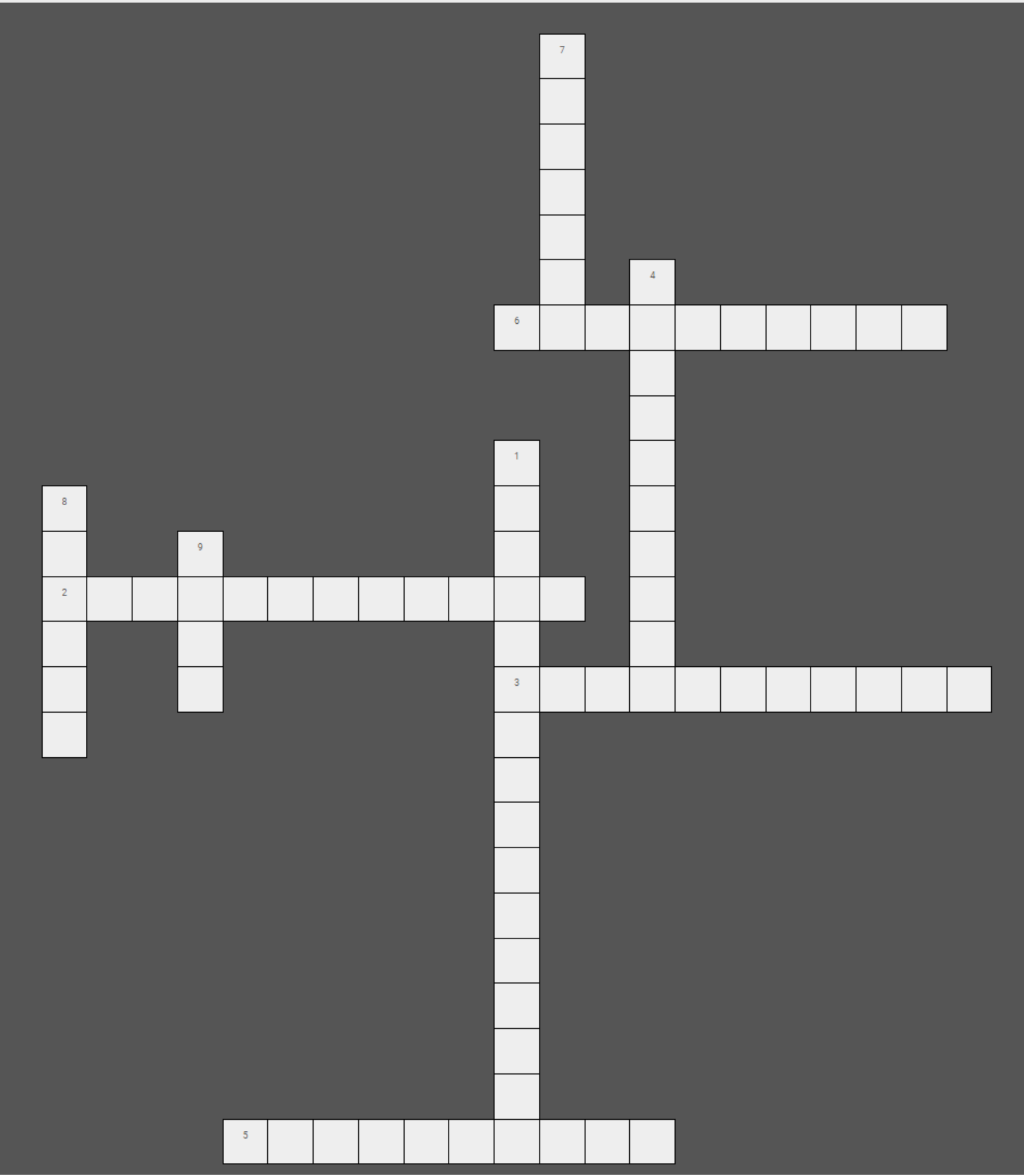
- **Évitez de laisser votre ordinateur ou vos appareils mobiles sans surveillance** dans des lieux publics.

- **Consultez des sources d'informations fiables** pour vous renseigner sur les dernières menaces de sécurité et les meilleures pratiques pour les éviter.

- **Ne téléchargez pas de fichiers ou de logiciels** à partir de liens partagés sur des forums ou des réseaux sociaux.

pn

TESTEZ VOS CONNAISSANCES



TESTEZ VOS CONNAISSANCES

VERTICAL

1. intimidation en ligne

4. forme de mot de passe utilisé pour renforcer la sécurité des comptes, des systèmes informatiques ou des données sensibles.

7. logiciel développé dans le but de nuire à un système informatique

8. personne qui s'engage dans des activités malveillantes sur les systèmes informatiques des particuliers, ou organisations.

9. forme d'escroquerie visant à tromper, manipuler ou piéger des individus dans le but de leur extorquer de l'argent, des informations personnelles ou d'autres biens de valeur

HORIZONTAL

2. programme malveillant dont le but est d'obtenir de la victime le paiement d'une rançon

3. technique d'escroquerie utilisée par des cybercriminels pour tromper les individus et les inciter à divulguer des informations personnelles sensibles

5. forme de fraude dans laquelle une personne se fait passer pour quelqu'un d'autre en utilisant ses informations personnelles

6. acte malveillant qui consiste à altérer ou à modifier le contenu d'un site web sans l'autorisation du propriétaire du site.

NUMÉROS D'AIDE

VOUS SOUHAITEZ SIGNALER UNE ESCROQUERIE EN LIGNE OU UN CONTENU ILLICITE SUR INTERNET ?

WWW.INTERNET-SIGNALEMENT.GOUV.FR

VOUS SOUHAITEZ DÉPOSER PLAINTE ?

RENDEZ-VOUS AU COMMISSARIAT DE POLICE OU À LA BRIGADE DE GENDARMERIE, OU ADRESSEZ NE PLAINTE PAR ÉCRIT AU PROCUREUR DE LA RÉPUBLIQUE DU TRIBUNALA JUDIFICAIRE DE VOTRE DOMICILE.

SI VOUS ÊTES UN PARTICULIER VICTIME D'UNE CYBERMALVEILLANCE À CARACTÈRE FINANCIER (CHANTAGE, SEXTORSION, ESCROQUERIE COMMERCIALE OU SENTIMENTALE, PIRATAGE DE MESSAGERIE OU RÉSEAUX SOCIAUX...), VOUS POUVEZ DÉPOSER PLAINTE EN LIGNE SUR LA PLATEFORME **THESEE** DU MINISTÈRE DE L'INTÉRIEUR.

WWW.SERVICE-PUBLIC.FR

SI VOUS ÊTES UN PARTICULIER, VOUS POUVEZ ÊTRE ACCOMPAGNÉ GRATUITEMENT DANS VOTRE DÉPÔT DE PLAINTE PAR L'ASSOCIATION FRANCE VICTIMES QUI OPÈRE LE NUMÉRO D'AIDE AUX VICTIMES DU MINISTÈRE DE LA JUSTICE : **116 006** (APPEL ET SERVICE GRATUITS, OUVERT 7 JOURS SUR 7 DE 9H À 19H).

WWW.FRANCE-VICTIMES.FR

CONTACTEZ-NOUS

cyber4good@capgemini.com

WWW.CAPGEMINI.COM