CYBERDÉFI 1

Antivirus

CYBERDÉFI 2

Application

CYBERDÉFI 3

Authentification

CYBERDÉFI 4

Biométrie

CYBERDÉFI 5

Brute force

CYBERDÉFI 6

Chiffrement

CYBERDÉFI 7

ChatGPT

CYBERDÉFI 8

Cheval de Troie

CYBERDÉFI 9

Cloud

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.

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

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

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

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

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

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

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

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

CYBERDÉFI 10

Code PIN

CYBERDÉFI 11

Compte

CYBERDÉFI 12

Consentement éclairé

CYBERDÉFI 13

Cookies

CYBERDÉFI 14

Cyberharcèlement

CYBERDÉFI 15

Cyberprédateur

CYBERDÉFI 16

Dark web

CYBERDÉFI 17

Défaçage

CYBERDÉFI 18

Déni de service

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

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

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

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

L'utilisation d'Internet pour harceler, menacer ou intimider une personne.
Une personne utilisant Internet pour cibler et exploiter des individus vulnérables, en particulier des mineurs.

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

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

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

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

CYBERDÉFI 19

Données

CYBERDÉFI 20

Données personnelles

CYBERDÉFI 21

Double authentification

CYBERDÉFI 22

Droit à l'oubli

CYBERDÉFI 23

Fake news

CYBERDÉFI 24

Faire chanter

CYBERDÉFI 25

Firewall personnel

CYBERDÉFI 26

Gestionnaire de mots de passe

CYBERDÉFI 27

Hackeur

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

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

Informations stockées, traitées et utilisées par des systèmes informatiques.

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

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

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

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

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

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

CYBERDÉFI 28

Héberger des données

CYBERDÉFI 29

Historique

CYBERDÉFI 30

Ingénierie sociale

CYBERDÉFI 31

Injection SQL

CYBERDÉFI 32

IP (Adresse IP)

CYBERDÉFI 33

Journalisation

CYBERDÉFI 34

Keylogger

CYBERDÉFI 35

Malvertising

CYBERDÉFI 36

Malware

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

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

Stocker des informations sur un serveur accessible via Internet.

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

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

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

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

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

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

CYBERDÉFI 37

Man in the middle

CYBERDÉFI 38

Patch

CYBERDÉFI 39

Pare-feu applicatif

CYBERDÉFI 40

Pharming

CYBERDÉFI 41

Phishing

CYBERDÉFI 42

Proxy

CYBERDÉFI 43

QR Code

CYBERDÉFI 44

Ransomware

CYBERDÉFI 45

RGPD

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

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

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

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

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

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

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

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

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

CYBERDÉFI 46

Risque cyber

CYBERDÉFI 47

Sauvegarde

CYBERDÉFI 48

Script kiddie

CYBERDÉFI 49

Sécurité physique

CYBERDÉFI 50

Spam

CYBERDÉFI 51

Spear Phishing

CYBERDÉFI 52

Spoofing

CYBERDÉFI 53

URL

CYBERDÉFI 54

Usurper l'identité

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

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

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

Une forme de phishing ciblée sur des individus spécifiques.

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

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

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

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

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

CYBERDÉFI 55

Virus

CYBERDÉFI 56

VPN

CYBERDÉFI 57

Vulnérabilité Zero-day

CYBERDÉFI 58

Wifi public

CYBERDÉFI 59

Worm (Ver informatique)

CYBERDÉFI 60

Zero Trust

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

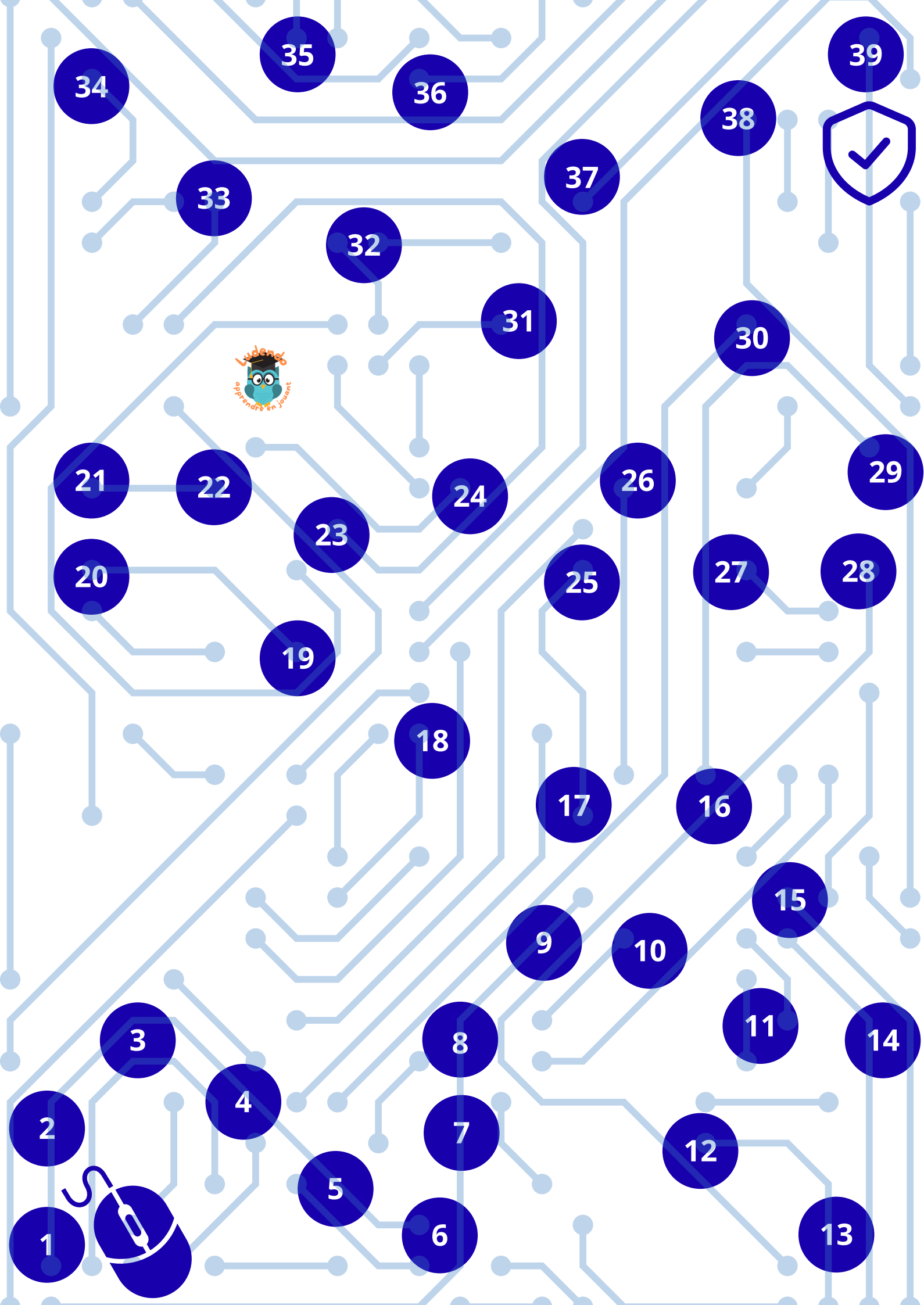
Un réseau privé virtuel garantissant la confidentialité et la sécurité des données en les transmettant de manière chiffrée.

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

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

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

Un réseau sans fil accessible au public.


1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39

Cyberdéfis

Matériel :

Le plateau de jeu, les pions pour la variante avancée
Les cartes avec les mots à définir (recto pour la version simple)
La correction

Déroulement

Objectifs pédagogiques :

- Connaître le vocabulaire clé de la cybersécurité
- Comprendre les concepts associés (attaques, protection, prévention)
- Sensibiliser aux risques numériques

Règle du jeu (version de base) :
But :
Associer correctement les cartes "Mot-clé" et "Définition".
Mise en place :

- Mélanger les deux types de cartes.
- Distribuer 5 cartes "Mot-clé" par joueur.
- Placer les cartes "Définition" en tas, face cachée.

Déroulement :

- Un joueur pioche une carte "Définition" et la lit à voix haute.
- Chaque joueur regarde ses cartes "Mot-clé" pour voir s'il possède la bonne réponse.
- Celui qui a la bonne carte la pose. Il gagne 1 point.
- Si personne n'a la bonne carte, la définition est remise en jeu.
- Le premier à 5 points gagne.

Variante « Avancée » : CyberQuiz

- version avec plateau de jeu, pions à avancer avec les définitions à donner pour chaque mot pioché au hasard