# Lexique de la Cybersécurité

## Antivirus

Un logiciel qui protège votre ordinateur en détectant et supprimant les programmes nuisibles, comme les virus et les logiciels malveillants.

## Application

Un programme informatique conçu pour effectuer des tâches spécifiques, comme les jeux, les réseaux sociaux ou la gestion des emails.

## Authentification

Le processus de vérification de l’identité d’un utilisateur, généralement à l’aide d’un nom d’utilisateur et d’un mot de passe.

## Biométrie

L’utilisation de caractéristiques physiques, comme les empreintes digitales ou la reconnaissance faciale, pour identifier et authentifier les utilisateurs.

## Brute force

Une méthode où les hackers essaient toutes les combinaisons possibles pour trouver un mot de passe.

## Chiffrement

Technique de sécurisation des données en les transformant en un code illisible sauf si on connait une clé de déchiffrement correspondante.

## ChatGPT

Un modèle informatique capable de comprendre et générer du texte en langage naturel, développé par OpenAI.

## Cheval de Troie

Des logiciels malveillants qui semblent inoffensifs mais exécutent des actions malveillantes une fois installés.

## Cloud

Un service en ligne qui permet de stocker et d’accéder à des fichiers via Internet plutôt que sur un disque dur local.

## Code PIN

Un numéro secret utilisé pour vérifier votre identité, souvent associé à des cartes bancaires ou des appareils électroniques.

## Compte

Un ensemble d’informations personnelles et d’autorisations associées à un utilisateur dans un système informatique.

## Consentement éclairé

Accord explicite donné par un individu après avoir été informé de manière transparente sur l’utilisation de ses données personnelles.

## Cookies

De petits fichiers texte stockés par votre navigateur, contenant des informations sur vos habitudes de navigation en ligne.

## Cyberharcèlement

L’utilisation d’Internet pour harceler, menacer ou intimider une personne.

## Cyberprédateur

Une personne utilisant Internet pour cibler et exploiter des individus vulnérables, en particulier des mineurs.

## Dark web

Une partie d’Internet inaccessible aux moteurs de recherche conventionnels, souvent associée à des activités illégales.

## Défaçage

Modifier le contenu d’un site web, parfois dans un but malveillant, pour afficher un message indésirable.

## Déni de service

Une attaque visant à rendre un service indisponible en inondant le serveur ou le réseau avec un trafic excessif.

## Données

Informations stockées, traitées et utilisées par des systèmes informatiques.

## Données personnelles

Informations qui permettent d’identifier une personne, comme le nom, l’adresse, le numéro de téléphone, etc.

## Double authentification

Un mécanisme de sécurité exigeant deux formes d’identification différentes pour accéder à un compte ou un système.

## Droit à l’oubli

Droit permettant à un individu de demander la suppression de ses données personnelles, notamment sur Internet.

## Fake news

Informations fausses ou trompeuses présentées comme des faits réels, généralement diffusées sur Internet.

## Faire chanter

Menacer de divulguer des informations compromettantes pour obtenir un avantage, souvent sous la forme d’argent.

## Firewall personnel

Un logiciel ou un dispositif matériel qui surveille et contrôle le trafic entrant et sortant d’un réseau personnel, renforçant la sécurité.

## Gestionnaire de mots de passe

Un outil facilitant la gestion et la sécurisation des mots de passe en les stockant de manière chiffrée.

## Hackeur

Une personne utilisant ses compétences techniques pour accéder à des systèmes informatiques de manière non autorisée.

## Héberger des données

Stocker des informations sur un serveur accessible via Internet.

## Historique

La liste des sites web visités et des actions effectuées sur un navigateur web.

## Ingénierie sociale

L’utilisation de tactiques psychologiques pour manipuler les individus et les inciter à divulguer des informations confidentielles.

## Injection SQL

Insérer du code SQL malveillant dans une requête pour accéder, modifier ou supprimer des données dans une base de données.

## IP (Adresse IP)

Une série unique de chiffres attribuée à chaque appareil connecté à un réseau, permettant de l’identifier.

## Journalisation

L’enregistrement systématique d’événements, d’activités ou de connexions, souvent utilisé pour l’analyse de sécurité.

## Keylogger

Un type de logiciel malveillant qui enregistre les frappes sur un clavier, permettant à un attaquant de capturer des informations sensibles telles que des mots de passe.

## Malvertising

La diffusion de publicités en ligne malveillantes contenant des logiciels malveillants ou des liens vers des sites dangereux.

## Malware

Logiciels malveillants conçus pour endommager, accéder ou perturber un système informatique.

## Man in the middle (homme du milieu)

Une attaque qui consiste à intercepter voire modifier les communications entre deux parties sans leur consentement.

## Patch

Une mise à jour logicielle destinée à corriger des vulnérabilités de sécurité ou à améliorer les performances d’un programme.

## Pare-feu applicatif (WAF)

Un pare-feu spécifiquement conçu pour protéger les applications web contre les attaques, telles que l’injection de code.

## Pharming

Une attaque visant à rediriger les utilisateurs vers de faux sites web, souvent dans le but de collecter des informations sensibles.

## Phishing

Une technique d’escroquerie en ligne visant à tromper les gens pour obtenir leurs informations personnelles.

## Proxy

Un serveur intermédiaire utilisé pour filtrer les requêtes web et améliorer l’anonymat en cachant l’adresse IP réelle de l’utilisateur.

## QR Code (Code QR)

Un code-barres bidimensionnel qui peut stocker des informations, souvent utilisé pour accéder à des sites web ou partager des informations rapidement.

## Ransomware

Un type de malware qui chiffre les fichiers d’un utilisateur, exigeant le paiement d’une rançon pour les débloquer.

## RGPD

Règlement de l’Union européenne sur la protection des données personnelles et la vie privée entré en vigueur en mai 2018.

## Risque cyber

Évaluation combinée de la probabilité d’être victime d’une cyberattaque et de l’ampleur des dommages ou pertes potentiels.

## Sauvegarde

Une copie de données importantes effectuée pour prévenir la perte en cas de défaillance du système.

## Script kiddie

Un individu qui utilise des outils et des scripts développés par d’autres, sans avoir de connaissances approfondies en programmation, pour mener des attaques.

## Sécurité physique

Les mesures de sécurité visant à protéger le matériel informatique et les données.

## Spam

Des messages électroniques non sollicités et indésirables envoyés en masse, souvent à des fins publicitaires ou malveillantes.

## Spear Phishing

Une forme de phishing ciblée sur des individus spécifiques.

## Spoofing

Une attaque qui consiste à usurper l’identité numérique de quelqu’un.

## URL

Uniform Resource Locator, l’adresse spécifique qui identifie une ressource sur Internet.

## Usurper l’identité

Faire semblant d’être quelqu’un d’autre en ligne.

## Virus

Un programme informatique malveillant capable de se reproduire et d’infecter d’autres programmes ou fichiers.

## VPN

Un réseau privé virtuel garantissant la confidentialité et la sécurité des données en les transmettant de manière chiffrée.

## Vulnérabilité Zero-day

Une faille de sécurité qui est exploitée avant qu’un correctif ne soit disponible.

## Wifi public

Un réseau sans fil accessible au public.

## Worm (Ver informatique)

Un type de logiciel malveillant qui se propage automatiquement d’un ordinateur à un autre.

## Zero Trust

Un modèle de sécurité qui n’accorde aucune confiance implicite, même aux utilisateurs internes.