VOCABULAIRE DE LA SÉCURITÉ INFORMATIQUE

Au cours des dernières années, le virage numérique de même que l'essor du télétravail et de l'infonuagique ont mis au premier plan la question de la sécurité informatique.

Afin de faciliter la compréhension de ce domaine d'actualité, l'Office québécois de la langue française propose un vocabulaire comportant près de 200 définitions, comme celles de *vulnérabilité logicielle*, d'*installation furtive*, d'*attaque par embuscade*, d'*enregistrement de frappe* et de *prime de bogues*.

Réalisé avec la collaboration d'experts de l'institut Cogentas, du Secrétariat du Conseil du trésor ainsi que du Département d'informatique du cégep de Sainte-Foy, le présent *Vocabulaire de la sécurité informatique* est destiné à quiconque souhaite nommer avec justesse les concepts associés aux cyberattaques, aux vulnérabilités ainsi qu'aux moyens existants pour se protéger.

Symboles

Termes privilégiés

Termes utilisés dans certains contextes

Termes déconseillés

Ce vocabulaire est accessible en ligne à l'adresse suivante :
oqlf.gouv.qc.ca/ressources/bibliotheque/dictionnaires/vocabulaire-securite-informatique.aspx.

Version PDF du 24 février 2025

Avertissement : Lors de la conversion du format HTML au format PDF, il est possible que certains caractères spéciaux ou signes typographiques (comme les espaces insécables) n'aient pas été correctement conservés. En cas de disparité, c'est la version en ligne du vocabulaire qui prévaut.

VOCABULAIRE DE LA SÉCURITÉ INFORMATIQUE

Index

Index

1. activité virale

Définition
Comportement anormal d'un système informatique causé par la présence d'un virus informatique.

Notes
Une activité virale, bien que détectable par l'utilisateur, est le plus souvent repérée par un logiciel antivirus ou un logiciel de détection de virus.

Il arrive qu'une requête d'écriture suspecte dans le secteur d'amorçage puisse être perçue comme une activité virale par un logiciel antivirus, sans qu'il s'agisse nécessairement d'un virus informatique.

activité virale n. f.

anglais
virus activity
computer virus activity
viral activity

---

2. algorithme à clé publique

Définition
Algorithme de chiffrement pour lequel deux clés différentes sont nécessaires, soit une clé privée et une clé publique.

Notes
Un algorithme à clé publique est une fonction cryptographique dont la clé de chiffrement est différente de la clé de déchiffrement.

Lorsque la clé servant au chiffrement d'un message est la clé publique, seul le propriétaire de la clé de déchiffrement correspondante (clé privée) peut le déchiffrer.

algorithme à clé publique n. m.
algorithme asymétrique n. m.

L'emploi de la graphie *clef* est en régression. De ce fait, les termes construits avec *clef* sont beaucoup moins répandus en cryptographie que ceux construits avec *clé*.

anglais
public key algorithm
asymmetric algorithm
public key cryptographic algorithm
asymmetric cryptographic algorithm
public key encryption algorithm
asymmetric encryption algorithm

---

3. algorithme à clé secrète

Définition
Algorithme de chiffrement pour lequel le chiffrement et le déchiffrement se font à partir d'une même clé cryptographique.

Notes
Avec les algorithmes à clé secrète, l'expéditeur et le destinataire d'un message partagent une même clé secrète, leur permettant à la fois de le chiffrer et de le déchiffrer.

algorithme à clé secrète n. m.
algorithme à clé symétrique n. m.
algorithme symétrique n. m.

L'emploi de la graphie *clef* est en régression. De ce fait, les termes construits avec *clef* sont beaucoup moins répandus en cryptographie que ceux construits avec *clé*.

anglais
secret key algorithm
symmetric key algorithm
secret key cryptographic algorithm
symmetric algorithm

---

4. algorithme de chiffrement

Définition
Algorithme basé sur l'association entre une fonction mathématique et une clé de chiffrement, dont la séquence d'opérations conduit au chiffrement ou au déchiffrement de données.

Notes
Les algorithmes de chiffrement peuvent par exemple être utilisés afin de garantir l'intégrité des données, de confirmer l'identité d'un expéditeur ou d'assurer la confidentialité des éléments d'information transmis.

algorithme de chiffrement n. m.
algorithme de cryptage n. m.
algorithme cryptographique n. m.

Bien que l'utilisation de *cryptage* ait parfois été critiquée pour désigner le chiffrement, on constate que ce terme et ses dérivés tendent à se généraliser dans la documentation spécialisée.

anglais
cryptographic algorithm
crypto-algorithm
encryption algorithm
ciphering algorithm
encipherment algorithm

---

5. algorithme de hachage

Définition
Fonction mathématique qui permet la création d'une empreinte numérique en transformant un groupe de données de taille variable en un code unique de taille fixe.

algorithme de hachage n. m.

anglais
hash algorithm
hashing algorithm

6. analyse de sécurité informatique

Définition
Examen exhaustif des risques informatiques, des mesures de sécurité existantes et des nouveaux moyens à mettre en place à l'intérieur d'une organisation compte tenu de sa politique de sécurité informatique et des contraintes auxquelles elle est assujettie.

Notes
Lors d'une analyse de sécurité informatique, les contraintes de nature technique, juridique, humaine, administrative, financière ou même géographique d'une organisation doivent être prises en compte.

analyse de sécurité informatique n. f.
analyse de sécurité n. f.

anglais
computer security analysis
computer system security analysis
security analysis

---

7. analyse des risques informatiques

Définition
Étape de l'analyse de sécurité informatique qui consiste à établir les risques auxquels est exposé l'actif informationnel d'une organisation, à les quantifier et à en évaluer l'importance relative.

Notes
L'analyse des risques informatiques peut survenir lors de la planification d'un projet, avant même la création du système informatique et l'existence d'un actif informationnel. Elle est généralement suivie de l'étape de la maîtrise des risques informatiques.

analyse des risques informatiques n. f.
analyse de risques informatiques n. f.
étude des risques informatiques n. f.

anglais
computer risk analysis
IT risk analysis
risk assessment
risk analysis

---

8. anti-logiciel espion

Définition
Logiciel servant à détecter et à éliminer les logiciels espions.

Notes
Les anti-logiciels espions, les logiciels antivirus et les pare-feu font généralement partie des solutions informatiques de sécurité.

anti-logiciel espion n. m.
antiespiogiciel n. m.
logiciel antiespion n. m.

Les mots formés avec le préfixe *anti-* s'écrivent généralement en un seul mot, sans trait d'union. Cependant, on met un trait d'union quand *anti-* est suivi d'un nom composé. Voir, à ce sujet, l'article *Trait d'union ou soudure avec l'élément* anti- de la *Banque de dépannage linguistique*.

Au pluriel, on écrira : *des anti-logiciels espions*. Le deuxième élément (*espions*) du terme complexe prend la marque du pluriel parce qu'il est en apport de qualification avec le premier. Voir, à ce sujet, l'article *Règle générale du pluriel et du trait d'union pour le nom complément du nom* de la *Banque de dépannage linguistique*.

anglais

anti-spyware
antispyware
anti-spyware software
antispyware software
anti-spyware program
antispyware program

---

9. anti-logiciel malveillant

Définition

Logiciel de sécurité informatique dont le but est de détecter les logiciels malveillants afin de bloquer leurs actions malintentionnées et de les supprimer d'un système infecté.

anti-logiciel malveillant n. m.
anti-programme malveillant n. m.
antimaliciel n. m.

Les mots formés avec le préfixe *anti-* s'écrivent généralement en un seul mot, sans trait d'union. Cependant, on met un trait d'union quand *anti-* est suivi d'un nom composé. Voir, à ce sujet, l'article *Trait d'union ou soudure avec l'élément* anti- de la *Banque de dépannage linguistique*.

anglais

antimalware
antimalicious software
antimalicious program

---

10. attaque par bourrage d'identifiants

Définition

Cyberattaque qui consiste à accéder de manière frauduleuse à un compte utilisateur d'une application Web à la suite de tentatives de connexion automatisées à partir d'une liste de données d'accès, généralement volée auprès d'une autre application Web.

Notes

Ce type de cyberattaque repose sur la présomption qu'un grand nombre d'utilisateurs et d'utilisatrices emploient les mêmes identifiants et authentifiants pour plusieurs applications Web.

attaque par bourrage d'identifiants n. f.

anglais

credential stuffing attack

---

11. attaque par déni de service

Définition

Cyberattaque qui consiste à submerger de requêtes le système informatique d'une organisation afin de le rendre inopérant et d'en bloquer l'accès aux utilisateurs légitimes.

attaque par déni de service n. f.
recommandé par l'OQLF
attaque par saturation n. f.
attaque par refus de service n. f. rare

anglais

denial of service attack
DoS attack
saturation attack

---

12. attaque par déni de service distribué

Définition

Attaque par déni de service dont les requêtes proviennent simultanément de multiples ordinateurs.

Notes

Une attaque par déni de service distribué est souvent menée au moyen d'ordinateurs zombies.

attaque par déni de service distribué n. f.

attaque par DDoS

Le sigle *DDoS*, abréviation du terme anglais *distributed denial of service*, en usage depuis peu de temps, est déconseillé parce qu'il ne s'intègre pas au système linguistique du français.

anglais

distributed denial of service attack
DDoS attack
distributed denial of service
DDoS

---

13. attaque par embuscade

Définition

Cyberattaque qui vise à compromettre de manière indirecte les ressources informatiques d'une organisation en piégeant un site Web légitime fréquemment consulté par ses membres afin d'en infecter le plus grand nombre.

attaque par embuscade n. f. recommandé par l'OQLF

Le terme *attaque par embuscade* a été proposé par l'Office québécois de la langue française en décembre 2020 pour désigner ce concept.

attaque de point d'eau

Le terme *attaque de point d'eau*, calqué sur l'anglais *watering hole attack*, est déconseillé. Ce terme fait allusion aux attaques embusquées réalisées par les prédateurs au détriment des animaux venus s'abreuver dans un point d'eau. Dans cette analogie, le point d'eau représente les sites Web fréquemment consultés qui sont piratés. Or, le terme *attaque de point d'eau* donne à penser que le piratage de ces sites constitue une fin en soi alors qu'il constitue plutôt le tremplin permettant de perpétrer la véritable cyberattaque.

anglais

watering hole attack
watering hole

---

14. attaque par épuisement de ressources

Définition

Attaque par déni de service qui consiste à consommer l'entièreté de la puissance de calcul des processeurs, à occuper tout l'espace disque ou mémoire d'un système informatique afin de le rendre inutilisable.

attaque par épuisement de ressources n. f.
attaque par épuisement des ressources n. f.
épuisement de ressources n. m.
épuisement des ressources n. m.

anglais

resource exhaustion attack
resource exhaustion
exhaustion attack

---

15. attaque par force brute

Définition

Cyberattaque qui consiste à trouver un mot de passe ou une clé cryptographique en essayant systématiquement et successivement toutes les combinaisons possibles.

attaque par force brute n. f.
attaque en force n. f.

anglais

brute force attack
brute-force attack

16. attaque par injection SQL

Définition

Cyberattaque qui consiste à saisir une requête en SQL dans un champ de saisie afin de communiquer directement avec le serveur et d'accéder frauduleusement à l'information contenue dans les bases de données du site Web.

Notes

Dans les cas où une base de données ne serait pas protégée contre ce type d'attaque, il serait par exemple possible pour un pirate informatique d'entrer un nom d'utilisateur dans le champ de saisie correspondant, et, dans le champ de saisie du mot de passe, d'inscrire une requête en langage SQL demandant au serveur de lui retourner le mot de passe associé à ce même utilisateur.

attaque par injection SQL n. f.
recommandé par l'OQLF
injection SQL n. f.
iSQL n. f. rare
attaque par injection de commandes SQL n. f.

anglais

SQL injection attack
SQL injection
SQLi

---

17. attaque par interception

Définition

Cyberattaque au cours de laquelle une personne intercepte les communications entre deux parties, notamment à l'aide d'une clé cryptographique obtenue frauduleusement, ce qui lui permet de se faire passer pour l'une des parties, ou les deux, ou encore de récupérer de l'information sensible.

attaque par interception n. f.
recommandé par l'OQLF
attaque par interposition n. f.
attaque de l'intercepteur n. f.

attaque de l'homme du milieu n. f.

Le terme *attaque de l'homme du milieu* est calqué sur l'anglais *man-in-the-middle attack,* expression issue du domaine du sport. Bien que cet emprunt soit présent dans les ouvrages spécialisés en sécurité informatique, il reste inusité et l'image véhiculée est peu compréhensible en français.

anglais

man-in-the-middle attack
MitMA
MitM attack
MitM
MiM attack
bucket brigade attack

---

18. attaque par usurpation d'adresse IP

Définition
Cyberattaque par laquelle une personne recourt à l'usurpation d'adresse IP afin d'accéder frauduleusement à un réseau informatique ou de dissimuler son identité.

attaque par usurpation d'adresse IP n. f.
recommandé par l'OQLF

anglais
IP spoofing attack

---

19. attribut biométrique

Définition
Caractéristique physique ou trait comportemental que l'on peut mesurer et analyser pour déterminer ou prouver l'identité des personnes.

Notes
Les empreintes digitales ou la structure de l'iris, par exemple, sont associées à la biométrie morphologique. L'analyse de la démarche d'une personne ou de sa vitesse de frappe sur un clavier relève, quant à elle, de la biométrie comportementale.

attribut biométrique n. m.
modalité biométrique n. f.

anglais
biometric modality
biometric attribute

---

20. audit de sécurité informatique

Définition
Audit des moyens mis en œuvre afin d'assurer la sécurité informatique dans une organisation, qui permet de déterminer le niveau de sécurité global de son système d'information.

Notes
L'audit de sécurité informatique permet de passer en revue toutes les activités informatiques afin de produire une analyse indépendante de l'efficacité et de la qualité des mesures de sécurité informatiques mises en place.

audit de sécurité informatique n. m.
audit de sécurité n. m.
audit sécurité n. m.

anglais
information security audit
ISA
security audit

---

21. audit informatique

Définition
Audit visant à établir et à analyser les risques associés aux activités informatiques d'une organisation.

audit informatique n. m.
audit des systèmes d'information n. m.

anglais
information system audit
IS audit
information technology audit
IT audit

---

22. authentifiant

Définition
Information fournie par une entité, au cours d'une procédure d'authentification, afin de démontrer qu'elle est bien la propriétaire légitime de l'identifiant présenté.

Notes
Les authentifiants sont souvent divisés en trois grandes catégories : « ce que je sais » (un mot de passe, un numéro d'identification personnel, une réponse à une question de sécurité), « ce que je suis » (une donnée biométrique comme une empreinte digitale) et « ce que je possède » (un jeton d'authentification, par exemple).

authentifiant n. m.
donnée d'authentification n. f.

anglais
authenticator
authentication information
authentication data

---

23. authentification

Définition
Procédure de contrôle consistant à vérifier et à valider l'identité d'une entité qui fait une demande d'accès à un réseau, à un système informatique ou à un logiciel.

Notes
Une entité peut être, par exemple, une personne, une organisation, un autre système informatique ou un appareil.

L'authentification fait généralement suite à l'étape d'identification. Pour une personne, l'authentification consiste le plus souvent à fournir une information qu'elle seule connaît (mot de passe, réponse à une question de sécurité, etc.) ou à utiliser un dispositif qu'elle seule possède (carte à puce, jeton, etc.).

authentification n. f.

anglais

authentication

---

24. authentification à deux facteurs

Définition

Authentification par laquelle l'utilisateur doit fournir deux éléments appartenant à deux facteurs d'authentification distincts.

Notes

Généralement, l'authentification à deux facteurs constitue une méthode d'authentification forte.

authentification à deux facteurs n. f.
A2F n. f.
authentification à double facteur n. f.
A2F n. f.

anglais

two-factor authentication
2FA

---

25. authentification biométrique

Définition

Authentification d'une personne par la captation d'une donnée biométrique.

Notes

Il peut s'agir par exemple d'authentifier une personne par l'analyse de ses empreintes digitales, de la physionomie de son visage, de sa voix ou de sa démarche.

Il arrive que l'identification biométrique et l'authentification biométrique se confondent parfois : une personne décline son identité en présentant un caractère biométrique qui lui est unique, et donc qui l'authentifie en même temps qu'il l'identifie.

authentification biométrique n. f.

anglais

biometric authentication

---

26. authentification forte

Définition

Authentification dont les procédés de vérification permettent d'authentifier l'identité des personnes ou des systèmes avec un niveau de fiabilité très élevé.

Notes
Souvent, l'authentification forte fait appel à plusieurs facteurs d'authentification. On parle alors d'authentification multifacteur.

Parmi les principaux facteurs d'authentification, on trouve : « ce que l'on sait » (par exemple, un mot de passe), « ce que l'on possède » (par exemple, un appareil mobile) et « ce que l'on est » (par exemple, une empreinte digitale).

authentification forte n. f.

anglais
strong authentication

---

27. authentification multifacteur

Définition
Authentification qui met en œuvre, de façon concomitante, des procédés de vérification faisant appel à au moins deux facteurs d'authentification différents.

Notes
Généralement, l'authentification multifacteur constitue une méthode d'authentification forte.

Parmi les principaux facteurs d'authentification, on trouve : « ce que l'on sait » (par exemple, un mot de passe), « ce que l'on possède » (par exemple, un appareil mobile), « ce que l'on est » (par exemple, une empreinte digitale).

authentification multifacteur n. f.
authentification multifactorielle n. f.
AMF n. f.

Au pluriel, on écrira : *des authentifications multifacteurs*, *des authentifications multifactorielles*.

anglais
multi-factor authentication
multifactorial authentication
MFA

---

28. autorité d'horodatage

Définition
Entité prestataire d'un service consistant à attribuer une marque temporelle précise à un document, à une donnée ou à une intervention, selon un protocole reconnu.

autorité d'horodatage n. f.

anglais
timestamping authority
TSA

29. balayage de ports

Définition
Technique consistant à vérifier automatiquement, à l'aide d'un balayeur de ports, une série d'adresses IP spécifiques afin de trouver les ports ouverts sur un ou plusieurs ordinateurs cibles accessibles via un réseau local ou Internet.

Notes
Le balayage de ports est utilisé autant par les administrateurs de système, afin de repérer les vulnérabilités informatiques pour éventuellement les corriger, que par les pirates informatiques, afin d'exploiter les ports ouverts pour une éventuelle intrusion informatique.

balayage de ports n. m.

scannage de ports

Le terme *scannage de ports* est déconseillé parce qu'il ne s'inscrit pas dans la norme sociolinguistique du français au Québec. En outre, l'élément *scannage*, emprunté à l'anglais, ne s'intègre pas au système linguistique du français.

anglais
port scanning
port scan

---

30. balayeur de ports

Définition
Programme qui tente de se connecter successivement à tous les ports d'un ou de plusieurs ordinateurs cibles afin de dresser une liste des ports ouverts ou des services actifs, et qui est utilisé à la fois par les administrateurs de système pour repérer les vulnérabilités informatiques et par les pirates en vue d'une intrusion informatique.

balayeur de ports n. m.

scanneur de ports
scanner de ports

Le terme *scanneur de ports* (et sa variante *scanner de ports*) est déconseillé parce qu'il ne s'inscrit pas dans la norme sociolinguistique du français au Québec. En outre, l'élément *scanneur* (ou *scanner*), emprunté à l'anglais, ne s'intègre pas au système linguistique du français.

anglais
port scanner

---

31. base de données

Définition
Ensemble structuré d'éléments d'information, généralement sous forme de tables, dans lequel les données sont organisées de manière à permettre leur exploitation.

Notes
Une base de données peut être composée d'un seul fichier, contenant lui-même plusieurs tables.

Bien que certaines sources emploient les termes *base de données* et banque de données de façon interchangeable, ce dernier terme est généralement employé pour désigner un ensemble comprenant plusieurs bases de données ou encore une base de données accessible à un grand nombre d'usagers.

base de données n. f.
BD n. f.

En France, le terme *base de données* est recommandé officiellement par la Commission d'enrichissement de la langue française, depuis 2000.

anglais
database
DB

---

32. biclé

Définition
Paire unique formée d'une clé publique et d'une clé privée, nécessaire au fonctionnement d'un algorithme à clé publique.

biclé n. f.
paire de clés n. f.
paire de clés publique et privée n. f.

L'emploi de la graphie *clef* est en régression. De ce fait, les termes construits avec *clef* sont beaucoup moins répandus en cryptographie que ceux construits avec *clé*.

Les mots formés avec le préfixe *bi-* s'écrivent normalement sans trait d'union.

anglais
key pair
public and private key pair
encryption and decryption key pair rare

---

33. biométrie

Définition
Analyse mathématique des caractéristiques uniques d'une personne, afin de déterminer ou de prouver son identité.

Notes
Dans les domaines judiciaire et médical, la biométrie repose souvent sur la reconnaissance de caractéristiques biologiques comme l'ADN, tandis que, dans le domaine de la sécurité, elle repose sur la reconnaissance de caractéristiques morphologiques (empreinte digitale, reconnaissance faciale) ou de caractéristiques comportementales (démarche, voix, écriture). On parle alors plus précisément de biométrie morphologique et de biométrie comportementale.

biométrie n. f.

anglais
biometrics
biometry

34. biométrie comportementale

Définition
Biométrie basée sur des données relatives à des mesures de caractéristiques dynamiques du corps à travers des actions.

Notes
Il peut s'agir par exemple d'identifier une personne par l'analyse de sa démarche, de sa voix ou de son rythme de frappe au clavier.

La biométrie comportementale s'oppose à la biométrie morphologique.

biométrie comportementale n. f.

anglais
behavioral biometrics
behavioural biometrics
behaviometrics

---

35. biométrie morphologique

Définition
Biométrie basée sur des données relatives à des mesures de caractéristiques fixes d'une partie du corps.

Notes
Il peut s'agir par exemple de la reconnaissance faciale ou de l'analyse des empreintes digitales, de l'iris et de la rétine.

La biométrie morphologique s'oppose à la biométrie comportementale.

biométrie morphologique n. f.
biométrie physique n. f.

biométrie physiologique n. f.

Bien que le terme *biométrie physiologique* soit fréquemment employé pour désigner le concept à l'étude, il n'est pas tout à fait adéquat. En effet, l'adjectif *physiologique* concerne le fonctionnement des organes et des organismes (respiration, digestion, etc.), alors que la biométrie morphologique s'intéresse plutôt aux caractéristiques physiques d'une partie du corps (dimension, forme, etc.). Le terme *biométrie physiologique* pourrait toutefois convenir pour désigner des méthodes basées sur des fonctions physiologiques, comme l'analyse des battements du cœur ou la lecture d'un électroencéphalogramme.

anglais
physical biometrics
physiological biometrics

36. bombe à retardement

Définition
Bombe logique qui s'active automatiquement à une date déterminée par son concepteur.

bombe à retardement n. f.
bombe temporelle n. f.

anglais
time bomb

---

37. bombe logique

Définition
Logiciel malveillant à déclenchement différé qui entre en action dès lors qu'un ensemble de conditions sont réunies.

Notes
La bombe logique peut par exemple s'attaquer à l'intégrité du disque dur si une rançon n'est pas versée dans un compte bancaire.

Lorsque la bombe logique est prévue pour s'activer à une date précise, on parle plus spécifiquement de bombe à retardement.

bombe logique n. f.
bombe programmée n. f.

En France, les termes *bombe logique* et *bombe programmée* sont recommandés officiellement par la Commission d'enrichissement de la langue française, depuis 2005.

anglais
logic bomb
slag code
soft bomb
software bomb

---

38. brèche de sécurité informatique

Définition
Vulnérabilité informatique ayant permis une intrusion illicite dans un système informatique, et pouvant entraîner le vol, la divulgation ou la destruction de données importantes pour une organisation.

brèche de sécurité informatique n. f.
brèche de sécurité n. f.
brèche informatique n. f.

Le terme *brèche* s'emploie en contexte pour désigner le présent concept.

anglais
computer security breach
security breach

Le terme *breach* s'emploie en contexte pour désigner le présent concept.

39. canular

Définition
Fausse information propagée dans un but malveillant, généralement par courrier électronique ou réseau social, qui incite les destinataires à la partager et à effectuer des opérations informatiques.

Notes
L'objet d'un canular peut notamment être une alerte au virus, une chaîne de solidarité ou une pétition, une promesse de récompense ou une occasion d'affaires en or. Il incite le plus souvent à la suppression d'un fichier indispensable au bon fonctionnement d'un système informatique ou au téléchargement d'un fichier contenant un logiciel malveillant.

canular n. m.
canular informatique n. m.

En France, le terme *canular* est recommandé officiellement par la Commission d'enrichissement de la langue française, depuis 2005.

anglais
hoax

---

40. centre de distribution de clés

Définition
Composant de logiciel permettant de produire, de chiffrer et de distribuer des clés de session dans un réseau de partage de données utilisant un système cryptographique à clé secrète, afin de créer un environnement sécuritaire pour l'échange d'informations confidentielles.

centre de distribution de clés n. m.
CDC n. m.
centre de distribution des clés n. m.
CDC n. m.

L'emploi de la graphie *clef* est en régression. De ce fait, les termes construits avec *clef* sont beaucoup moins répandus en cryptographie que ceux construits avec *clé*.

anglais
key distribution centre
KDC
key distribution center
KDC

---

41. certificat numérique

Définition
Certificat délivré par une autorité de certification, accompagnant la transmission d'un document électronique pour attester l'identité de l'expéditeur et l'authenticité de sa clé publique, dans un système cryptographique à clé publique.

Notes
Un certificat numérique contient notamment les informations sur l'identité du détenteur de la clé publique, la clé publique elle-même ainsi que sa date d'expiration. Avec ces informations, le destinataire sera en mesure de confirmer la validité du certificat et de répondre à l'expéditeur de manière sécurisée.

certificat numérique n. m.
certificat électronique n. m.
certificat de clé publique n. m.

Le terme *certificat* s'emploie en contexte pour désigner le présent concept.

anglais

digital certificate
public key certificate
digital identity certificate
identity certificate
digital ID certificate
digital ID

---

42. chaîne cybercriminelle

Définition

Représentation schématique des différentes étapes nécessaires à l'infiltration et à l'exploitation d'un système ou d'un réseau informatique par un pirate informatique.

Notes

En fonction des modèles de chaînes cybercriminelles, les étapes et leurs dénominations peuvent différer. Plusieurs modèles intègrent notamment les étapes de reconnaissance, d'armement et d'exploitation.

chaîne cybercriminelle n. f.
chaîne de frappe n. f.

Le mot *chaîne* peut aussi s'écrire *chaine* en vertu des rectifications de l'orthographe (*chaine cybercriminelle*, *chaine de frappe*).

anglais

kill chain
Cyber Kill Chain marque de commerce

---

43. chapeau blanc

Définition

Personne qui utilise ses compétences en informatique afin de détecter, dans un cadre légal, des vulnérabilités dans les systèmes de sécurité informatique d'une organisation.

Notes

Un chapeau blanc opère avec l'approbation des organisations ciblées, ou du moins, dans le but d'aider une organisation. Entre autres choses, il peut réaliser des tests d'intrusion ou mener des audits de vulnérabilité. En ce sens, il accomplit des tâches analogues à celles d'un analyste en menaces informatiques, mais en demeurant extérieur à une organisation.

Le chapeau blanc s'oppose au chapeau noir, qui opère dans l'illégalité.

chapeau blanc n. m. ou f.

Le terme *chapeau blanc*, calque de l'anglais *white hat hacker*, est acceptable parce qu'il est intégrable au système linguistique du français. En effet, *chapeau blanc* fait ici référence aux clichés de certains films.

anglais

white hat hacker
white hat
ethical hacker

---

44. chapeau gris

Définition

Personne qui utilise ses compétences en informatique afin de détecter, généralement dans un cadre légal, les vulnérabilités des systèmes de sécurité informatique d'une organisation et de les lui signaler.

Notes

Le terme *chapeau gris* sert également à désigner les référenceuses ou référenceurs Web recourant à des pratiques qui sont considérées aux limites de l'acceptable par les moteurs de recherche.

chapeau gris n. m. ou f.

Le terme *chapeau gris*, calque de l'anglais *grey hat hacker*, est acceptable parce qu'il est intégrable au système linguistique du français. En effet, *chapeau gris* renvoie à une personne qui emprunte à la fois aux pratiques des chapeaux blancs et des chapeaux noirs.

anglais

grey hat hacker
gray hat hacker

---

45. chasse aux menaces informatiques

Définition

Recherche proactive et en continu, au sein d'une organisation, de codes d'exploitation ayant déjoué les mécanismes de sécurité en place, d'intrusions informatiques en cours ou encore de vulnérabilités informatiques susceptibles d'être exploitées.

Notes

La chasse aux menaces informatiques vise notamment la neutralisation de cyberattaques persistantes basées sur des méthodes perfectionnées qui complexifient grandement leur détection par les logiciels de sécurité informatique habituels.

La mise en œuvre d'un programme de chasse aux menaces informatiques dans une organisation passe généralement par l'ajout dans la structure organisationnelle d'une équipe d'analystes en menaces informatiques.

chasse aux menaces informatiques n. f.
chasse aux cybermenaces n. f.

anglais

cyber threat hunting
threat hunting

46. cheval de Troie

Définition

Logiciel malveillant dissimulé à l'intérieur d'un programme en apparence inoffensif, qui exécute des opérations nuisibles à l'insu de l'utilisateur.

Notes

Généralement, le cheval de Troie donne un accès à l'ordinateur sur lequel il est exécuté en ouvrant une porte dérobée.

✓ **cheval de Troie** n. m.

En France, le terme *cheval de Troie* est recommandé officiellement par la Commission d'enrichissement de la langue française, depuis 2005.

anglais

Trojan horse
Trojan
Trojan horse program
Trojan program

---

47. chiffrement

Définition

Opération par laquelle des données sont transformées à l'aide d'un algorithme de chiffrement de manière à les rendre inexploitables par quiconque ne possède pas la clé cryptographique permettant de les ramener à leur forme initiale.

✓ **chiffrement** n. m.
cryptage n. m.

Bien que l'utilisation de *cryptage* ait parfois été critiquée pour désigner le chiffrement, on constate que ce terme et ses dérivés tendent à se généraliser dans la documentation spécialisée.

✗ **encryption**

L'emprunt à l'anglais *encryption* est déconseillé puisqu'il ne s'inscrit pas dans la norme sociolinguistique du français au Québec.

anglais

encryption
encipherment
encrypting
enciphering

---

48. clé cryptographique

Définition

Clé utilisée dans un algorithme de chiffrement pour authentifier, chiffrer ou déchiffrer des données ou encore pour créer ou valider une signature numérique.

Notes

Il existe plusieurs types de clés cryptographiques, notamment la clé secrète, la clé publique, la clé de chiffrement et la clé de déchiffrement.

Bien que le terme *clé de chiffrement* soit parfois utilisé dans le sens de « clé cryptographique », il désigne plus spécifiquement la clé servant à chiffrer des données.

clé cryptographique n. f.
clé de données n. f.

L'emploi de la graphie *clef* est en régression. De ce fait, les termes construits avec *clef* sont beaucoup moins répandus en cryptographie que ceux construits avec *clé*.

anglais

cryptographic key
data encryption key
DEK
data key
KD

---

49. clé de chiffrement

Définition

Clé cryptographique utilisée dans un algorithme de chiffrement pour chiffrer des données, les rendant ainsi inaccessibles sans une clé de déchiffrement.

clé de chiffrement n. f.
clé de cryptage n. f.

L'emploi de la graphie *clef* est en régression. De ce fait, les termes construits avec *clef* sont beaucoup moins répandus en cryptographie que ceux construits avec *clé*.

Bien que l'utilisation de *cryptage* ait parfois été critiquée pour désigner le chiffrement, on constate que ce terme et ses dérivés tendent à se généraliser dans la documentation spécialisée.

anglais

encryption key
encipherment key
enciphering key

---

50. clé de déchiffrement

Définition

Clé cryptographique utilisée dans un algorithme de chiffrement pour déchiffrer des données afin de les rendre exploitables.

clé de déchiffrement n. f.

L'emploi de la graphie *clef* est en régression. De ce fait, les termes construits avec *clef* sont beaucoup moins répandus en cryptographie que ceux construits avec *clé*.

clé de décryptage n. f.

Comme le terme décryptage désigne une opération de décodage sans connaissance préalable de la clé de chiffrement, il serait illogique de parler d'une *clé de décryptage*.

anglais

decryption key
deciphering key
decipherment key

---

51. clé de session

Définition

Clé cryptographique à usage unique, le plus souvent générée de manière aléatoire, qui est utilisée dans un système cryptographique à clé secrète afin de sécuriser les échanges lors d'une session.

clé de session n. f.

L'emploi de la graphie *clef* est en régression. De ce fait, les termes construits avec *clef* sont beaucoup moins répandus en cryptographie que ceux construits avec *clé*.

anglais

session key
once-only key
one-time key

---

52. clé privée

Définition

Clé cryptographique utilisée dans un système cryptographique à clé publique pour apposer la signature numérique d'un expéditeur ou pour déchiffrer des données qui ont été chiffrées à l'aide de la clé publique correspondante.

Notes

La clé publique et la clé privée sont les deux composantes d'une biclé.

On distingue la clé privée de la clé secrète, qui est une clé cryptographique connue exclusivement de l'expéditeur et du destinataire d'un message.

clé privée n. f.

L'emploi de la graphie *clef* est en régression. De ce fait, les termes construits avec *clef* sont beaucoup moins répandus en cryptographie que ceux construits avec *clé*.

anglais

private key

---

53. clé publique

Définition

Clé cryptographique utilisée dans un système cryptographique à clé publique pour authentifier la signature numérique d'un expéditeur ou pour chiffrer des données qui ne pourront être déchiffrées que par le détenteur de la clé privée correspondante.

Notes
La clé publique et la clé privée sont les deux composantes de la biclé.

clé publique n. f.
clé révélée n. f.

L'emploi de la graphie *clef* est en régression. De ce fait, les termes construits avec *clef* sont beaucoup moins répandus en cryptographie que ceux construits avec *clé*.

anglais
public key

---

54. clé secrète

Définition
Clé cryptographique utilisée dans un système cryptographique à clé secrète pour procéder au chiffrement et au déchiffrement de données, connue exclusivement de l'expéditeur et du destinataire de celles-ci.

Notes
On distingue la clé secrète de la clé privée, qui est une clé cryptographique utilisée pour déchiffrer des données chiffrées à l'aide de la clé publique correspondante.

clé secrète n. f.

En français, l'emploi de la graphie *clef* est en régression. De ce fait, les termes construits avec *clef* sont beaucoup moins répandus en cryptographie que ceux construits avec *clé*.

anglais
secret key

---

55. code de hachage

Définition
Code qui résulte de la transformation, au moyen d'une fonction de hachage cryptographique, d'un ensemble de données en une séquence alphanumérique de taille réduite, et qui permet d'identifier les données de départ sans y accéder.

Notes
La longueur du code de hachage dépend de l'algorithme de hachage utilisé.

Dans le domaine de la cryptomonnaie, le code de hachage permettant la validation d'un bloc est généralement désigné par le terme empreinte numérique.

code de hachage n. m.
code haché n. m.

anglais
hash code
hash

56. confidentialité des données

Définition

Caractère des données dont l'accès et la diffusion doivent être limités, par des mesures de protection des données, aux seules personnes ou autres entités autorisées.

confidentialité des données n. f.
confidentialité des renseignements n. f.

confidentialité des données personnelles n. f.
confidentialité des renseignements personnels n. f.

On emploie parfois les termes *confidentialité des données personnelles* et *confidentialité des renseignements personnels* pour désigner plus précisément la confidentialité des renseignements personnels, par opposition, par exemple, à celle des données de nature stratégique (données d'entreprise, secret commercial, etc.).

anglais

data privacy
data confidentiality
personal data privacy

On emploie parfois le terme *personal data privacy* pour désigner plus précisément la confidentialité des renseignements personnels, par opposition, par exemple, à celle des données de nature stratégique (données d'entreprise, secret commercial, etc.).

---

57. contrôle d'accès

Définition

Processus par lequel un système informatique analyse le droit d'accès d'une entité afin de déterminer si elle est autorisée à consulter ou à exploiter des données.

contrôle d'accès n. m.
contrôle de l'accès n. m.

anglais

access control
control of access

---

58. copie de sauvegarde

Définition

Copie d'un ou plusieurs fichiers ou programmes, le plus souvent mise à jour à intervalles réguliers, et qui permet la restauration des données en cas de perte.

Notes

Les copies de sauvegarde peuvent être effectuées sur un support amovible tel qu'un disque dur ou une clé USB, ou encore dans le nuage informatique, généralement de manière automatisée.

copie de sauvegarde n. f.
copie de sécurité n. f.
copie de secours n. f.

En contexte, les termes *sauvegarde* et *copie* sont parfois employés seuls pour désigner ce concept.

anglais

backup copy
backup

---

59. correctif

Définition

Portion de code qui modifie un programme de façon sommaire, dans le but de corriger un bogue ou un dysfonctionnement, ou encore d'améliorer ce programme par l'addition d'une fonction, d'une caractéristique, ou par une mise à jour.

correctif n. m.
correctif logiciel n. m.
retouche n. f.
rustine n. f. rare
pièce n. f.

pansement logiciel n. m. désuet

En France, les termes *correctif* et *retouche* sont recommandés officiellement par la Commission d'enrichissement de la langue française, depuis 2003.

anglais

patch
service patch
software patch
software fix

---

60. correctif d'urgence

Définition

Correctif publié en urgence et mis à la disposition des utilisateurs d'un logiciel afin de réparer rapidement un bogue ou d'éliminer une vulnérabilité informatique.

Notes

Un correctif d'urgence vise à colmater en vitesse une vulnérabilité décelée, souvent sans que des tests exhaustifs aient pu être menés en vue d'évaluer les répercussions globales du correctif sur le système.

correctif d'urgence n. m.
correctif à chaud n. m.
correctif provisoire n. m.

anglais

hotfix
hot fix
emergency patch

61. cryptanalyse

Définition
Ensemble des méthodes et procédés de décodage visant à rétablir en clair un cryptogramme, sans connaissance préalable de la clé de chiffrement.

Notes
On utilise la cryptanalyse pour mettre à l'épreuve les procédés de chiffrement utilisés en cryptographie.

La cryptanalyse emploie des méthodes telles que l'attaque par force brute et l'analyse de trafic.

cryptanalyse n. f.
cryptoanalyse n. f.
analyse cryptographique n. f.

anglais
cryptanalysis
cryptoanalysis

---

62. cryptogramme

Définition
Données textuelles rendues inintelligibles à l'aide d'un algorithme de chiffrement et d'une clé de chiffrement, déchiffrables uniquement par la clé de déchiffrement correspondante.

cryptogramme n. m.
message chiffré n. m.
texte chiffré n. m.

anglais
cryptogram
ciphertext
cyphertext
cryptotext
enciphered message
encrypted message

---

63. cryptographie

Définition
Ensemble des principes et techniques permettant le chiffrement et le déchiffrement des données, le plus souvent dans le but d'en préserver la confidentialité et l'intégrité.

Notes
La cryptographie est notamment utilisée afin d'assurer l'intégrité des transactions commerciales ou bancaires ainsi que la confidentialité des messages transmis.

cryptographie n. f.

anglais

cryptography

---

64. cyberactivisme

Définition

Ensemble des actions visant à perturber des sites Web ou des réseaux informatiques de gouvernements ou de grandes entreprises dans le but de défendre une cause politique ou sociale.

Notes

Le cyberactivisme se manifeste notamment par des attaques par déni de service, par le vol et la divulgation de renseignements personnels ou confidentiels, par l'envoi massif de courriers électroniques, par la parodie ou par la modification de sites Web.

En principe, les opérations menées à l'encontre des sites Web et des réseaux informatiques ne visent pas à causer de dégâts sérieux.

✓ **cyberactivisme** n. m. **cybermilitantisme** n. m.	Les mots formés avec *cyber-* ne prennent généralement pas de trait d'union.
✗ **hacktivisme**	L'emprunt intégral adapté *hacktivisme* ne s'inscrit pas dans la norme sociolinguistique du français au Québec. De plus, il ne s'intègre pas au système linguistique du français sur les plans morphologique et sémantique.

anglais

hacktivism
hactivism

---

65. cyberattaque

Définition

Ensemble coordonné d'actions malveillantes conduites par l'intermédiaire du cyberespace, qui visent à endommager, à forcer ou à détourner un réseau ou un système informatique afin de commettre un acte préjudiciable.

Notes

Une cyberattaque peut notamment avoir comme objectif de voler des informations sensibles, d'espionner une personne ou une organisation ou encore d'endommager un système ou d'en altérer le fonctionnement normal.

Une cyberattaque peut notamment cibler des ordinateurs ou des serveurs, isolés ou en réseau, des équipements périphériques et des appareils mobiles.

✓ **cyberattaque** n. f.	Les mots formés avec cyber- ne prennent généralement pas de trait d'union. En France, le terme *cyberattaque* est recommandé officiellement par la Commission d'enrichissement de la langue française, depuis 2017.

anglais

cyberattack
cyber attack
cyber-attack

---

66. déchiffrement

Définition

Opération par laquelle un cryptogramme est rétabli en clair à l'aide de la clé cryptographique correspondante.

Notes

Le déchiffrement est l'opération inverse du chiffrement.

On distingue le déchiffrement du décryptage, qui désigne plutôt le fait de rétablir en clair un cryptogramme dont on ne connaît pas la clé de chiffrement.

déchiffrement n. m.

anglais

decryption
decipherment
decrypting
deciphering

---

67. décryptage

Définition

Opération de décodage d'un cryptogramme, effectuée par cryptanalyse.

Notes

Si le décryptage d'un texte ancien est tout à fait légitime, le décryptage en informatique est parfois illégal. Dans ce cas, on parle alors de piratage informatique.

décryptage n. m.
décryptement n. m.

Il ne faut pas confondre les termes *décryptage* et déchiffrement, souvent employés à tort indifféremment. Cette confusion vient du fait qu'en anglais, on utilise le même terme (*decryption*) pour désigner les deux concepts.

anglais

decryption
codebreaking

68. déni de service

Définition
Impossibilité, pour un usager, d'accéder à un service en ligne en raison d'une augmentation soudaine du nombre de requêtes effectuées auprès du serveur hébergeant ce service.

Notes
Le déni de service est généralement provoqué par une attaque par déni de service ou par un problème de programmation logicielle.

déni de service n. m.

anglais
denial of service
DoS

---

69. destructeur de fichiers

Définition
Logiciel ayant comme fonction de supprimer définitivement des données de manière sécurisée.

Notes
Contrairement à la suppression par le biais de la corbeille, la suppression à l'aide d'un destructeur de fichiers élimine toute possibilité de restauration de données.

destructeur de fichiers n. m.
destructeur de données n. m.
broyeur de fichiers n. m.

Employés seuls, les termes fichier et donnée nomment des concepts qui, bien que connexes, se distinguent l'un de l'autre. Ils peuvent néanmoins être employés de manière interchangeable lorsqu'ils entrent dans la composition de termes complexes (par exemple synchronisation de données, *synchronisation de fichiers*, propriétaire de fichier, *propriétaire de données*, etc.).

anglais
data shredder
file shredder

---

70. détournement de domaine

Définition
Cyberattaque qui consiste à rediriger une adresse URL ou un nom de domaine vers une adresse IP illégitime afin d'induire les utilisateurs en erreur et, ainsi, de collecter leurs informations personnelles.

Notes
Le site d'arrivée illégitime revêt le plus souvent exactement la même apparence que celle du site qu'il reproduit, dans le but de convaincre les utilisateurs de son authenticité présumée.

détournement de domaine n. m.
détournement de nom de domaine n. m.

anglais

pharming
pharming attack

Le terme *pharming* a été formé à partir de la contraction des termes *farming* et *phishing*.

---

71. données d'accès

Définition

Données de connexion que l'utilisateur doit fournir pour avoir accès à un système informatique, à une application ou à un service Web.

Notes

Les données d'accès comportent un identifiant, comme un nom d'utilisateur, et au moins un authentifiant, comme un mot de passe, un numéro d'identification personnel (NIP) ou la réponse à une question de sécurité prédéterminée.

données d'accès n. f. pl.
données d'ouverture de session n. f. pl.
clé d'accès n. f.
justificatifs d'accès n. m. pl.
justificatifs de connexion n. m. pl.
justificatifs d'ouverture de session n. m. pl.

anglais

login credentials
sign-in information
access key

---

72. données résiduelles

Définition

Données restées en mémoire après suppression d'un fichier et avant nettoyage du support.

Notes

Les données résiduelles sont susceptibles de faire l'objet d'une exploitation non autorisée jusqu'à leur suppression définitive par écrasement.

données résiduelles n. f. pl.
résidus n. m. pl.

Les termes *données résiduelles* et *résidus* sont généralement employés au pluriel.

anglais

residual data
residue

73. double chiffrement

Définition
Procédé cryptographique qui consiste à chiffrer une donnée qui a déjà été chiffrée une fois, généralement en utilisant une clé cryptographique ou un algorithme de chiffrement différents.

Notes
Le double chiffrement est une approche spécifique de surchiffrement.

double chiffrement n. m.
double cryptage n. m.

anglais
double encryption
double encipherment

---

74. droit d'accès

Définition
Droit accordé à une entité, lui permettant d'accéder à des données afin de les consulter ou de les exploiter.

Notes
Il ne faut pas confondre le droit d'accès et le privilège d'accès, qui est un droit d'accès particulier utilisé pour assurer la protection des systèmes d'information.

droit d'accès n. m.

anglais
access right
right of access

---

75. empreinte numérique

Définition
Séquence de caractères alphanumériques de longueur fixe, qui représente le contenu d'un message ou d'un fichier sans le révéler, dont la valeur unique est produite par un algorithme de hachage.

Notes
L'empreinte numérique est notamment utilisée pour valider l'intégrité d'un fichier téléchargé sur Internet, l'expéditeur d'un message ou les transactions de cryptomonnaies, ou encore pour le stockage des mots de passe par les fureteurs.

Par exemple, le destinataire valide le contenu d'un message reçu en calculant son empreinte numérique puis en la comparant à celle calculée par le destinateur avant l'envoi du message. Si les deux empreintes numériques sont identiques, le destinataire est assuré de son intégrité.

empreinte numérique n. f.
empreinte de hachage n. f.
valeur de hachage n. f.
condensé n. m.
condensat n. m.
somme de contrôle n. f.

On trouve également les termes *condensé du message*, *résumé de message* et *résumé du message*.

anglais

message digest
hash value
hash digest
fingerprint
cryptographic hash
cryptographic message digest

---

76. enregistrement de frappe

Définition

Fonction d'un logiciel malveillant qui enregistre chacune des touches utilisées sur le clavier d'ordinateur afin de récupérer des informations confidentielles.

enregistrement de frappe n. m.

Par métonymie, le terme *enregistrement de frappe* désigne aussi le résultat de l'opération, soit le fichier comportant les informations, ou chacune des informations saisies.

anglais

keylogging
key logging
keystroke logging
keyboard recording
keystroke recording

---

77. enregistreur de frappe

Définition

Logiciel malveillant qui enregistre chacune des touches utilisées sur le clavier d'un ordinateur.

Notes

L'enregistreur de frappe peut être installé de façon logicielle (à distance ou non), ou de façon matérielle (à l'aide d'un dispositif comme une clé USB, par exemple). Il permet à une personne malveillante de récupérer les renseignements personnels de l'utilisateur, comme des mots de passe, des informations bancaires, des données de navigation sur Internet, etc.

enregistreur de frappe n. m.
espion de clavier n. m.

En France, le terme *enregistreur de frappe* est recommandé officiellement par la Commission d'enrichissement de la langue française, depuis 2013.

anglais

keylogger
key logger
keystroke recorder
keystroke logger

---

78. facteur d'authentification

Définition

Catégorie d'éléments de même nature servant à l'authentification d'un utilisateur.

Notes

Parmi les principaux facteurs d'authentification, on trouve : « ce que l'on sait » (par exemple, un mot de passe), « ce que l'on possède » (par exemple, un appareil mobile), « ce que l'on est » (par exemple, une empreinte digitale).

Lorsqu'un système d'authentification nécessite l'utilisation de plus d'un facteur d'authentification, on parle alors d'authentification à deux facteurs ou d'authentification multifacteur.

facteur d'authentification n. m.

anglais

authentication factor

---

79. falsification de requête intersites

Définition

Cyberattaque visant à exploiter de manière malveillante un site Web en lui transmettant des commandes non autorisées à partir du compte d'un utilisateur connecté, authentifié et qui dispose des privilèges requis, et ce, sans son consentement.

Notes

L'utilisateur est généralement piégé lors d'une visite sur un site malveillant contenant un script invisible qui s'exécute automatiquement au chargement de la page. Cet utilisateur s'étant récemment connecté au site Web cible, le script peut transmettre les commandes à son insu puisque les informations d'authentification ont préalablement été saisies et sont envoyées automatiquement au serveur.

Une falsification de requête intersites peut notamment être utilisée pour publier des données non autorisées, obtenir des numéros de cartes de crédit ou effectuer des transactions financières frauduleuses.

falsification de requête intersites n. f.

Le préfixe *inter-*, dans *intersites*, se soude à l'élément qui suit.

Lorsqu'un adjectif est formé du préfixe *inter-* et d'un nom, cet adjectif se met au pluriel quand il renvoie à plusieurs entités, même si le nom auquel il se rapporte est singulier.

anglais

cross-site request forgery
CSRF
XSRF
session riding
one-click attack
hostile linking
sea surf

---

80. fermeture de session

Définition

Opération que doit effectuer un utilisateur pour mettre fin de façon sécuritaire à une session de connexion à un système informatique, à une application ou à un service Web, de sorte qu'un utilisateur non autorisé ne puisse y accéder.

fermeture de session n. f.
déconnexion n. f.

anglais

logout
log-out
logoff
log-off
sign-out
sign-off

Les graphies *log out*, *log off*, *sign out* et *sign off*, sans trait d'union, sont également utilisées pour désigner l'opération, mais elles désignent plus fréquemment le verbe (*fermer une session*, *se déconnecter*).

---

81. fonction de hachage cryptographique

Définition

Fonction mathématique qui, appliquée à un ensemble de données de départ, génère un code de hachage.

Notes

La fonction de hachage cryptographique implique que le moindre changement dans les données de départ entraîne une modification importante du code d'arrivée.

La longueur du code de hachage obtenu varie selon l'algorithme de hachage utilisé.

Dans le domaine de la cryptomonnaie, la fonction de hachage cryptographique est une fonction intégrale appliquée à divers composants du système : signature de transaction, preuve de travail, arbre de Merkle, etc.

fonction de hachage cryptographique n. f.
fonction de hachage n. f.
fonction de condensation n. f.

anglais

cryptographic hash function
cryptographic hashing function
hash function
hashing function

---

82. fuite d'information

Définition
Transmission non autorisée d'informations sensibles à l'insu et au préjudice de l'organisation qui les détient, et qui constitue une atteinte à la confidentialité.

Notes
Une fuite d'information peut être intentionnelle ou accidentelle.

fuite d'information n. f.
fuite de données n. f.

anglais
information leakage
data leakage

---

83. gestion des privilèges

Définition
Gestion de la création et de la distribution des droits d'accès aux divers comptes utilisateur d'une organisation.

Notes
L'administrateur responsable de la gestion des privilèges doit également établir les contrôles d'accès qui déterminent les ressources auxquelles peut accéder un compte utilisateur.

gestion des privilèges n. f.
gestion de privilèges n. f.

anglais
privilege management

---

84. hachage

Définition
Opération qui consiste à appliquer une fonction mathématique à un groupe de données de taille variable afin de générer un code unique de taille fixe, que l'on utilisera pour l'authentification et le stockage d'information.

Notes
Le hachage est notamment utilisé dans le domaine de la cryptomonnaie pour la compression de données relatives aux blocs de transactions à enregistrer sur une chaîne de blocs.

hachage n. m.

anglais
hashing
hash coding

85. hameçonnage

Définition

Technique de fraude basée sur l'usurpation d'identité, qui consiste à envoyer massivement un message en se faisant passer pour une institution financière ou une entreprise commerciale de renom afin d'induire les destinataires en erreur et de les inciter à révéler des informations sensibles à leur insu.

Notes

Par exemple, un courriel frauduleux semblant provenir d'une banque connue pourrait inviter le destinataire à mettre à jour son compte en cliquant sur un hyperlien qui le redirige vers une copie conforme du site Web de cette banque, où le fraudeur peut récupérer des renseignements susceptibles de servir à détourner des fonds (mot de passe, numéro de carte de crédit, etc.).

hameçonnage n. m.

Le terme *hameçonnage* a été proposé par l'Office québécois de la langue française, en avril 2004, pour désigner ce concept.

Tout comme pour *hameçon*, dont le *h* initial n'est pas un *h* aspiré, on écrira *l'hameçonnage* et non *le hameçonnage*. En effet, devant un mot commençant par un *h* muet, on fait l'élision, qui est marquée à l'écrit par l'apostrophe, qui remplace la lettre élidée *e*. De plus, à l'oral, avec *un*, *des*, *cet*, *ces*, etc., on fera la liaison.

En France, le terme *hameçonnage* est recommandé officiellement par la Commission d'enrichissement de la langue française, depuis 2021.

filoutage n. m.

Bien que l'on emploie parfois le terme *filoutage* au sens de « hameçonnage », ce terme a une valeur plus générale et peut désigner toute forme d'escroquerie.

escroquerie par courriel
phishing

Le terme *escroquerie par courriel* est déconseillé pour désigner le présent concept, en raison de son manque de précision. De plus, il est possible de faire de l'hameçonnage par d'autres moyens que le courrier électronique.

L'emprunt intégral à l'anglais *phishing* est déconseillé parce qu'il n'est pas légitimé dans l'usage en français au Québec. En outre, il ne s'intègre pas au système linguistique du français.

anglais

phishing
phishing attack
phishing scam

Le terme *phishing* est dérivé du terme *fishing* (*pêche*) et s'écrit avec un *ph*, comme c'est souvent le cas dans le jargon des pirates où il y a substitution de lettres (par exemple *phreaking*, qui vient de *phone freak*, où *phone* devient *fone* et *freak* devient *phreak*, puis *phreaking*). Ce terme fait allusion à la pêche à la ligne (Internet est métaphorisé par l'océan, et les utilisateurs, par des poissons).

86. harponnage

Définition

Hameçonnage par lequel sont visés de façon plus précise un nombre très restreint d'internautes, le plus souvent des employés d'une grande société ou d'un organisme gouvernemental, afin de leur soutirer des informations sensibles, ce qui permet ensuite de pénétrer les systèmes informatiques.

Notes

Les harponneurs peuvent augmenter la vraisemblance du message à l'aide de données spécifiques, comme le nom, le prénom et l'adresse postale de l'internaute.

Les messages de harponnage peuvent notamment prendre la forme d'un courrier ou d'une note interne émanant d'un service de l'entreprise ou de l'organisme, et ce, afin d'obtenir des renseignements sur son réseau informatique, à des fins de vol de propriété intellectuelle et d'autres informations sensibles (commerciales ou gouvernementales).

✓ **harponnage** n. m.
hameçonnage ciblé n. m.

Tout comme pour *harpon*, dont le *h* initial est un *h* aspiré, on écrit *le harponnage* et non *l'harponnage*. Il faut noter que pour *hameçonnage*, la règle est inversée : puisque le *h* initial n'est pas un *h* aspiré, on écrit *l'hameçonnage* et non *le hameçonnage*.

✗ **phishing ciblé**
spear-phishing

Les emprunts *phishing ciblé* et *spear-phishing* sont déconseillés parce qu'ils ne s'inscrivent pas dans la norme sociolinguistique du français au Québec. En outre, ces termes ne s'intègrent pas au système linguistique du français.

anglais

spear phishing
spear-phishing
spear phishing attack
spear-phishing attack
spear phishing scam
spear-phishing scam

---

87. horodatage

Définition

Opération consistant à attribuer une marque temporelle précise, incluant la date et l'heure, à un document, à une donnée ou à une intervention.

Notes

Lorsqu'il est nécessaire que l'horodatage soit certifié, il est généralement fait par un tiers appelé autorité d'horodatage.

✓ **horodatage** n. m.
horodatation n. f.

anglais

timestamping

88. identifiant

Définition
Information fournie par une entité, au cours d'une procédure d'identification, pour décliner son identité en tant qu'utilisateur afin d'accéder à un réseau, à un système ou à une application.

Notes
Pour un système donné, chaque identifiant doit être unique. Il peut s'agir, par exemple, d'une carte bancaire, d'un nom d'utilisateur, d'une adresse de courrier électronique ou d'un numéro de compte.

L'identifiant se distingue de l'authentifiant, qui, lui, est fourni pour prouver que l'utilisateur est bien le propriétaire de l'identifiant déclaré.

identifiant n. m.

anglais
identifier

---

89. information confidentielle

Définition
Information qui ne doit être communiquée ou rendue accessible qu'aux personnes et aux entités autorisées.

information confidentielle n. f.
donnée confidentielle n. f.

On parlera plus spécifiquement d'information sensible lorsqu'une information confidentielle a le potentiel de mettre en péril l'intégrité de la personne ou de l'organisation qu'elle concerne.

anglais
confidential information
confidential data

---

90. information sensible

Définition
Information confidentielle dont la divulgation, l'altération, la perte ou la destruction sont susceptibles de porter préjudice à la personne ou à l'organisation qu'elle concerne.

Notes
Les informations sensibles peuvent notamment être de nature nominative, professionnelle, économique, financière, stratégique ou organisationnelle.

information sensible n. f.
donnée sensible n. f.
information critique n. f.
donnée critique n. f.

En ce qui concerne la sécurité des individus et des organisations, les termes *information sensible* et *donnée sensible*, bien que calqués sur l'anglais, sont acceptables. Ils s'emploient aujourd'hui couramment dans le domaine de l'informatique, où ils ont acquis un sens bien précis, puisqu'ils permettent d'exprimer à la fois les idées de « confidentialité », de « risque de préjudice » et de « risque d'atteinte à la sécurité ».

anglais

sensitive information
sensitive data
sensitive asset

---

91. installation furtive

Définition

Installation de logiciels malveillants qui s'effectue à l'insu d'un internaute lorsqu'il installe un programme, souvent gratuit, qui semble digne de confiance, mais qui est en réalité corrompu.

installation furtive n. f.

anglais

drive-by install
drive-by installation

---

92. intégrité des données

Définition

Propriété des données qui ne subissent aucune altération accidentelle ou non autorisée lors de leur traitement, de leur transmission ou de leur conservation.

intégrité des données n. f.
intégrité n. f.

anglais

data integrity
integrity

---

93. interface truquée

Définition

Interface d'un site Internet comportant des astuces ergonomiques destinées à duper les utilisateurs.

Notes

Par exemple, des options sont présélectionnées; certaines informations sont dissimulées, de sorte qu'elles sont difficilement repérables; lors de l'achat d'un produit ou d'un service, des produits complémentaires comme une garantie ou une assurance sont ajoutés par défaut; des astuces amènent de façon subtile l'utilisateur à souscrire un abonnement sans qu'il l'ait souhaité, etc.

interface truquée n. f.

Le terme *interface truquée* a été proposé par l'Office québécois de la langue française en 2018 pour désigner ce concept.

anglais

dark pattern

---

94. intrusion informatique

Définition

Accès non autorisé à un système informatique ou à un réseau, obtenu en contournant ou en désamorçant les dispositifs de sécurité en place.

Notes

Une intrusion informatique peut être perpétrée pour diverses raisons, notamment pour modifier ou voler de l'information confidentielle, fausser, contaminer ou détruire les données du système, ou encore exploiter les ressources matérielles. Par ailleurs, un test d'intrusion peut être réalisé afin de détecter les vulnérabilités informatiques d'un système.

intrusion informatique n. f.
cyberintrusion n. f.
intrusion n. f.
pénétration informatique n. f.
intrusion électronique n. f. rare
intrusion logique n. f. rare

anglais

computer system intrusion
intrusion
penetration

---

95. jeton d'authentification

Définition

Authentifiant, généralement valide pour une durée limitée, qu'un utilisateur obtient par le biais d'un logiciel d'application ou d'un dispositif de sécurité qu'il a en sa possession.

Notes

Le jeton d'authentification est souvent couplé avec un autre facteur d'authentification : quelque chose que l'utilisateur sait (mot de passe, numéro d'identification personnel) ou quelque chose que l'utilisateur est (donnée biométrique). On parle alors d'authentification multifacteur.

jeton d'authentification n. m.
jeton de sécurité n. m.

Par métonymie, les termes *jeton d'authentification* et *jeton de sécurité* (voir jeton d'authentification matériel) désignent également le dispositif électronique utilisé.

anglais

authentication token
security token

---

96. jeton d'authentification matériel

Définition

Dispositif de sécurité conçu pour être transporté avec soi et qui sert à produire des authentifiants généralement valides pour une durée limitée.

Notes
Le dispositif peut se présenter sous différentes formes : carte, porte-clé, clé USB, etc.

jeton d'authentification matériel n. m.
jeton de sécurité matériel n. m.
jeton matériel n. m.
jeton d'authentification n. m.
jeton de sécurité n. m.

Les termes jeton d'authentification et *jeton de sécurité* désignent d'abord l'authentifiant créé par le dispositif.

anglais
authentication token device
security token device
hardware authentication token
hardware security token
authentication token
hardware token

On trouve aussi les termes *hard authentication token*, *hard security token, hard token* et *security token* employés pour désigner le présent concept.

---

97. journalisation

Définition
Enregistrement chronologique, dans un fichier ou une base de données, des opérations effectuées dans un système informatique, un programme ou un fichier.

Notes
La journalisation peut notamment permettre d'effectuer des analyses diverses, de garder des traces des différents utilisateurs et de faciliter le débogage. Elle peut également, dans certains cas, avoir une valeur juridique.

journalisation n. f.

anglais
logging
security logging
journaling

---

98. liste de droits d'accès

Définition
Liste des entités autorisées décrivant leur habilitation de sécurité respective.

Notes
La liste de droits d'accès est enregistrée dans un système informatique, de manière à ce que celui-ci puisse procéder aux vérifications nécessaires à chaque tentative d'accès aux données.

liste de droits d'accès n. f.
liste de contrôle d'accès n. f.
LCA n. f.
liste d'accès n. f.
liste des autorisations n. f.
table des droits d'accès n. f.

anglais

access control list
ACL
access list
authorization list

---

99. logiciel antivirus

Définition

Logiciel de sécurité informatique qui procède à l'analyse de données afin de détecter les virus, de bloquer leur intrusion ou de les supprimer d'un système infecté.

Notes

Les logiciels antivirus comprennent généralement un logiciel de détection de virus, un éradicateur de virus et un logiciel de prévention agissant en amont des tentatives d'infection.

logiciel antivirus n. m.
antivirus n. m.
logiciel AV n. m.
logiciel de protection antivirus n. m.

En France, les termes *logiciel antivirus* et *antivirus* sont recommandés officiellement par la Commission d'enrichissement de la langue française, depuis 2005.

anglais

antivirus software
antivirus
AV software
antivirus program
virus-protection software

---

100. logiciel de rançon

Définition

Logiciel malveillant qui permet de verrouiller un ordinateur ou d'en chiffrer les données, dans le but d'extorquer de l'argent à l'utilisateur.

Notes

L'accès aux données ne sera pas nécessairement rendu à l'utilisateur après le versement d'une somme d'argent.

logiciel de rançon n. m.
logiciel rançonneur n. m.
logiciel d'extorsion n. m.
rançongiciel n. m.

Au pluriel, on écrira : *des logiciels de rançon*, *des rançongiciels*, *des logiciels rançonneurs*, *des logiciels d'extorsion*.

anglais

ransomware

---

101. logiciel espion

Définition

Logiciel généralement indétectable qui s'infiltre dans un système informatique lors d'un téléchargement ou d'une installation dans le but d'employer la connexion Internet d'un utilisateur pour recueillir et transmettre ses renseignements personnels à son insu.

Notes

Les logiciels espions recueillent le plus souvent des renseignements personnels portant sur les intérêts et les habitudes de navigation à des fins commerciales.

Les logiciels espions ne sont pas répertoriés dans le système comme des logiciels et ne peuvent donc pas être désinstallés. On peut cependant les repérer et les supprimer à l'aide d'un anti-logiciel espion.

logiciel espion n. m.
logiciel-espion n. m.
programme espion n. m.
espiogiciel n. m.
mouchard n. m.

En informatique, lorsque les termes logiciel et programme participent à la formation de termes complexes (ex. : logiciel antivirus, *programme antivirus*, logiciel d'application, *programme d'application*), ces deux termes s'utilisent le plus souvent de manière interchangeable.

En France, le terme *logiciel espion* est recommandé officiellement par la Commission d'enrichissement de la langue française, depuis 2007.

Au pluriel, on écrira : *des logiciels espions* (*logiciels-espions*) ou *des programmes espions*. Dans ces termes, le deuxième élément (*espions*) prend la marque du pluriel parce qu'il est en apport de qualification avec le premier. Voir, à ce sujet, l'article Règle générale du pluriel et du trait d'union pour le nom complément du nom de la *Banque de dépannage linguistique*.

Le terme *espiogiciel* est un mot-valise issu de la contraction des termes *espion* et *logiciel*.

anglais

spyware

---

102. logiciel hôte

Définition

Logiciel infecté qui, une fois lancé, provoque l'activation et la reproduction d'un virus informatique, le plus souvent de manière indétectable.

Notes

Le logiciel hôte conserve généralement toutes ses fonctionnalités lorsqu'il est infecté, ce qui rend ardue la détection du virus informatique.

logiciel hôte n. m.
programme hôte n. m.

En informatique, lorsque les termes logiciel et programme participent à la formation de termes complexes (ex. : logiciel d'application, *programme d'application*, logiciel espion, *programme espion*), ils s'utilisent le plus souvent de manière interchangeable.

Le terme *hôte* s'emploie parfois en contexte pour désigner le présent concept.

fichier hôte n. m.

On emploie plus spécifiquement le terme *fichier hôte* pour désigner un fichier infecté par un virus informatique.

anglais

host program
host software
host file

Le terme *host* s'emploie parfois en contexte pour désigner le présent concept.

Le terme *host file* est plus spécifiquement employé pour désigner un fichier infecté par un virus informatique.

---

103. logiciel malveillant

Définition

Logiciel visant à voler, à altérer ou à détruire des données afin de porter préjudice à leur propriétaire ou de nuire au fonctionnement d'un système informatique.

Notes

On trouve, parmi les différents types de logiciels malveillants, les vers informatiques, les chevaux de Troie, les bombes logiques et les logiciels espions.

logiciel malveillant n. m.
programme malveillant n. m.
logiciel pernicieux n. m.
maliciel n. m.
pourriciel n. m.

En France, le terme *logiciel malveillant* est recommandé officiellement par la Commission d'enrichissement de la langue française, depuis 2005.

Le terme *pourriciel* est principalement employé en Europe francophone.

anglais

malicious software
malware
malicious program

---

104. menace active

Définition

Menace informatique dont la réalisation entraîne une modification illicite de l'état du système.

Notes

La modification non autorisée d'un fichier et l'insertion de faux messages, par exemple, constituent des menaces actives.

On oppose généralement les menaces actives aux menaces passives, qui n'ont trait qu'à la confidentialité.

menace active n. f.

anglais

active threat

---

105. menace informatique

Définition

Événement potentiel et appréhendé, susceptible de porter atteinte à un système informatique.

menace informatique n. f.
cybermenace n. f.
menace n. f.

Les mots formés avec *cyber-* ne prennent généralement pas de trait d'union, sauf lorsque l'élément qui le suit est un nom propre.

anglais

information security threat
cyber threat
cyberthreat
security threat
computer threat
threat

---

106. menace passive

Définition

Menace informatique dont la réalisation constitue une atteinte à la seule confidentialité, n'entraînant de ce fait aucune modification illicite du système.

Notes

À titre d'exemples, un coup d'œil indiscret sur un écran affichant des données pour lesquelles aucun droit de lecture n'a été accordé ou encore l'enregistrement non autorisé de données sont des menaces passives.

On oppose généralement les menaces passives aux menaces actives, qui concernent plutôt l'intégrité des données.

menace passive n. f.

anglais

passive threat

---

107. modèle à vérification systématique

Définition

Modèle de sécurité par lequel tous les usagers, programmes ou systèmes qui tentent de se connecter au réseau d'une organisation doivent être systématiquement authentifiés et autorisés.

Notes
Le modèle à vérification systématique, en accordant aux utilisateurs uniquement l'accès aux ressources dont ils ont spécifiquement besoin, améliore la gestion des accès et la sécurisation des applications, de même qu'il offre une performance optimisée.

modèle à vérification systématique n. m.

Le terme *modèle à vérification systématique* a été proposé par l'Office québécois de la langue française en décembre 2019 pour désigner ce concept.

anglais
zero trust model
zero trust network
zero trust architecture
zero trust

---

108. mot de passe

Définition
Chaîne de caractères associée à un compte, que le titulaire doit entrer lors de la procédure d'accès afin de s'authentifier.

Notes
Le mot de passe est le plus souvent couplé à un nom d'utilisateur ou à une carte informatique.

Un mot de passe est réputé plus efficace lorsqu'il comporte des lettres majuscules et minuscules, des chiffres et des caractères spéciaux.

On distingue deux types de mots de passe : le mot de passe statique et le mot de passe dynamique.

mot de passe n. m.

anglais
password
pwd

---

109. mot de passe dynamique

Définition
Mot de passe ne pouvant être utilisé qu'une seule fois, qui est généré par un algorithme sur un appareil informatique auquel seul l'utilisateur habilité a accès.

Notes
Le mot de passe dynamique est le plus souvent utilisé pour l'authentification à deux facteurs.

mot de passe dynamique n. m.
mot de passe à usage unique n. m.

anglais

dynamic password
one-time password
OTP

---

110. mot de passe dynamique fondé sur le temps

Définition

Mot de passe dynamique temporaire obtenu à partir d'une fonction de hachage cryptographique combinant une clé unique ainsi qu'une estampille temporelle, et qui se renouvelle à intervalles réguliers.

Notes

Le mot de passe dynamique fondé sur le temps est généralement valide pendant une minute et peut être généré même en étant hors ligne.

mot de passe dynamique fondé sur le temps n. m.
mot de passe dynamique temporel n. m.

Les termes *mot de passe dynamique fondé sur le temps* et *mot de passe dynamique temporel* ont été proposés par l'Office québécois de la langue française en novembre 2020 pour désigner ce concept.

anglais

time-based one-time password
TOTP

---

111. mot de passe statique

Définition

Mot de passe qu'un utilisateur doit entrer lors de chaque procédure d'accès à son compte afin de s'authentifier.

Notes

Contrairement au mot de passe dynamique, le mot de passe statique associé à un compte est généralement valide pendant une certaine période ou jusqu'à ce que le titulaire le change.

mot de passe statique n. m.

anglais

static password

---

112. mystification

Définition

Technique de violation de la sécurité informatique, qui amène une entité à se livrer à un acte préjudiciable pour elle-même ou pour son organisation, en lui faisant croire qu'elle est en communication avec un système informatique légitime ou avec une personne autorisée.

Notes
La mystification vise, le plus souvent, à obtenir de l'information pour laquelle aucun accès n'a été accordé, en amenant un utilisateur légitime détenant un accès privilégié à fournir malgré lui son mot de passe.

Cette technique frauduleuse recourt notamment à l'usurpation d'adresse IP ou à l'usurpation d'adresse électronique.

mystification n. f.
incitation à la faute n. f.

Plusieurs autres termes plus génériques, comme *arnaque* ou *tromperie*, sont parfois utilisés pour désigner une mystification.

anglais
spoofing

---

113. nom d'utilisateur

Définition
Identifiant consistant en une chaîne de caractères, attribué à un utilisateur ou choisi par lui et permettant de le distinguer des autres utilisateurs d'un système.

Notes
Par exemple, dans une adresse de courrier électronique, la partie qui précède le a commercial constitue un nom d'utilisateur.

nom d'utilisateur n. m.
nom utilisateur n. m.
ID utilisateur n. m.

L'emploi de *ID* comme forme abrégée de *identification* découle probablement de son usage en anglais. Le terme *ID utilisateur* est acceptable parce qu'il est légitimé en français au Québec et ailleurs en francophonie.

anglais
username
user identifier
user ID
personal identifier

---

114. numéro d'identification personnel

Définition
Authentifiant prenant la forme d'un code numérique.

Notes
En Europe francophone, on emploie aussi le sigle anglais *PIN*, seul ou dans *code PIN*, pour désigner ce concept.

numéro d'identification personnel n. m.
NIP n. m.

anglais
personal identification number
PIN
PIN number

Le terme *PIN number* est parfois critiqué, puisqu'il implique la répétition du mot *number*, *PIN* étant l'acronyme de *personal identification number*.

115. ordinateur zombie

Définition
Ordinateur ayant été compromis par un logiciel malveillant, qui sert de relais pour l'envoi massif de pourriels ou qui participe à des cyberattaques à l'insu de son propriétaire.

Notes
Les ordinateurs zombies cherchent également à infecter d'autres ordinateurs, de manière à créer un réseau d'ordinateurs zombies aptes à lancer des cyberattaques d'envergure, par exemple des attaques par déni de service distribué.

ordinateur zombie n. m.
machine zombie n. f.
zombie n. m.

Au pluriel, on écrira : *des ordinateurs zombies*, *des zombies*, *des machines zombies*.

anglais
zombie computer
zombie
bot
zombie bot

---

116. ouverture de session

Définition
Procédure consistant à fournir ses données d'accès afin d'utiliser un système informatique, une application ou un service Web.

Notes
Les données d'accès à fournir sont un identifiant (par exemple, un nom d'utilisateur) et un authentifiant (par exemple, un mot de passe).

ouverture de session n. f.
connexion n. f.

Par extension, le terme *connexion* peut aussi désigner le fait d'être connecté à un système, à une application. C'est ainsi que l'on peut parler de *temps de connexion* ou de *maintien de la connexion*.

En France, le terme *connexion* est recommandé officiellement par la Commission d'enrichissement de la langue française, depuis 1998.

anglais
login
log-in
sign-in

Les termes formés avec la préposition *on* (*logon*, *log-on*, *sign-on*) sont aussi employés, mais moins couramment.

Les graphies *log in* et *sign in*, sans trait d'union, sont également utilisées pour désigner la procédure, mais elles désignent plus fréquemment le verbe (équivalent de *ouvrir une session*, *se connecter*).

117. paiement sécurisé

Définition

Paiement effectué en ligne sur un site sécurisé qui utilise un protocole de sécurité assurant le chiffrement des données afin de conserver leur confidentialité.

paiement sécurisé n. m.

anglais

secure payment
secured payment

---

118. pare-feu

Définition

Système de sécurité conçu pour filtrer les flux de données entre un réseau et un autre réseau de confiance moindre, le plus souvent Internet, selon une politique d'accès préétablie.

Notes

Les pare-feu peuvent prendre différentes formes selon les besoins de protection. En effet, ils peuvent notamment être constitués par un ou plusieurs logiciels de sécurité hébergés sur un ordinateur de bureau, par exemple, ou encore par un ensemble de matériels et de logiciels spécialement conçu pour la protection d'un réseau de grande envergure.

pare-feu n. m. recommandé par l'OQLF
coupe-feu n. m. recommandé par l'OQLF

Au pluriel, on écrira : *des pare-feu, des coupe-feu,* selon la graphie traditionnelle, et *des pare-feux*, *des coupe-feux*, selon la graphie rectifiée. Voir, à ce sujet, l'article *Rectifications liées au pluriel des mots composés* de la *Banque de dépannage linguistique*.

On trouve aussi, assez rarement, les termes *barrière de sécurité* et *garde-barrière*.

En France, les termes *pare-feu* et *barrière de sécurité* sont recommandés officiellement par la Commission d'enrichissement de la langue française, depuis 2022.

firewall

L'emprunt à l'anglais *firewall*, employé fréquemment au Québec et ailleurs en francophonie pour désigner le concept, est déconseillé. Il est parfois accompagné de commentaires précisant qu'il appartient à la langue anglaise. De plus, il entre en concurrence avec les termes français bien implantés dans l'usage.

anglais

firewall

119. passerelle sécurisée d'accès au nuage

Définition

Logiciel agissant à titre d'intermédiaire entre l'utilisateur et le nuage informatique d'un service infonuagique, qui vérifie que chaque tentative d'accès à celui-ci est conforme aux politiques de sécurité du service.

Notes

La passerelle sécurisée d'accès au nuage est notamment utilisée pour appliquer automatiquement des règlements et des politiques de confidentialité des données; assurer une gestion et un contrôle des identifiants, des authentifiants et des fichiers partagés; prévenir les fuites d'information (à l'aide d'une méthode d'avertissement ou de chiffrement, par exemple).

✓	**passerelle sécurisée d'accès au nuage** n. f.	Le terme *passerelle sécurisée d'accès au nuage* a été proposé en juillet 2021 par l'Office québécois de la langue française pour désigner ce concept.

anglais

cloud access security broker
CASB

---

120. pixel espion

Définition

Image le plus souvent transparente, de la taille d'un pixel et dont le chargement, lors de la visite d'un site Web ou de l'ouverture du courrier électronique, provoque une requête sur un serveur tiers visant à collecter des informations à l'insu de l'internaute.

Notes

Le pixel espion permet notamment de recueillir des données concernant le système d'exploitation utilisé, le temps de lecture, les actions réalisées sur un site Web, le fournisseur de services Internet et la localisation.

Le pixel espion fonctionne en tandem avec les témoins.

Le gestionnaire d'un site Web ou l'expéditeur d'un courrier électronique y intègre le pixel espion au moyen d'une chaîne de code HTML qui contient un lien externe vers un serveur.

✓	**pixel espion** n. m. **pixel invisible** n. m. **image invisible** n. f.	
!	**GIF invisible** n. m.	On emploie le terme *GIF invisible* lorsque le pixel espion est une image de format GIF.

anglais

Web bug
pixel tag
Web beacon
tracking bug
tracking pixel
invisible GIF
clear GIF
tracker GIF
single-pixel GIF

On trouve également les termes *clear pixel*, *invisible pixel* et *HTML bug*.

On emploie les termes *invisible GIF*, *clear GIF*, *tracker GIF* et *single-pixel GIF* lorsque le pixel espion est une image de format GIF.

---

121. placement de publicité malveillante

Définition

Utilisation de l'espace publicitaire des sites Web afin de mettre en ligne des publicités malveillantes visant à propager un logiciel malveillant.

Notes

Le placement de publicité malveillante peut être conçu pour entrer en action dès le chargement de la publicité, ou encore seulement lorsqu'un utilisateur clique sur la publicité.

placement de publicité malveillante n. m.

Le terme *placement de publicité malveillante* a été proposé par l'Office québécois de la langue française en décembre 2020 pour désigner ce concept.

malvertising

Malvertising est déconseillé parce qu'il n'est pas légitimé dans l'usage en français par les spécialistes de la sécurité informatique. En effet, il est généralement employé en italique ou entre guillemets, signe que les usagers émettent des doutent quant à sa légitimité.

anglais

malicious advertising
malvertising

---

122. plan de continuité d'activité

Définition

Ensemble des mesures visant à assurer le maintien des services essentiels selon les principaux scénarios d'indisponibilité des ressources informatiques.

Notes

Le plan de continuité d'activité doit permettre de prévoir la majorité des circonstances entraînant l'arrêt de l'exploitation des ressources informatiques lors de crises, de même que toutes les mesures palliatives et curatives applicables à chacune de celles-ci.

Le plan de continuité d'activité est une composante essentielle du plan de sécurité informatique.

plan de continuité d'activité n. m.
PCA n. m.
plan de continuité des activités n. m.
PCA n. m.
plan de continuité des affaires n. m.
PCA n. m.
plan de continuité d'exploitation n. m.
PCE n. m.

plan de continuité des opérations
PCO

Le terme *plan de continuité des opérations* ainsi que son abréviation *PCO* sont déconseillés pour désigner le présent concept. En effet, *opération* a un sens plus restreint que l'anglais *operation* et désigne une « action produisant un effet donné » ou encore un « ensemble de manœuvres accomplies dans un but déterminé »; il ne peut s'employer au sens plus général de « fonctionnement » ou d'« exploitation ».

anglais

business continuity plan
BCP
continuity plan

---

123. plan de reprise après sinistre

Définition

Plan dans lequel sont prévues les différentes étapes nécessaires au transfert et à la reprise graduelle des activités d'une organisation en cas de sinistre informatique.

Notes

Un plan de reprise après sinistre prévoit généralement le transfert progressif, sur une période déterminée, de l'exploitation dans un centre de secours. En effet, le nombre d'applications devenant critiques augmente au fur et à mesure que passe le temps d'indisponibilité des ressources.

plan de reprise après sinistre n. m.
PRS n. m.
plan antisinistre n. m.
plan anticatastrophe n. m.

anglais

disaster recovery plan
DRP
computer disaster plan
IT disaster recovery plan
backup operation plan

124. plan de sauvegarde des données

Définition
Ensemble de règles précises ayant trait à la sauvegarde informatique des fichiers, particulièrement en vue d'une restauration rapide après un sinistre informatique.

Notes
Le plan de sauvegarde présente l'ensemble des procédures de sauvegarde concernant les fichiers stratégiques de même que la périodicité, le lieu et la durée de stockage des copies de sauvegarde.

plan de sauvegarde des données n. m.
plan de sauvegarde n. m.

anglais
data backup plan
backup plan

---

125. point de restauration

Définition
Point d'un programme en cours d'exécution ou d'un système d'exploitation à partir duquel la restauration pourra être effectuée si une erreur humaine ou une défaillance du système entraîne l'interruption des opérations.

point de restauration n. m.
point de reprise n. m.
point de contrôle n. m.
point de rétablissement n. m.
point de cohérence n. m.

anglais
restore point
restart point
recovery point
rescue point
rerun point
checkpoint

---

126. politique de sécurité informatique

Définition
Énoncé général émanant de la direction d'une organisation, et indiquant la ligne de conduite adoptée relativement à la sécurité informatique, à sa mise en œuvre et à sa gestion.

politique de sécurité informatique n. f.
politique de sécurité n. f.

anglais

computer security policy
security policy

---

127. porte dérobée

Définition

Accès caché à un programme prévu pour les tests et la maintenance, ou ajouté de manière malveillante a posteriori, et qui permet le contournement des mécanismes de sécurité.

porte dérobée n. f.
trappe n. f.
porte dissimulée n. f.

anglais

backdoor
trapdoor
manhole

---

128. posture en matière de sécurité

Définition

Situation générale d'une organisation en ce qui a trait à la sécurité, tant logicielle que physique, de ses systèmes d'information.

Notes

Une organisation sera en plus ou moins bonne posture pour assurer l'intégrité, la disponibilité et la confidentialité de ses systèmes d'information, selon qu'elle aura adopté une politique de sécurité, qu'elle aura élaboré une stratégie en matière de sécurité et qu'elle aura instauré un ensemble de mesures permettant d'atteindre le niveau de sécurité souhaité.

posture en matière de sécurité n. f.
posture de sécurité n. f.

Pour désigner le présent concept, le terme *posture de sécurité*, calqué sur l'anglais, est acceptable parce qu'il s'intègre au système linguistique du français. En effet, le terme *posture* peut faire référence, en anglais comme en français, à une situation, à une condition particulière dans laquelle se trouve une personne ou une entité représentant un ensemble de personnes. Le complément *de sécurité* est, quant à lui, employé adéquatement au sens de « qui a trait à la sécurité », comme dans les syntagmes *indice de sécurité* ou *politique de sécurité*. Le terme *posture de sécurité* est souvent employé erronément pour désigner un ensemble de dispositifs ou de mécanismes contribuant à la sécurité d'un système d'information, pour désigner un indice ou un niveau de sécurité ou encore une approche adoptée en matière de sécurité. Dans ces cas, il conviendra d'employer des expressions appropriées et précises telles que *dispositif de sécurité*, *indice* ou *niveau de sécurité*, ou encore *stratégie de sécurité*.

anglais

security posture
security stance

---

129. pot de miel

Définition

Système ou réseau informatique volontairement vulnérable et faisant office de leurre, destiné à attirer les pirates informatiques afin d'analyser leurs méthodes d'attaque, de les identifier ainsi que de les détourner des ressources informatiques réelles.

Notes

Les communications établies avec un pot de miel sont considérées comme suspectes puisque les utilisateurs légitimes n'ont aucune raison d'y accéder.

pot de miel n. m.
piège à pirates n. m.
piège à pirate n. m.

L'expression *pot de miel* suggère l'idée d'un appât (comme le miel servant à attirer les ours), utilisé pour piéger les pirates et permettre de les observer en pleine action.

anglais

honeypot
honey pot

---

130. preuve à divulgation nulle de connaissance

Définition

Protocole interactif permettant à une entité de prouver à un tiers qu'une proposition est vraie sans toutefois en révéler quoi que ce soit.

Notes

Par exemple, une entreprise d'audit pourrait avoir recours à la preuve à divulgation nulle de connaissance afin d'évaluer la santé financière d'une entreprise, lors d'une acquisition, sans que cette dernière ait à transmettre des informations sensibles.

La preuve à divulgation nulle de connaissance est notamment utilisée en cryptographie, en assurance ainsi que pour la cryptomonnaie.

preuve à divulgation nulle de connaissance n. f.

anglais

zero-knowledge proof
ZKP
zero-knowledge protocol
ZKP

131. prime de bogues

Définition
Récompense, généralement pécuniaire, remise par une organisation à une personne qui détecte un bogue ou une vulnérabilité informatique dans l'un de ses produits.

Notes
L'offre de primes de bogues est une forme d'externalisation ouverte. Le montant de la prime est souvent fixé selon la gravité de la menace relevée.

✓ **prime de bogues** n. f.
prime aux bogues n. f.

✗ **bug bounty**

L'emploi du terme *bug bounty* est déconseillé parce qu'il a été emprunté à l'anglais depuis peu de temps et qu'il ne s'intègre pas au système linguistique du français. En effet, si l'emprunt *bogue* est acceptable et répandu en français (avec sa graphie adaptée), ce n'est pas le cas de *bounty*.

anglais
bug bounty

---

132. principe de privilège minimal

Définition
Principe selon lequel un compte utilisateur ne doit avoir que les droits d'accès nécessaires à la réalisation de ses tâches.

✓ **principe de privilège minimal** n. m.
principe de droit d'accès minimal n. m.
principe de moindre privilège n. m.
principe du moindre privilège n. m.

anglais
principle of least privilege
POLP
least privilege access

---

133. privilège d'accès

Définition
Droit d'accès particulier généralement réservé à des entités ayant la responsabilité de la protection et de la gestion des systèmes d'information.

Notes
Le privilège d'accès peut être accordé à une personne, comme l'administrateur de système, afin qu'elle travaille à maintenir la sécurité des données et la confidentialité des informations.

privilège d'accès n. m.

anglais

access privilege

---

134. programme de correction

Définition

Programme qui applique un correctif à un logiciel afin d'y corriger une erreur, un dysfonctionnement, ou d'en effectuer une mise à jour.

programme de correction n. m.
correcteur n. m.

anglais

patcher program
patch program

---

135. protection autonome d'application

Définition

Ensemble des techniques visant à protéger un logiciel d'application contre les environnements d'exécution non sécurisés et les vulnérabilités logicielles en rendant le code plus résistant aux intrusions, aux altérations ainsi qu'à l'ingénierie inverse.

Notes

Le brouillage et le chiffrement sont des exemples de protection autonome d'application.

protection autonome d'application n. f.

Le terme *protection autonome d'application* a été proposé par l'Office québécois de la langue française en 2019 pour désigner ce concept.

anglais

application shielding
binary protection

---

136. protocole de sécurité

Définition

Protocole de communication qui permet l'échange de données chiffrées au cours d'une liaison sécurisée.

Notes

Les protocoles TLS, HTTPS et WPA3 sont des exemples de protocoles de sécurité.

protocole de sécurité n. m.

anglais

security protocol

---

137. protocole TLS

Définition

Protocole utilisant des algorithmes de chiffrement pour assurer l'authenticité et la confidentialité des échanges de données, le plus souvent sur le Web.

Notes

Le protocole TLS est une technologie qui a remplacé le protocole SSL dans les serveurs sécurisés. On constate cependant que le terme *protocole SSL* est parfois utilisé pour désigner la nouvelle technologie.

protocole TLS n. m.
protocole de sécurité de la couche transport n. m.
protocole de sécurité de la couche de transport n. m.

Le sigle *TLS*, pour *transport layer security*, est acceptable en français parce qu'il désigne une technologie qui fait office de standard international dans le domaine de la sécurité informatique. Il est parfois employé seul (*le TLS*).

anglais

Transport Layer Security protocol
TLS protocol
TLS

---

138. publicité malveillante

Définition

Publicité en ligne infectée par un logiciel malveillant.

Notes

Si certaines catégories de sites Web semblent plus propices à contenir des publicités malveillantes, ces dernières peuvent également se trouver sur des sites qui semblent dignes de confiance, ou encore dans les espaces publicitaires des moteurs de recherche.

publicité malveillante n. f.

anglais

malicious advertisement
malvertisement
malicious ad

---

139. reconnaissance faciale

Définition

Méthode d'identification biométrique reposant sur l'analyse des principales caractéristiques physionomiques du visage à partir de photos ou de vidéos.

Notes
Les logiciels de reconnaissance faciale fonctionnent à partir de l'analyse de caractéristiques physionomiques telles que la distance entre les yeux, la taille de la bouche, la forme des oreilles, l'angle du menton et la longueur du nez.

La reconnaissance faciale est le plus souvent utilisée pour déverrouiller un appareil informatique, mais elle a également plusieurs autres applications, notamment en vidéosurveillance, en domotique, en intelligence artificielle, en marketing ainsi que sur les réseaux sociaux.

reconnaissance faciale n. f.

anglais
facial recognition

---

140. redondance

Définition
Duplication d'information ou de matériel essentiel en vue de pallier une éventuelle défaillance et d'assurer la continuité du fonctionnement d'un service ou d'un système.

Notes
La redondance en sécurité informatique peut s'appliquer aussi bien à un centre informatique qu'à des éléments d'information, à du matériel, à des installations de sécurité, à des procédures et aux éléments vitaux d'un système informatique.

redondance n. f.

anglais
redundancy
computer redundancy

---

141. refus d'accès

Définition
Fait pour un système informatique de refuser à une entité l'accès à des données.

Notes
Généralement, une entité se voit refuser un accès lorsque la procédure d'authentification n'a pas été respectée (par exemple, champ de données resté vide, échec du test captcha) ou lorsqu'un identifiant ou un authentifiant ne correspond pas à la valeur de référence dans le système.

refus d'accès n. m.

anglais
denial of access
acces denial

142. renseignements personnels

Définition
Renseignements propres à une personne physique, qui permettent de l'identifier directement ou indirectement.

Notes
Le renseignement personnel correspond par exemple à un nom, une adresse physique ou électronique, un numéro de téléphone, une date de naissance, un numéro d'assurance sociale, une plaque d'immatriculation, des photos, des empreintes digitales, un appel passé sur un téléphone intelligent, une connexion à Internet, un historique médical, des transactions financières, etc.

Un individu peut être identifié directement, à l'aide d'un renseignement personnel concret comme son nom, ou indirectement en établissant son profil, à l'aide d'un renseignement personnel plus abstrait comme un critère socioéconomique, psychologique ou idéologique.

renseignements personnels n. m. pl.
données personnelles n. f. pl.
données à caractère personnel n. f. pl.
DCP n. f. pl.

informations personnelles identifiables n. f. pl.

Certains pays ou organismes internationaux établissent une distinction entre les termes *renseignements personnels* et *informations personnelles identifiables*, dans laquelle le second renvoie spécifiquement à de l'information qui permet d'identifier directement un individu. Cette distinction ne se reflète cependant pas dans la législation canadienne où l'on n'emploie que *renseignements personnels,* que l'information permette d'identifier directement ou indirectement un individu.

anglais

personal information
sensitive personal information
SPI
personal data
personally identifiable information
PII

Certains pays ou organismes internationaux établissent une distinction entre les termes *personal information* et *personally identifiable information,* dans laquelle le second renvoie à de l'information qui permet d'identifier directement un individu. Cette distinction ne se reflète cependant pas dans la législation canadienne où l'on n'emploie que *personal information,* que l'information permette d'identifier directement ou indirectement un individu.

---

143. reprise sur sinistre

Définition
Reprise des activités informatiques d'une organisation à la suite d'un sinistre informatique les ayant dégradées ou en ayant entraîné l'interruption.

reprise sur sinistre n. f.
reprise après sinistre n. f.
RS n. f.
rétablissement après catastrophe n. m.
RC n. m.
reprise après catastrophe n. f.
RC n. f.

anglais

disaster recovery
DR

---

144. réseau d'ordinateurs zombies

Définition

Réseau d'ordinateurs infectés par un logiciel malveillant, qui est utilisé afin de mener des cyberattaques coordonnées et anonymes à l'insu des utilisateurs.

Notes

Contrôlés à distance, les ordinateurs zombies du réseau peuvent par exemple mener une attaque par déni de service distribué.

réseau d'ordinateurs zombies n. m.
réseau de zombies n. m.
réseau zombie n. m.

anglais

botnet
zombie network
zombie army
zombie net
robot network

Le terme *botnet* est formé à partir de *robot* et de *network*.

---

145. réseau privé virtuel

Définition

Canal de communication privé dont les extrémités sont mutuellement authentifiées, utilisant l'infrastructure d'un réseau public, le plus souvent Internet, afin de transmettre des données protégées grâce à l'utilisation de techniques de chiffrement.

Notes

Les réseaux privés virtuels sont par exemple utilisés pour le télétravail ou pour relier des bureaux distants par Internet afin de transmettre des informations confidentielles.

réseau privé virtuel n. m.
RPV n. m.
réseau virtuel privé n. m.
RVP n. m.

En France, les termes *réseau privé virtuel* et *RPV* sont recommandés officiellement par la Commission d'enrichissement de la langue française, depuis 2006.

anglais

virtual private network
VPN

146. responsable de la sécurité de l'information

Définition
Personne qui, dans une entreprise ou un organisme, est chargée de la gestion et de la coordination de tous les aspects de la sécurité de l'information, principalement numérique.

Notes
Dans la plupart des cas, le responsable de la sécurité de l'information fait partie de l'équipe de cadres supérieurs. Son rôle consiste notamment à mettre au point, à appliquer et à communiquer les politiques et directives concernant la sécurité de l'information, à assurer la sécurité de systèmes d'information et à gérer les éventuelles situations d'urgence. Souvent, il supervise une équipe d'experts et fournit des conseils, de l'aide, des renseignements et de la formation à toutes les personnes touchées par la sécurité de l'information.

responsable de la sécurité de l'information
n. m. ou f.
RSI n. m. ou f.
directeur de la sécurité de l'information
n. m.
DSI n. m.
directrice de la sécurité de l'information
n. f.
DSI n. f.

anglais
chief information security officer
CISO

---

147. risque informatique

Définition
Probabilité plus ou moins grande de voir une menace informatique se transformer en événement réel entraînant une perte.

Notes
Les risques informatiques peuvent être d'origine naturelle ou humaine, accidentelle ou intentionnelle.

risque informatique n. m.
risque n. m.

anglais
information technology risk
IT risk
computer security risk
computer risk
risk
electronic data processing risk désuet
EDP-risk désuet

148. sauvegarde de données

Définition
Opération qui consiste à copier, généralement sur un support informatique externe, les données mises en mémoire afin de permettre leur restauration en cas de suppression ou de corruption.

Notes
La sauvegarde informatique s'effectue le plus souvent sur un support informatique tel qu'un disque optique, une clé USB ou un disque dur externe, et parfois sur une partition.

sauvegarde de données n. f.
sauvegarde informatique n. f.
sauvegarde n. f.

anglais
backup
data backup

---

149. schéma de déverrouillage

Définition
Authentifiant prenant la forme d'un schéma tracé à l'écran et permettant d'accéder au contenu et aux fonctions d'un appareil électronique.

Notes
L'authentification par un schéma de déverrouillage est souvent utilisée sur une tablette électronique ou sur un téléphone cellulaire, par exemple.

Le schéma est généralement tracé en reliant entre eux des points disposés de la même façon que les chiffres d'un pavé numérique.

schéma de déverrouillage n. m.
motif de déverrouillage n. m.
schéma de verrouillage n. m.
motif de verrouillage n. m.

Le schéma de déverrouillage est utile au propriétaire de l'appareil pour le déverrouiller, mais il est sous-entendu que cela implique une fonction de verrouillage. C'est pourquoi les termes formés avec *déverrouillage* et avec *verrouillage* sont acceptables.

anglais
pattern lock
lock pattern
pattern code
unlock pattern

---

150. sécurisation des données

Définition
Ensemble de méthodes et de techniques visant à améliorer la sécurité des données afin d'éviter leur manipulation par des personnes non autorisées, leur perte ou leur détérioration accidentelle ou intentionnelle.

Notes
L'authentification, le chiffrement, l'automatisation des sauvegardes de données et les signatures numériques font partie des méthodes et techniques de sécurisation des données, notamment dans le contexte du commerce électronique.

sécurisation des données n. f.

anglais
data securisation
data securization
data securement

---

151. sécurisation dès la conception

Définition
Approche de la conception logicielle dans laquelle les questions relatives à la sécurité informatique sont abordées dès les premières étapes du cycle de vie du développement logiciel.

Notes
Dans cette approche, le recours au principe de privilège minimal ou à la revue de code est planifié en amont du processus de conception, plutôt qu'en aval.

sécurisation dès la conception n. f.

anglais
security by design
SbD
secure by design

---

152. sécurité de l'information

Définition
Ensemble de mesures mises en place pour assurer la protection des informations selon le niveau de confidentialité, d'intégrité et de disponibilité jugé nécessaire.

Notes
La sécurité informatique constitue un aspect important de la sécurité de l'information.

sécurité de l'information n. f.

anglais
information security
informational security

153. sécurité des terminaux

Définition
Ensemble de solutions informatiques implanté sur les terminaux pouvant se connecter à un réseau local via Internet, afin de le protéger des intrusions.

Notes
Les logiciels antivirus, les anti-logiciels malveillants et les pare-feu font partie des solutions de sécurité des terminaux.

sécurité des terminaux n. f.
protection des terminaux n. f.

sécurité des points d'extrémité
protection des points finaux
protection des points d'extrémité
sécurité des points finaux

Les calques *sécurité des points d'extrémité*, *protection des points d'extrémité*, *sécurité des points finaux* et *protection des points finaux* sont déconseillés parce qu'ils ne s'intègrent pas au système linguistique du français. En effet, si le terme anglais *endpoint* désigne un appareil relié à un réseau de communication, utilisé pour recevoir ou envoyer des données, ce n'est pas le cas des syntagmes *points d'extrémité* et *points finaux,* qui sont par ailleurs peu fréquents en français.

anglais
endpoint security
endpoint protection

---

154. sécurité informatique

Définition
Ensemble de mesures de sécurité mises en place en vue d'assurer la protection des biens informatiques et des ressources informationnelles qu'ils contiennent.

Notes
Les mesures peuvent découler de la sécurité physique, de la sécurité logique ou de la sécurité administrative, par exemple.

sécurité informatique n. f.
sécurité des systèmes d'information n. f.
SSI n. f.
sécurité des systèmes informatiques n. f.
SSI n. f.

anglais
information technology security
IT security
computer security
computer systems security
information systems security

155. sécurité Internet

Définition
Ensemble des mesures de sécurité informatique appliquées aux données qui passent par le réseau Internet.

sécurité Internet n. f.
cybersécurité n. f.
sécurité en ligne n. f.

anglais
Internet security
cybersecurity
online security

---

156. sécurité logique

Définition
Ensemble des procédures et des moyens logiciels permettant d'assurer la confidentialité, la disponibilité et l'intégrité des données et des opérations informatiques.

sécurité logique n. f.
sécurité logicielle n. f.

anglais
logical security

---

157. sécurité physique

Définition
Ensemble des procédures et des moyens physiques permettant d'assurer la protection du matériel informatique et de son environnement contre toute forme de menace, accidentelle ou volontaire.

Notes
La sécurité physique concerne aussi bien le centre informatique et son périmètre que le matériel de servitude (alimentation électrique, climatisation, aération, etc.) et l'équipement informatique (écrans, serveurs, ordinateurs, etc.).

sécurité physique n. f.

anglais
physical security

---

158. serveur mandataire

Définition
Serveur faisant office d'intermédiaire entre un réseau local et d'autres serveurs, généralement des serveurs Web, permettant ainsi à des données de sortir du réseau local et d'y entrer, sans mettre en danger la sécurité du réseau.

Notes
Un serveur cache est un type de serveur mandataire.

serveur mandataire n. m. recommandé par l'OQLF
mandataire n. m.

En France, les termes *serveur mandataire* et *mandataire* sont recommandés officiellement par la Commission d'enrichissement de la langue française, depuis 1999.

En contexte, la forme courte *mandataire* est fréquemment employée pour désigner le présent concept.

serveur proxy
proxy

Le terme anglais *proxy* vient du latin *procuratio*, qui veut dire « procuration ». C'est sous l'influence de l'anglais que les termes *serveur proxy* et *proxy* sont utilisés en français. Ces termes sont toutefois déconseillés, car l'emploi de *proxy* n'est pas légitimé dans l'usage en français au Québec. Par ailleurs, il fait l'objet de critiques dans la plupart des ouvrages de langue générale.

anglais
proxy server
proxy

---

159. serveur mandataire d'application

Définition
Serveur mandataire destiné à servir d'intermédiaire pour une application en particulier, ou un ensemble d'applications, le plus souvent sur Internet.

serveur mandataire d'application n. m.
serveur mandataire applicatif n. m.
mandataire d'application n. m.
mandataire applicatif n. m.

proxy d'application
proxy applicatif

Le terme anglais *proxy* vient du latin *procuratio*, qui veut dire « procuration ». C'est sous l'influence de l'anglais que les termes *proxy d'application* et *proxy applicatif* sont utilisés en français. Ces termes sont toutefois déconseillés, car l'emploi de *proxy* n'est pas légitimé dans l'usage en français au Québec; il fait l'objet de critiques dans la plupart des ouvrages de langue générale.

anglais
application proxy server
application proxy

---

160. serveur sécurisé

Définition
Serveur qui permet, grâce au chiffrement, d'assurer la confidentialité et la sécurité des informations qui y transitent.

Notes
Les serveurs sécurisés s'appuient sur un protocole qui assure la sécurisation des échanges d'informations, tel le protocole TLS. Ils sont notamment utilisés pour les transactions financières et commerciales sur le Web.

serveur sécurisé n. m.	S'il est utile de préciser qu'il s'agit d'un serveur Web ou d'un serveur Internet, on emploiera les termes *serveur Web sécurisé* ou *serveur Internet sécurisé*.

anglais
secure server
secured server

---

161. service de non-répudiation

Définition
Service fournissant la preuve qu'une personne ou une entité a reçu ou émis un message, ou qu'une action ou une transaction a eu lieu.

Notes
La preuve, généralement basée sur une signature unique ainsi que sur l'horodatage, permet notamment à une organisation de se prémunir contre les utilisateurs de mauvaise foi qui auraient envoyé ou reçu un message et affirmeraient le contraire, ou de déterminer la cause d'un évènement néfaste.

service de non-répudiation n. m. **non-répudiation** n. f.	Le terme *non-répudiation*, qui, dans son sens premier, désigne l'impossibilité de nier avoir reçu ou émis un message, en est venu à désigner le service ou la fonction capable d'apporter cette preuve d'émission ou de réception grâce à laquelle la répudiation devient impossible.

anglais
non-repudiation service
non-repudiation

---

162. signature électronique

Définition
Acte par lequel une personne exprime son consentement à l'égard d'un document à l'aide d'un moyen électronique.

Notes
Par extension, le terme *signature électronique* désigne également la preuve numérique de ce consentement.

Les moyens utilisés pour une signature électronique peuvent notamment être : une signature manuscrite numérisée, une case à cocher dans un courriel sécurisé ou un numéro d'identification personnel.

Au Québec, tout moyen établissant un lien entre un individu et un document a la même valeur juridique qu'une signature manuscrite sur un document papier; ainsi une signature électronique satisfait aux exigences du Code civil du Québec.

On distingue la signature électronique de la signature numérique, qui correspond plutôt à un procédé cryptographique de vérification de l'identité de l'expéditeur et d'assurance de l'intégrité des données d'un document.

signature électronique n. f. recommandé par l'OQLF

e-signature

L'emprunt intégral *e-signature* (*e* pour *electronic*) est déconseillé. En effet, *électronique* ne peut être abrégé en *e-*, comme c'est le cas pour l'anglais *electronic*. En outre, en français, les éléments qui caractérisent un nom sont le plus souvent postposés à celui-ci. Voir, à ce sujet, la recommandation générale d'usage *Équivalents français à donner au préfixe anglais* e-.

anglais

electronic signature
e-signature

---

163. signature numérique (1)

Définition

Procédé cryptographique par lequel un bloc de données généralement chiffrées à l'aide d'un algorithme à clé publique est joint à un document électronique afin d'identifier son expéditeur, d'assurer l'intégrité des données et d'en garantir la non-répudiation.

Notes

On distingue la signature numérique de la signature électronique, qui est l'acte par lequel une personne exprime son consentement à l'aide d'un moyen électronique.

signature numérique n. f. recommandé par l'OQLF

signature digitale

Le terme *signature digitale* est un calque de l'anglais. En français, l'adjectif *digital* signifie « relatif aux doigts », alors que l'anglais *digital* vient de *digit*, qui veut dire « nombre », et se traduit en français par *numérique*. Voir, à ce sujet, l'article *Emploi déconseillé de l'emprunt* digital de la *Banque de dépannage linguistique*.

anglais

digital signature

---

164. signature numérique (2)

Définition

Résultat du procédé cryptographique de vérification de l'authenticité du signataire et d'assurance de l'intégrité et de la non-répudiation des données d'un document, qui constitue une preuve de consentement.

signature numérique n. f. recommandé par l'OQLF
signature électronique cryptée n. f.
signature cryptographique n. f.

anglais

digital signature
encrypted electronic signature
encrypted e-signature

---

165. sinistre informatique

Définition

Événement grave d'origine naturelle ou humaine, accidentelle ou intentionnelle, occasionnant des pertes et des dommages importants aux systèmes informatiques d'une organisation ou d'un individu.

Notes

Les sinistres informatiques se déclinent en sinistre matériel et sinistre immatériel.

sinistre informatique n. m.	Le terme *sinistre*, dans *sinistre informatique*, revêt un sens technique. Il réfère à un événement catastrophique pouvant être couvert par une assurance.
désastre informatique	Le terme *désastre informatique*, calqué sur l'anglais *computer disaster*, est déconseillé parce que son sens ne correspond pas à celui du concept à l'étude. En effet, un désastre informatique est généralement entendu comme un raté lié à la mise sur pied d'un système informatique ou à l'implantation d'un programme.

anglais

computer disaster
IT disaster
disaster

---

166. site sécurisé

Définition

Site Web doté d'un protocole de sécurité, qui permet, grâce au chiffrement des données, d'assurer la confidentialité des informations qui y transitent.

Notes

On reconnaît souvent un site sécurisé à la présence d'une image de cadenas fermé près de la barre d'adresse. De plus, l'adresse URL d'un site sécurisé commence habituellement par *https* au lieu de *http*.

Les sites Web permettant d'effectuer des transactions commerciales ou financières sont généralement des sites sécurisés.

site sécurisé n. m.
site Web sécurisé n. m.

anglais

secure site
secure website
secured site

---

167. surchiffrement

Définition
Procédé cryptographique qui consiste à chiffrer une donnée à plusieurs reprises, généralement en utilisant différentes clés cryptographiques ou différents algorithmes de chiffrement.

Notes
Lorsqu'une donnée est chiffrée à deux reprises, on parle plus précisément de double chiffrement.

surchiffrement n. m.
chiffrement multiple n. m.

anglais
multiple encryption
multiple encipherment
superencryption
superencipherment
cascade encryption
cascade ciphering

---

168. système cryptographique

Définition
Ensemble d'instruments, de documents et de techniques associées permettant le chiffrement et le déchiffrement des données selon un algorithme de chiffrement particulier.

Notes
De façon générale, un système cryptographique est satisfaisant, pour une application donnée, s'il répond à trois conditions fondamentales : la simplicité du chiffrement et du déchiffrement; la difficulté d'utilisation des clés de chiffrement pour les non-initiés; l'absence de liens entre la confidentialité de l'algorithme de chiffrement et le chiffrement lui-même.

système cryptographique n. m.
système de cryptographie n. m.
cryptosystème n. m.
système de chiffrement n. m.
système de cryptage n. m.

anglais
cryptography system
cryptographic system
cryptosystem
cipher system

---

169. système cryptographique à clé publique

Définition
Système cryptographique faisant appel à une biclé pour le chiffrement et le déchiffrement d'un message.

système cryptographique à clé publique n. m.
système cryptographique asymétrique n. m.
cryptosystème à clé publique n. m.
cryptosystème asymétrique n. m.
système à clé publique n. m.
système asymétrique n. m.

L'emploi de la graphie *clef* est en régression. De ce fait, les termes construits avec *clef* sont beaucoup moins répandus en cryptographie que ceux construits avec *clé*.

On trouve également les termes *système cryptographique à clés publiques*, *cryptosystème à clés publiques*, *système à clés publiques* et *système à deux clés*.

anglais

public-key cryptographic system
asymmetric cryptosystem
public-key cryptosystem
public-key system
two-key cryptosystem
two-key system

On trouve également les termes *two-key cryptographic system*, *asymmetric system*, *asymmetric-key system*, *asymmetric cryptographic system*, *asymmetric-key cryptographic system* et *asymmetric-key cryptosystem*.

---

170. système cryptographique à clé secrète

Définition

Système cryptographique qui fait appel à une clé secrète pour le chiffrement et le déchiffrement d'un message.

système cryptographique à clé secrète n. m.
système cryptographique symétrique n. m.
système cryptographique à clé unique n. m.
cryptosystème à clé secrète n. m.
cryptosystème symétrique n. m.
cryptosystème à clé unique n. m.

L'emploi de la graphie *clef* est en régression. De ce fait, les termes construits avec *clef* sont beaucoup moins répandus en cryptographie que ceux construits avec *clé*.

On trouve également les termes *système à clé secrète*, *système à clé symétrique*, *système à clé unique*, *système symétrique*, *système cryptographique à clé symétrique* et *cryptosystème à clé symétrique*.

anglais

secret-key cryptographic system
symmetric cryptosystem
secret-key cryptosystem
single-key cryptosystem
secret-key system
single-key system

On trouve également les termes *single-key cryptographic system*, *symmetric cryptographic system*, *symmetric-key cryptosystem*, *one-key system*, *one-key cryptosystem* et *symmetric-key system*.

---

171. système d'authentification biométrique

Définition

Système permettant de vérifier, par la captation d'une donnée biométrique, l'identité d'une personne.

Notes

Les systèmes d'authentification biométrique comportent notamment un dispositif servant à mesurer un attribut biométrique (par exemple l'empreinte digitale, l'iris ou la voix) et une base de données de référence.

système d'authentification biométrique n. m.
système d'identification biométrique n. m.
système de contrôle d'accès biométrique n. m.

En sécurité informatique, l'identification et l'authentification sont deux concepts différents. Toutefois, dans le cas de la biométrique, l'identification et l'authentification se confondent pour ainsi dire, puisque la personne décline son identité en présentant un caractère biométrique qui lui est unique, et donc qui l'authentifie en même temps qu'il l'identifie. C'est pourquoi le terme *système d'identification biométrique* est un synonyme acceptable de *système d'authentification biométrique*.

anglais

biometric authentication system
biometric identification system
biometric access control system

---

172. système de détection d'intrusion

Définition

Système combinant logiciel et matériel, qui permet de détecter en temps réel les tentatives d'intrusion sur un réseau interne ou sur un ordinateur hôte afin d'en alerter les administrateurs.

Notes

Deux méthodes sont principalement utilisées par les systèmes de détection d'intrusion : la reconnaissance de signatures et la détection d'anomalies. La reconnaissance de signatures est une approche consistant à rechercher dans l'activité de l'élément surveillé les signatures (ou empreintes) d'attaques connues. Pour sa part, la détection d'anomalies se fait grâce à l'analyse de statistiques du système : changement de mémoire, utilisation excessive de l'unité centrale, etc.

système de détection d'intrusion n. m.
SDI n. m.
système de détection d'intrusions n. m.
SDI n. m.
système de détection des intrusions n. m.
SDI n. m.
système IDS n. m.
IDS n. m.

L'emprunt intégral à l'anglais *IDS* (*intrusion detection system*) est acceptable parce que son usage est bien établi dans le domaine spécialisé de la sécurité informatique.

anglais

intrusion detection system
IDS
IDS system

---

173. tatouage numérique (1)

Définition

Technique de marquage qui consiste à insérer une signature permanente à l'intérieur de documents numériques, généralement des fichiers audiovisuels, afin de lutter contre la fraude et le piratage et d'assurer la protection des droits de propriété intellectuelle.

Notes
Le tatouage numérique permet notamment de garantir la preuve de paternité d'une œuvre numérique et de dissuader les pirates dans la mesure où la signature peut être retrouvée dans chaque copie de l'image originellement marquée.

Le tatouage numérique est parfois visible (un logo, par exemple) et parfois invisible (ou inaudible, dans le cas des fichiers audio).

tatouage numérique n. m.
marquage numérique n. m.
filigranage numérique n. m.

anglais
digital watermarking

---

174. tatouage numérique (2)

Définition
Données constituant une marque permanente insérée par tatouage numérique dans un document, permettant notamment d'en garantir la paternité et de lutter contre le piratage.

Notes
Le tatouage numérique peut être perceptible ou non, en fonction de la nature et de l'intention du détenteur des droits de propriété intellectuelle d'un document électronique.

Le tatouage numérique est conçu de manière à ce qu'une modification au document n'altère pas sa fonction.

tatouage numérique n. m.
filigrane numérique n. m.
marque numérique n. f.

Les termes *tatouage*, *filigrane* et *marque* s'emploient en contexte pour désigner le présent concept.

anglais
digital watermark
forensic watermark
watermark

---

175. test à données aléatoires

Définition
Test fonctionnel qui a pour objectif de déceler d'éventuelles défaillances informatiques, en entrant aléatoirement des données, notamment à l'intérieur d'un champ.

Notes
On utilise le test à données aléatoires pour, par exemple, repérer des bogues simples ou des vulnérabilités informatiques. Par ailleurs, on peut faire passer ce test manuellement ou automatiquement à l'aide d'un logiciel.

test à données aléatoires n. m.

anglais

fuzzing
fuzz testing

---

176. test captcha

Définition

Programme qui protège les sites Web et les applications contre les robots logiciels en générant des tests qui ne peuvent être accomplis que par des humains.

Notes

Un test captcha consiste notamment dans l'identification de lettres et de chiffres visibles sur une image distordue ou dans la sélection, dans une série de photos, de celles sur lesquelles figure un objet donné.

test captcha n. m.
captcha n. m.

Les emprunts *test captcha* et *captcha* sont acceptables parce qu'ils s'inscrivent dans la norme sociolinguistique du français au Québec. En outre, *captcha* est également employé dans plusieurs autres langues.

En France, le terme *test captcha* est recommandé officiellement par la Commission d'enrichissement de la langue française, depuis 2013.

Au pluriel, on écrira : *des tests captchas*, *des captchas*.

anglais

captcha test
captcha

Le terme *captcha* est l'acronyme de *completely automated public turing test to tell computers and humans apart*.

---

177. test d'intrusion

Définition

Test visant à reproduire de manière contrôlée les conditions réelles d'une attaque sur un réseau ou un système d'information afin de détecter les failles de sécurité et d'évaluer leur exploitabilité en vue de les corriger.

Notes

Les tests d'intrusion peuvent être effectués depuis l'intérieur du système d'information ou du réseau testé, ou depuis l'extérieur.

test d'intrusion n. m.
test de pénétration n. m.
essai de pénétration n. m.

anglais

intrusion test
penetration test
pentest
pen test
ethical hacking

178. texte en clair

Définition
Données textuelles intelligibles pouvant être exploitées sans recours au déchiffrement, généralement destinées à être expédiées ou stockées.

texte en clair n. m.
texte clair n. m.

La locution *en clair* est employée de la même façon dans des termes comme *données en clair*, *message en clair* ou *éléments d'information en clair*.

anglais
cleartext

Bien que le terme *plaintext* soit parfois employé pour désigner le présent concept, il s'agit plutôt d'un équivalent du terme *texte brut*.

---

179. tunnellisation partagée

Définition
Tunnellisation permettant l'utilisation de deux tunnels, l'un à destination d'un réseau privé, sécurisé grâce au chiffrement des données, et l'autre, sans protection particulière, généralement destiné au réseau Internet.

Notes
La tunnellisation partagée permet de réduire la quantité des données transmises par le biais du réseau privé, en améliorant ainsi les performances, mais peut par ailleurs augmenter les risques de cyberattaque.

tunnellisation partagée n. f.
tunnellisation fractionnée n. f.

anglais
split tunneling
split tunnelling

---

180. usurpation d'adresse IP

Définition
Fraude par laquelle un pirate informatique remplace son adresse IP par celle d'un tiers, à des fins malveillantes.

Notes
L'usurpation d'adresse IP est notamment utilisée afin de garder l'anonymat lors d'une action malveillante, d'accéder frauduleusement à un réseau informatique ou de perpétrer une attaque par déni de service distribué.

usurpation d'adresse IP n. f.

anglais
IP spoofing
IP address spoofing
Internet protocol spoofing

181. usurpation de carte SIM

Définition
Fraude par laquelle une personne se fait passer pour le titulaire d'une ligne de téléphonie mobile auprès de son opérateur dans le but de s'approprier son numéro de téléphone en se faisant remettre une nouvelle carte SIM.

Notes
L'usurpation de carte SIM permet aux fraudeurs de contourner l'authentification à deux facteurs reposant sur la messagerie texto et de prendre le contrôle de comptes en ligne, ouvrant ainsi la porte à plusieurs types d'escroqueries telles que l'usurpation d'identité, le chantage et le vol d'argent.

usurpation de carte SIM n. f.

anglais
SIM swapping
SIM swap
SIM splitting
simjacking
port-out scam

Les termes *SIM swapping*, *SIM swap* et *SIM splitting* peuvent être suivis des noms *fraud*, *scam*, *attack* ou *scheme*.

---

182. usurpation d'identité

Définition
Fraude qui consiste à usurper l'identité d'un utilisateur en s'appropriant son identifiant ainsi que les authentifiants qui y sont associés, généralement dans le but d'obtenir des informations sensibles ou de se livrer à des opérations non autorisées.

usurpation d'identité n. f.
mascarade n. f.

anglais
identity theft
impersonation
masquerading

---

183. ver informatique

Définition
Logiciel malveillant, autonome et parasite, capable de se reproduire par lui-même.

Notes
À la différence des virus informatiques, les vers informatiques n'ont pas besoin d'un programme hôte pour se reproduire. Autonomes, ils se déplacent dans la mémoire d'ordinateur, qu'ils surchargent et minent progressivement, consommant, parfois jusqu'à la paralysie, les ressources du système informatique.

Les vers informatiques se déclinent notamment en ver de station de travail et en ver de réseau.

ver informatique n. m.
ver n. m.

En France, le terme *ver* est recommandé officiellement par la Commission d'enrichissement de la langue française, depuis 2005.

anglais

worm

---

184. virus informatique

Définition

Logiciel malveillant le plus souvent transmis par un réseau ou un support de stockage externe, ayant pour but d'infecter un fichier qui, lorsqu'il est exécuté, lui permettra de se propager et de produire les effets pour lesquels il a été conçu.

Notes

Un virus informatique peut comporter, par exemple, une bombe logique.

virus informatique n. m.
virus n. m.

En France, le terme *virus* est recommandé officiellement par la Commission d'enrichissement de la langue française, depuis 2005.

anglais

computer virus
virus

---

185. virus polymorphe

Définition

Virus informatique capable de se modifier lui-même, au fur et à mesure qu'il se propage, afin d'éviter la détection en présentant une apparence différente après chaque reproduction.

Notes

Il est possible de détecter les virus polymorphes grâce à l'analyse heuristique.

virus polymorphe n. m.
virus polymorphique n. m.

anglais

polymorphic virus
polymorphic computer virus

---

186. vulnérabilité informatique

Définition

Faiblesse d'un système informatique se traduisant par une incapacité partielle de celui-ci à faire face aux attaques ou aux intrusions informatiques.

Notes

Les systèmes informatiques sont tous, à des degrés divers, vulnérables aux événements, accidentels ou frauduleux, qui peuvent nuire à leur fonctionnement, provoquer leur détérioration ou leur destruction, ou permettre la violation des données qui s'y trouvent stockées.

L'évaluation de la vulnérabilité d'un système, l'analyse des causes de menaces informatiques et la mise en place des contre-mesures de sécurité informatique appropriées permettent d'atteindre un seuil minimal de vulnérabilité, désigné habituellement par le terme vulnérabilité résiduelle.

Il est courant, pour le propriétaire d'un système informatique, de concevoir et de publier un programme de correction permettant d'empêcher l'exploitation du système, dès lors qu'une vulnérabilité est décelée.

vulnérabilité informatique n. f.
vulnérabilité n. f.
défaut de sécurité n. m.
faille de sécurité informatique n. f.
faille n. f.

anglais

security vulnerability
vulnerability
security flaw
security exploit
exploit

---

187. vulnérabilité logicielle

Définition

Vulnérabilité informatique causée par une défaillance dans la conception ou le fonctionnement d'un logiciel.

Notes

En règle générale, les développeurs de logiciels proposent rapidement un programme de correction sous forme de mise à jour après la découverte d'une vulnérabilité logicielle.

vulnérabilité logicielle n. f.
faille logicielle n. f.

anglais

software vulnerability
software flaw
software exploit

---

188. vulnérabilité matérielle

Définition

Vulnérabilité informatique causée par une défaillance dans la conception ou le fonctionnement d'un composant matériel.

Notes

Les solutions aux vulnérabilités matérielles sont généralement difficiles à trouver et à mettre en œuvre, et influencent négativement les performances du système.

vulnérabilité matérielle n. f.
faille matérielle n. f.

anglais

hardware vulnerability
hardware flaw
hardware exploit

VOCABULAIRE DE LA SÉCURITÉ INFORMATIQUE

Pour accéder à l'ensemble des vocabulaires de l'Office québécois de la langue française :
oqlf.gouv.qc.ca/ressources/bibliotheque/dictionnaires/index_lexvoc.html.

Pour connaître les outils et les services linguistiques de l'Office :
vitrinelinguistique.oqlf.gouv.qc.ca/a-propos-de-la-vitrine-linguistique/offre-de-services-linguistiques.

Pour consulter les ressources de la Vitrine linguistique :
vitrinelinguistique.oqlf.gouv.qc.ca.

Pour visiter le site de l'Office :
oqlf.gouv.qc.ca/accueil.aspx.

Office québécois de la langue française
Québec