JOURNAL DE MISSION

10-14 ANS

TON PRÉNOM DE CYBEREXPERT·E

EURO SPACE CENTER

MISSION

OPÉRATION CYBER ESPACE

Salut à toi, CyberExpert·e !

Tu viens d'effectuer la mission "Opération Cyber Espace" : les astronautes à bord de l'ISS et les satellites gérés par l'ESA sont maintenant en sécurité.

BRAVO pour tout ce que vous avez fait, ton équipe et toi !

Il est l'heure d'en apprendre plus sur la cybersécurité.
Dans ton journal de mission, tu vas trouver toutes les informations nécessaires pour devenir un·e véritable CyberExpert·e. Tu vas tout comprendre grâce à des comparaisons super simples ! Tu verras comment on se protège des attaques, ce que font les pros de la cybersécurité contre les différents types d'attaques qui existent. Et si tu rencontres un mot bizarre que tu ne connais pas (et que ce mot est souligné), pas de panique, va jeter un œil à la section "Vocabulaire de CyberExpert·es" pour tout savoir.

Bonne lecture !

En français, on utilise le masculin pour parler de tout le monde. Mais ici, pour respecter l'égalité entre filles et garçons, on va alterner les mots féminins et masculins. Parfois, on va même utiliser le point médian " . " pour mettre les deux formes en même temps.

C'EST QUOI L'ESA ?

L'Agence Spatiale Européenne est une organisation qui rassemble des expert·es de différents pays européens pour explorer l'espace. Leur mission est de développer les capacités spatiales de l'Europe et de s'assurer que tout le monde profite des avancées technologiques et scientifiques obtenues grâce à leurs travaux. L'ESA, c'est une grande équipe qui construit des fusées, envoie des satellites pour surveiller la Terre (météo, télécommunication, etc.), envoie des sondes explorer Mars, ou encore envoie des astronautes à la Station Spatiale Internationale (ISS). Ils étudient aussi les planètes, les étoiles et l'univers pour mieux les comprendre. Avec 22 pays membres qui partagent leurs compétences et leurs ressources, l'ESA peut réaliser des projets ambitieux et complexes, bien au-delà de ce qu'un seul pays pourrait faire seul.

C'EST QUOI L'ISS ?

La Station Spatiale Internationale est la plus grande station qui tourne autour de la Terre à environ 400 km de hauteur. Elle a été construite directement dans l'espace à partir de 1998. En 2024, elle mesure 110 mètres de long et 74 mètres de large, à peu près la taille d'un terrain de football. Depuis l'an 2000, des astronautes de différents pays y vivent en permanence, jour et nuit. Ces astronautes se relaient pour faire des expériences et découvrir de nouvelles choses sur l'espace. Par exemple, iels étudient comment les plantes poussent sans gravité, comment le corps humain réagit à de longs séjours dans l'espace, et même comment créer de nouveaux matériaux. Leurs découvertes aident à améliorer la vie sur Terre, comme en développant de nouveaux médicaments ou en apprenant à fabriquer des objets plus résistants.

↪ Une petite info amusante : l'ISS fait le tour de la Terre en seulement 92 minutes, à une vitesse de 27 600 km/h. Chaque jour, les astronautes voient environ 16 levers et couchers de soleil !

Photo : Crédit ESA/NASA

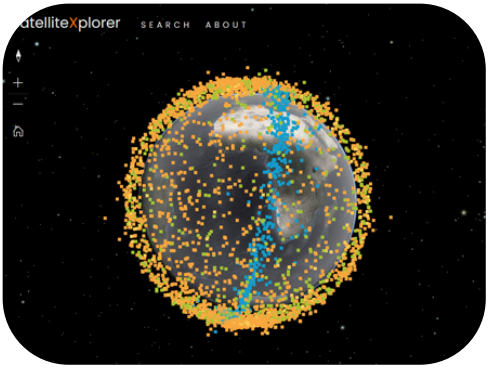
Ceci est une photo de l'astronaute de l'ESA, Samantha Cristoforetti, observant l'espace depuis la coupole de la station ISS.
Samantha est devenue en 2022 la première femme européenne commandante de l'ISS.

DÉBRIS SPATIAUX ET POLLUTION SPATIALE

En 2013, le film Gravity, réalisé par Alfonso Cuarón, est le premier film de fiction à aborder le problème des débris spatiaux. L'histoire suit les astronautes Ryan et Matt, en danger après que leur navette a été endommagée par des débris flottants dans l'espace.

Chaque année, de plus en plus de satellites sont envoyés dans l'espace. Beaucoup de ces satellites deviennent inutiles après un certain temps et se transforment en débris spatiaux.
Ces débris flottent autour de la Terre, créant une pollution spatiale, et peuvent entrer en collision avec d'autres débris ou des satellites. Lors de ces collisions, les objets se cassent en petits morceaux, créant encore plus de débris.

Cela rend l'espace autour de la Terre très encombré et dangereux. Ce problème est appelé le syndrome de Kessler, du nom du scientifique américain Donald Kessler qui a décrit ce phénomène en 1978. Selon Kessler, si la quantité de débris spatiaux dépasse un certain seuil, certaines orbites pourraient devenir trop dangereuses pour les satellites et les missions spatiales.
Cette prédiction scientifique a inspiré la cyberattaque la plus dangereuse du jeu "Opération Cyber Espace" : le "Chaos Orbital".



Tu as envie de visualiser les orbites des satellites ou les débris spatiaux ? C'est possible grâce à l'outil SatelliteXplorer, disponible à l'adresse suivante : bit.ly/4hCWQNn ou via le QR code

C'est quoi
LA CYBERSÉCURITÉ ?

Est-ce que tu aimerais que des personnes entrent chez toi pour voler tes affaires préférées ? Bien sûr que non ! C'est pourquoi ta famille et toi prenez des mesures pour protéger votre maison. Eh bien, c'est pareil pour les systèmes informatiques (les ordinateurs-matériels et les programmes-logiciels) : ils doivent être protégés contre les hackeurs et hackeuses qui essaient d'y entrer sans permission. Toutes les actions qu'on fait pour les protéger s'appellent la cybersécurité.

Pour t'aider à mieux comprendre, voici des exemples de protections pour les systèmes informatiques, comparés à des choses que tu pourrais faire pour sécuriser ta maison. Il y a évidemment plein d'autres exemples possibles, n'hésite pas à relire les cartes cyberdéfense pour trouver des idées 😉

SYSTÈMES INFORMATIQUES	MAISON
Pour protéger tes comptes en ligne et tes informations personnelles, tu dois inventer des mots de passe forts que les hackeurs n'arriveront pas à deviner.	**C'est comme si tu installais une serrure robuste sur la porte de ta maison pour empêcher les voleurs d'entrer.**
Tu peux activer l'authentification à deux facteurs sur tes comptes en ligne : cela ajoute une étape supplémentaire de vérification pour confirmer ton identité avant d'accéder à tes comptes.	**C'est comme si tu vérifiais l'identité des invitées avant de les laisser entrer dans ta maison.**
Pour empêcher les hackeuses d'introduire un programme malveillant sur ton ordinateur ou ta tablette, tu peux installer un antivirus qui détecte les menaces avant qu'elles ne causent des dégâts.	**C'est comme si tu installais un système d'alarme qui déclenche une alerte si une personne essaie de pénétrer dans la maison sans autorisation.**
Pour éviter que quelqu'un ne se fasse passer pour toi, tu dois faire attention à qui tu divulgues tes informations personnelles, par exemple ton numéro de téléphone ou ton adresse.	**C'est comme si tu donnais aux voleurs le code de l'alarme de ta maison et que tu leur indiquais exactement où sont cachés tes objets préférés. Il ne faut pas leur faciliter le travail !**
De nombreux systèmes de messagerie chiffrent les conversations en les transformant en un code illisible sans la clé de déchiffrage appropriée.	**C'est comme si tu utilisais un coffre-fort (dont le voleur ne connaît pas le code) pour protéger les objets de valeur.**

Une recette
EN CINQ ÉTAPES

Pour aider les gens à protéger leurs ordinateurs et leurs informations, l'Institut National des Normes et de la Technologie (NIST) a créé une sorte de plan d'action pour la cybersécurité. Ce plan comprend cinq étapes importantes pour rendre les systèmes plus sûrs.

En reprenant l'exemple de la protection de ta maison, cela donne :

Ces cinq actions forment un cycle, ce qui signifie qu'on les répète encore et encore pour garder les systèmes toujours protégés.

Actions
DES CYBEREXPERT·ES

Dans le jeu, les cinq actions du cadre NIST sont chacune représentées par une équipe. Les cinq équipes travaillent ensemble pour empêcher les cyberattaques visant les systèmes informatiques de l'ESA. Chaque équipe a des tâches spécifiques à accomplir (illustrée ci-dessous par des cartes cyberdéfense). Bien que le jeu ne démontre pas toujours comment les compétences des équipes sont directement liées à la protection contre les cyberattaques, ces connexions existent dans la réalité.

IDENTIFIER

Cette action vise à comprendre ce dont une organisation, telle que L'ESA, a besoin pour se protéger et protéger ses systèmes informatiques. Cela implique d'identifier les failles de sécurité dans les systèmes et de repérer les menaces les plus à risques. Cette action est préventive et aide à anticiper les cybermenaces avant qu'elles ne se transforment en cyberattaques.

PROTÉGER

Après l'identification des failles et des menaces, il faut mettre en place des mesures pour protéger les systèmes informatiques de l'organisation. Cela comprend à la fois des protections informatiques sur des objets connectés ou des protections physiques sur les infrastructures (cadenas, système d'identification par badges, barrières de sécurité, etc.).

DÉTECTER

La troisième action consiste à détecter les cybermenaces, ou les cyberattaques si elles ont déjà commencé. Il est important de repérer rapidement si quelqu'un essaie de s'introduire dans les systèmes informatiques, avant que la menace ne se transforme en attaque réelle.

RÉAGIR

Lorsqu'une cyberattaque est détectée, il est crucial de réagir rapidement pour la stopper et réduire les dommages. Une équipe se réunit alors immédiatement pour élaborer un plan d'action afin de gérer l'attaque de manière efficace.

RESTAURER

La dernière action est de restaurer les systèmes informatiques après une cyberattaque. Cela signifie réparer et remettre en marche les éléments qui ont été affectés par l'attaque pour réduire les dégâts.

Dans le cas où l'ESA ferait appel à toi et ton équipe de CyberExpert·es pour protéger ses données importantes, le plan d'action pourrait être le suivant :

- D'abord, l'équipe des **CyberInspecteur·rices** identifie quelles sont les données importantes car ce sont ces données auxquelles il faudra faire le plus attention.
- Une fois que les données importantes sont identifiées, l'équipe des **CyberGuardien·nes** protège ces données en créant un mot de passe fort que les hackeuses ne pourront pas trouver.
- Lorsqu'un hackeur essaie de s'introduire dans les systèmes informatiques pour voler les données importantes, l'équipe des **CyberChasseur·euses de menaces** détecte son activité suspecte et lance l'alarme.
- L'équipe des **CyberUrgentistes** doit alors réagir très vite pour contrer l'attaque et faire en sorte que le hackeur ne puisse pas voler les données importantes. Pour cela, elle va bloquer l'accès aux données importantes en changeant en urgence tous les mots de passe qui les protègent et va limiter la propagation des dégâts.
- Si malheureusement, le hackeur a réussi à voler ou à chiffrer certaines données, l'équipe des **CyberDocteur·esses** essaiera de restaurer ces données grâce à d'anciennes sauvegardes saines et utilisera des systèmes auxiliaires le temps de la restauration.

Mais ce n'est pas tout à fait comme ça que cela se passe dans la réalité.
En effet, il est rare que les professionnel·les de la cybersécurité se concentrent uniquement sur une seule action. Souvent, une personne dans ce domaine doit gérer plusieurs actions en même temps !

"En tant qu'avocate, je représente les personnes qui sont victimes de cybercriminalité. Mais je défends également les personnes accusées d'avoir commis un crime dans le cyberespace".

Lou, avocate

"Mon travail consiste à diriger et à soutenir les différentes équipes de cybersécurité afin de m'assurer qu'elles agissent ensemble. Une équipe doit être plus forte et plus performante que la somme de ses membres individuels".

Richard, responsable de la sécurité informatique

"Je soutiens les responsables du CERT (Computer Emergency and Response Team) et du CSOC (CyberSecurity Operation Center) dans leurs tâches de gestion. Je participe aussi à l'achat des outils de sécurité nécessaires à nos équipes. ".

Bastien, expert junior en cybersécurité

"Je veille à ce que toutes les informations critiques contenues dans nos systèmes soient protégées. Je dirige une équipe qui surveille en permanence toute activité suspecte et réagit rapidement pour prévenir et atténuer les cyberattaques".

Sergio, responsable des opération du CSOC

"J'aide les entreprises à sécuriser leurs systèmes en accord avec leurs objectifs. Mon rôle consiste à définir avec précision leurs besoins en sécurité et à proposer des solutions sur mesure pour les protéger efficacement contre les menaces. ".

Manel, consultante en cybersécurité

Quel·le CyberExpert·e ES-TU ?

En fonction de tes talents et de ta personnalité, quel(s) métier(s) en cybersécurité te conviendrait le mieux ?

Remplis les cases comme suit :

- Ça ne te correspond pas du tout = 1
- Ça t'arrive de temps en temps = 2
- Ça te correspond parfaitement = 3

CyberInspecteur·ice

Quand tu es dans un pièce, tu repères rapidement des endroits spéciaux où tu pourrais cacher tes objets préférés. →

Tu te souviens facilement où tu as rangé tes affaires. →

Tu aimes connaître les secrets de tes ami·es ou de ta famille. →

Total :

CyberGardien·ne

Tu aimes construire des cabanes avec des couvertures, des branches, etc. →

Tu prends soin de tes jouets pour qu'ils ne soient pas abimés. →

Tu gardes tes affaires importantes dans un endroit secret. →

Total :

CyberChasseur·euse de menaces

Tu es doué·e pour trouver des indices dans une chasse aux trésors. →

Quand tu joues à cache-cache, tu préfères essayer de trouver où se cachent les autres. →

Tu repères rapidement quand on essaie de te faire une blague. →

Total :

CyberUrgentiste

Tu es doué·e dans des exercices où il faut être rapide à répondre. →

Tu aimes aider tes ami·es quand ils ou elles ont besoin d'aide. →

Quand tu as des envahisseurs affamés qui convoitent ton dessert, tu n'hésites pas à le protéger. →

Total :

CyberDocteur·esse

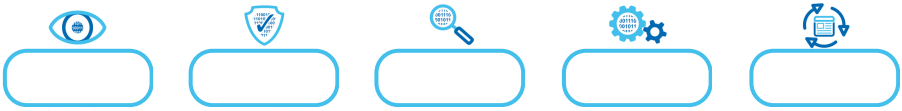
Tu es doué·e pour trouver des solutions quand quelque chose se passe mal. →

Tu aimes réparer des jouets cassés ou des objets abîmés. →

Tu es doué·e pour consoler tes ami·es quand ils ou elles se sentent tristes. →

Total :

Additionne les points pour chaque métiers et répertorie les totaux ci-dessous.
Quel métier a obtenu le meilleur score ?



Bravo ! Tu ferais un·e excellent·e .....

Attention
AUX CYBERATTAQUES

Bien que de nouvelles formes de cyberattaques apparaissent régulièrement, il est possible de classer les attaques les plus courantes en fonction des failles que les hackeurs utilisent pour lancer leurs attaques :

Selon l'Organisation des Nations Unies, une cyberattaque a lieu quelques part sur Terre toutes les 39 secondes environ !

1 L'ATTAQUE PAR INGÉNIERIE SOCIALE

La faille vient de l'humain. Une personne commet une erreur ou divulgue des informations confidentielles, permettant aux hackeuses de pénétrer dans les systèmes informatiques.

2 L'ATTAQUE PAR LOGICIEL

La faille provient d'un logiciel. Les hackeurs exploitent les vulnérabilités d'un logiciel pour accéder aux systèmes informatiques, voler des données ou causer des dommages.

3 L'ATTAQUE PAR RÉSEAU

La faille provient du réseau. Les hackeuses ciblent l'infrastructure de réseau pour interrompre, intercepter ou manipuler les communications entre les systèmes.

As-tu déjà entendu parler de l'une de ces attaques dans les médias ou autour de toi ? Quelqu'un dans ta famille a-t-il été victime de l'une de ces cyberattaques ?

Exemples de cyberattaques

Ingénierie sociale

Attaque par force brute :
Un hackeur essaie de trouver ton mot de passe en utilisant des algorithmes qui testent une grande quantité de combinaison (lettres, chiffres et caractères spéciaux).

Hameçonnage (phishing) :
Une hackeuse rentre en contact (mail, message, appel, etc.) avec toi en se faisant passer pour une personne de confiance afin que tu divulgues des renseignements personnels ou que tu cliques sur un lien frauduleux.

Logiciel

Cheval de Troie :
Un hackeur dissimule un programme malveillant derrière un logiciel inoffensif pour que tu l'installes sur ton ordinateur. Il tente ainsi de perturber le fonctionnement normal de ta machine ou de dérober des informations personnelles qu'elle contient.

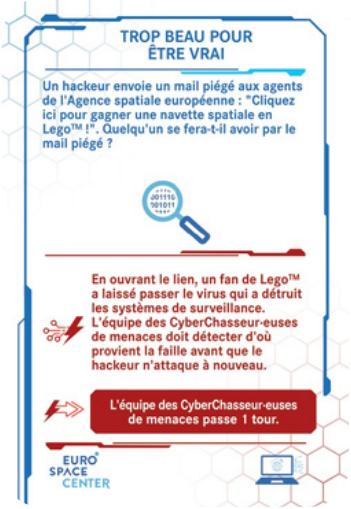
Rançongiciels (ransomware) :
Une hackeuse utilise un logiciel chiffrant certaines de tes données pour en bloquer l'accès. Elle te demande une rançon pour que tu puisses à nouveau y accéder.

Réseau

Man in the middle :
Une hackeuse s'installe au milieu d'une de tes communications ou un de tes transferts de données. Elle peut ainsi en intercepter le contenu.

Attaque par déni de service (DDoS) :
Un hackeur submerge ton système informatique de requêtes dans le but de le ralentir, voire même de le paralyser totalement.

Plus tu connais et reconnais les cyberattaques, mieux tu pourras te protéger contres elles. Pour t'exercer, essaie d'associer ces 4 cartes issues du jeu avec les types d'attaques que tu viens de découvrir !



Vocabulaire
DE CYBEREXPERT·E

ANTIVIRUS

Un antivirus est un programme installé sur les systèmes informatiques qui permet de détecter, bloquer et supprimer les programmes malveillants. Il analyse régulièrement les fichiers et le réseau pour repérer les menaces et les neutraliser avant qu'elles ne causent des dommages.

BLACKOUT

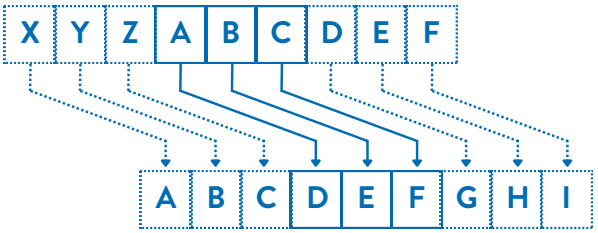
Un blackout est une panne de courant généralisée.

CHEVAL DE TROIE

Un cheval de Troie est un type de programme malveillant d'apparence inoffensive mais qui cache en son sein un comportement anormal. Par exemple, un utilisateur télécharge un jeu gratuit sur Internet et pendant qu'il joue une partie, ses fichiers personnels sont dérobés.

CHIFFREMENT/DÉCHIFFRER

Le chiffrement est un processus qui transforme les données en une forme illisible pour les personnes non autorisées, afin de protéger leur confidentialité (accès limité) et leur intégrité (fiabilité). Cela se fait en utilisant des algorithmes mathématiques. Par exemple, le code César est un chiffrement simple basé sur un décalage de l'alphabet. Si on applique un décalage de trois lettre, chaque lettre du texte d'origine est remplacée par une lettre située trois positions plus loin dans l'alphabet. En utilisant ce chiffrement, le mot "cybersécurité" devient alors "fbehuvhfxulwh". Ce type de chiffrement était utilisé par Jules César pour protéger ses messages secrets. Aujourd'hui, des algorithmes beaucoup plus complexes sont utilisés pour assurer la sécurité des données.



CYBERATTAQUE

Une cyberattaque est une action délibérée et malveillante menée par une hackeuse pour cibler des systèmes informatiques. Elle utilise des failles humaines, logicielles ou dans le réseau pour accéder de manière non autorisées aux données contenues dans ces systèmes.

CYBERMENACE

Une cybermenace désigne toute situation où un hackeur tente d'accéder de manière non autorisée aux données contenues dans des systèmes informatiques. Si cette tentative réussit, elle devient une cyberattaque.

DONNÉES

Les données sont des faits bruts, des chiffres ou des caractères dont le contexte n'est pas précisé. Ce sont des éléments qui, pris seuls, n'ont pas de signification spécifique. Par exemple, 42 000, 23-08 ou 25. Cependant, lorsque ces données sont traitées et interprétées, elles deviennent de l'information utile et significative : 42 000 est un nombre, 23-08 est une date et 25 est température en degrés celsius.

DONNÉES IMPORTANTES

Les données importantes sont liées à des informations qui, si elles étaient compromises ou perdues, pourraient avoir des conséquences négatives, telles que le vol d'argent ou le vol d'identité. Ces données importantes sont par exemple des photos et vidéos personnelles, des communications privées (e-mails, messages), des documents financiers (relevés bancaires, déclaration d'impôts), des documents légaux (contrats, diplômes), des plans stratégiques d'une organisation, des bases de de données clients d'une organisation, etc.

DONNÉES SENSIBLES

Les données sensibles sont un sous-ensemble des données importantes. Elles sont liées à des informations qui doivent être protégées en raison de leur nature personnelle, confidentielle ou délicate. Leur divulgation non autorisée peut entraîner des violations de la vie privée, des fraudes ou d'autres dommages. Par exemple, les numéros de sécurité sociale, les informations de carte de crédit, les dossiers médicaux, les identifiants de connexion, etc.

DOUBLE FACTEUR D'AUTHENTIFICATION (2FA)

Le double facteur d'authentification est une méthode de sécurité renforcée qui protège les systèmes informatiques en demandant deux formes différentes de vérification pour confirmer l'identité d'un utilisateur. Cela signifie que, pour accéder à un compte ou à un système, l'utilisateur doit fournir deux éléments distincts de preuve de son identité. Par exemple, un mot de passe et une empreinte digitale, une carte bancaire (via un lecteur) et un code PIN (numéro d'identification personnel), etc. Cette méthode rend l'accès à un compte plus difficile pour les personnes non autorisées, même si elles connaissent les identifiants de connexion.

FAILLE

Une faille, ou vulnérabilité, est un point faible ou un défaut dans un système informatique. Elle représente une faiblesse qui peut être exploitée par des hackeuses pour causer des dommages, voler des données ou prendre le contrôle du système. Ces failles peuvent se classer en trois grandes catégories : humaines, logicielles ou de réseau.

GÉO-POSITIONNEMENT

Le géo-positionnement est une méthode pour déterminer la position géographique d'un objet, d'une personne ou d'un lieu sur la surface de la Terre. Cette technique utilise diverses méthodes pour obtenir des coordonnées géographiques précises, souvent en terme de latitude, longitude et altitude.

HACKEUR·EUSE

Les hackeur·euses dont des personnes très compétentes en informatique. Ils ou elles utilisent leurs compétences pour explorer et tester les systèmes informatiques de manière créative. Parfois, les hackeur·euses aident à améliorer la sécurité des systèmes en trouvant et en corrigeant des failles. Cependant, ils ou elles peuvent aussi utiliser leurs compétences pour des activités illégales, comme accéder à des systèmes sans autorisation et voler des données (importantes et/ou sensibles) en exploitant des failles de sécurité.

HYGIÈNE INFORMATIQUE

L'hygiène informatique comprend les gestes simples et quotidiens que chacun doit adopter pour protéger ses systèmes informatiques contre les cybermenaces et les cyberattaques. Par exemple, utiliser un antivirus, choisir un bon mot de passe fort, réaliser régulièrement les mises à jour des logiciels, être prudent avec les e-mails et les pièces jointes, etc.

IDENTIFIANTS (DE CONNEXION)

Les identifiants de connexion sont un ensemble d'informations utilisées pour vérifier l'identité d'une utilisatrice lorsqu'elle se connecte à un système informatique. Cela inclut généralement un nom d'utilisateur et un mot de passe, mais peut aussi inclure d'autres éléments comme un code PIN ou un identifiant biométrique (comme une empreinte digitale).

INFORMATION

L'information est le résultat du traitement et de l'analyse des données. C'est lorsque les données sont organisées, interprétées et contextualisées qu'elles deviennent de l'information. L'information a une signification, elle est utile pour prendre des décisions ou pour comprendre quelque chose. Par exemple, "le total des ventes pour le mois de juillet est de 42 000 euros" (donnée brute : 42 000) ou "la température maximale du 23 août est de 25°C" (données brutes : 23-08, 25).

INTELLIGENCE ARTIFICIELLE

L'intelligence artificielle (IA) est une technologie qui permet à des ordinateurs d'exécuter des tâches en suivant des instructions précises. Par exemple, l'IA peut trier des photos, répondre à des questions ou aider à trouver des itinéraires sur une carte. L'IA fonctionne en utilisant les programmes et des données pour résoudre des problèmes ou accomplir des actions de manière automatique.

INTELLIGENCE ARTIFICIELLE GÉNÉRATIVE

L'intelligence artificielle (IA) générative est une technologie qui utilise des modèles mathématiques et des données pour produire du contenu comme des images, du texte ou de la musique. Par exemple, en analysant de nombreux dessins, une IA générative peut créer de nouvelles images ressemblantes, sans intervention humaine directe.

INTERNET

Internet est un réseau mondial qui connecte des millions d'ordinateurs partout dans le monde. Il permet aux gens de communiquer, de partager des données, ou d'accéder à des sites web, des vidéos, des jeux, et bien plus encore.

LOGICIEL

Un logiciel est un ensemble de programmes regroupés pour accomplir une série de tâches. Par exemple, un logiciel de dessin peut contenir plusieurs programmes qui permettent de dessiner, colorier et enregistrer l'image.

MISE À JOUR

Une mise à jour est un processus qui consiste à améliorer ou corriger un logiciel présent sur un système informatique en installant une nouvelle version. Ces mises à jour peuvent ajouter de nouvelles fonctionnalités, améliorer les performances, ou réparer des problèmes de sécurité pour protéger le système contre les menaces/attaques.

MOT DE PASSE FORT/PHRASE DE PASSE

Un mot de passe fort est un mot de passe difficile à deviner ou à craquer par des méthodes comme les attaques par force brute. Pour qu'un mot de passe soit fort, il doit être long (au moins 12 caractères) et contenir des lettres minuscules, des lettres majuscules, des chiffres et des caractères spéciaux. Par exemple, "4jli$oju?A5t" est un mot de passe fort.
Une phrase de passe est un série de mots, de chiffres et de caractères spéciaux formant une phrase pour créer un mot de passe plus long (et donc plus sécurisé), mais surtout plus facile à retenir. Par exemple, "MonCh@tMLe5Po1sson5" est une phrase de passe.

Temps nécessaire à un hackeur pour forcer votre mot de passe en 2023

Nombre de caractères	Seulement des chiffres	Lettres minuscules	Lettres minuscules et majuscules	Chiffres, lettres minuscules et majuscules	Symboles, chiffres, lettres minuscules et majuscules
4	Instantané	Instantané	Instantané	Instantané	Instantané
5	Instantané	Instantané	Instantané	Instantané	Instantané
6	Instantané	Instantané	Instantané	Instantané	Instantané
7	Instantané	Instantané	1 seconde	2 secondes	4 secondes
8	Instantané	Instantané	28 secondes	2 minutes	5 minutes
9	Instantané	3 secondes	24 minutes	2 heures	6 heures
10	Instantané	1 minute	21 heures	5 jours	2 semaines
11	Instantané	32 minutes	1 mois	10 mois	3 ans
12	1 seconde	14 heures	6 ans	53 ans	226 ans
13	5 secondes	2 semaines	332 ans	3.10^3 ans	15.10^3 ans
14	52 secondes	1 an	17.10^3 ans	202.10^3 ans	1.10^6 ans
15	9 minutes	27 ans	898.10^3 ans	12.10^6 ans	77.10^6 ans
16	1 heure	713 ans	46.10^6 ans	779.10^6 ans	5.10^9 ans
17	14 heures	18.10^3 ans	2.10^9 ans	48.10^9 ans	380.10^9 ans
18	6 jours	481.10^3 ans	126.10^9 ans	2.10^{12} ans	26.10^{12} ans

ORDINATEUR

Un ordinateur est une machine électronique qui peut recevoir, traiter, stocker et envoyer des informations. Il peut faire différentes choses en exécutant des programmes, comme écrire des documents, naviguer sur Internet ou encore jouer à des jeux. Une montre connectée, un smartphone et un robot tondeuse sont des exemples d'ordinateur.

ORDINATEUR QUANTIQUE

Un ordinateur quantique est une machine qui effectue des calculs beaucoup plus rapidement et efficacement que les ordinateurs "classiques" pour certains types de problèmes. Par exemple, un ordinateur quantique peut chiffrer les données importantes de manière beaucoup plus complexe pour les sécuriser davantage.

PARE-FEU

Un pare-feu est un dispositif, matériel ou logiciel, qui protège un réseau informatique. Il filtre les communications entre des machines connectées pour autoriser celles qui sont sûres et bloquer celles qui pourraient être dangereuses, agissant comme une barrière.

PROGRAMME

Un programme est un ensemble d'instructions qui dit à l'ordinateur ce qu'il doit faire pour accomplir une tâche précise. C'est comme une recette que l'ordinateur suit pour obtenir un résultat.

PROGRAMME MALVEILLANT

Un programme malveillant est un programme développé pour infiltrer et nuire à un système informatique, sans le consentement de l'utilisatrice. Les programmes malveillants peuvent causer tout un tas de dommages comme le vol ou la suppression des données importantes.

REQUÊTE INFORMATIQUE

Une requête informatique est une demande envoyée à un système informatique pour obtenir des données ou effectuer une tâche spécifique. Par exemple, lorsque vous tapez une question dans un moteur de recherche tel que Google, vous envoyez une requête informatique au serveur de Google. Ce serveur traite votre demande et vous renvoie les données qui répondent à votre question.

RÉSEAU (INFORMATIQUE)

Un réseau informatique est un ensemble d'ordinateurs et autres appareils connectés entre eux notamment pour partager des données et des ressources, comme des disques durs, des serveurs ou encore des imprimantes. Les réseaux peuvent être de différentes tailles, allant de petites réseaux locaux comme ceux dans une maison ou d'une entreprise, à des réseaux étendus qui couvrent des régions entières ou même le monde entier, comme Internet.

ROUTEUR

Un routeur est un appareil permettant la communication entre un réseau local et Internet. Il est la première ligne de sécurité contre l'intrusion dans un réseau.

SAUVEGARDE SAINE

Une sauvegarde saine est la dernière sauvegarde des données qui n'a pas été corrompue par des hackeurs lors d'une cyberattaque. C'est à partir de cette sauvegarde que les experts en cybersécurité vont essayer de restaurer les données.

SERVEUR

Un serveur est un système informatique, généralement un ordinateur robuste et puissant, qui est conçu pour gérer et répondre aux requêtes des utilisatrices ou d'autres systèmes au sein d'un réseau.

SYSTÈME INFORMATIQUE

Un système informatique est un ensemble d'éléments matériels et logiciels avec lesquels l'humain interagir, conçu pour traiter, stocker, gérer et transmettre des informations afin de réaliser des tâches spécifiques et répondre aux besoins des utilisatrices.

TÉLÉCOMMUNICATION

La télécommunication permet d'envoyer et de recevoir des données, comme des voix, des vidéos ou des messages, entre des personnes ou des appareils qui ne sont pas physiquement proches les uns des autres. Cela se fait via des câbles, des ondes radio, des satellites ou d'autres technologies et cela permet d'échanger rapidement et efficacement des informations travers le monde.

VER

Un ver est un logiciel malveillant auto-reproducteur qui, contrairement au virus, n'a pas besoin d'un programme hôte. Le ver est capable de se propager à d'autres systèmes informatiques sans intervention humaine. Par exemple, il peut se reproduire et s'expédier lui-même à tous les contacts du carnet d'adresses électronique.

VIRUS

Le terme "virus" est souvent utilisé à tort pour désigner tout programme malveillant, mais il ne s'agit en réalité que d'une forme spécifique de ce type de programme. Les vers et les chevaux de Troie sont d'autres exemples. Un virus informatique se reproduit en s'intégrant dans des programmes inoffensifs, appelés "hôtes". Il est généralement caché dans un programme et n'infecte le système informatique que lorsque l'utilisateur l'ouvre. Une fois actif, il perturbe le fonctionnement du système, parfois gravement. Le virus est conçu pour se propager à d'autres systèmes via divers moyens de partage de données, comme les réseaux ou les clés USB, souvent sans que l'utilisateur en soit conscient.

WEB

Le Web, ou World Wide Web, est un système d'information mondial qui utilise Internet pour permettre aux utilisatrices de consulter et d'échanger des informations. Il est constitué de sites web accessibles via des navigateurs (tel que Firefox ou Google Chrome), qui permettent d'afficher des pages contenant du texte, des images, des vidéos et d'autres types de contenus.

En savoir plus sur le jeu
ET SES DÉVELOPPEUR·EUSES

Auteur·ices à créditer (par ordre alphabétique) :
Chot Hugo, Dardenne Charline, Henry Julie & Wauthoz Bastien.
Édition : Septembre 2024 (V1)

Le jeu et les ressources associées ont été développés grâce au soutien du Gouvernement wallon via le projet 13 du Plan de Relance de la Wallonie.

Wallonie Relance | Les Talents du futur sont ici !

EURO SPACE CENTER

L'Euro Space Center, ouvert depuis 1991, est un parc à thème éducatif dédié aux sciences spatiales, accueillant plus de 100 000 visiteurs de près de 40 nationalités chaque année. Ce centre propose une immersion captivante dans l'univers de l'espace et des sciences à travers des expositions interactives et des attractions uniques. Que ce soit pour une visite, une journée à thème, un stage de vacances ou une sortie scolaire avec votre classe, l'Euro Space Center promet des expériences inoubliables : Marchez sur la Lune, ressentez l'adrénaline de la chute libre ou simuler un décollage en fusée...

L'Euro Space Center s'engage aussi dans des projets éducatifs innovants, comme "Opération Cyber Espace", qui sensibilise enseignants et élèves aux réalités de la cybersécurité. Ce projet a été coordonné par Caroline Peeters et Bénédicte Joguet, avec Hugo Chot en charge des aspects pédagogiques et du développement du jeu.

EURO SPACE CENTER

DESIGNED BY ACRITARCHE

Designed by Acritarche est un éditeur indépendant de jeux de rôle à Haut Potentiel Ludique : un minimum de blabla pour un maximum de jeu. Il s'est fait remarquer pour “En terres sauvages”, “Impitoyables bourgades”, le “Jeu du destin”, “Sanctuaire” et le “Guide de Dungeon World”. “Horrifique” a été jeu du mois sur le Grog et nominé aux Prix rôliste (meilleur système de jeu et meilleur jeu francophone). Il a été salué tant par le public que par la critique pour son utilisation innovante des aides de jeu.

Bastien Wauthoz, cheville ouvrière de Designed by Acritarche, est un game designer primé pour les “Masques-tombes d'Olinmar” et il a été nominé aux Graals d'or pour “La Laverie”. Il a plus de 30 ans d'expérience en game design et plus de 15 dans l'édition de jeux.

UNIVERSITÉ DE NAMUR

L’Université de Namur (UNamur), fondée en 1831, est une institution universitaire qui accueille plus de 7000 étudiants. Elle propose une vaste gamme de programmes d’études dans des domaines variés tels que les sciences (informatique, chimie, biologie, médecine, etc.), les lettres, le droit, et les sciences économiques .L'UNamur est également active dans la recherche, avec 11 instituts spécialisés. Lors du développement du jeu “Opération Cyber Espace”, Julie Henry et Charline Dardenne étaient chercheuses au sein de l’un d’entre eux : le Namur Digital Institute (NADI). Elles sont les designeuses pédagogiques du jeu et des ressources associées.

NEXOVA GROUP

Nexova est une société belge privée qui combine des solutions d'ingénierie et des services de sécurité pour les infrastructures et opérations critiques à travers l'Europe. Nexova croit à un avenir dans lequel la société pourra exploiter le pouvoir positif de la technologie et de la numérisation.

En tant qu'entreprise européenne dédiée à la cybersécurité, Nexova a pour mission de favoriser la cyber-résilience et la confiance numérique grâce à des services de cybersécurité fiables fournis par des experts hautement qualifiés et des technologies propriétaires avancées. Tirant parti de son expertise unique acquise dans le secteur spatial, Nexova a diversifié diversifié ses services de cybersécurité et propose désormais une gamme complète de solutions offrant une cyber-résilience inégalée pour les environnements les plus complexes et les plus exigeants.

DESIGNED by ACRITARCHE

UNIVERSITÉ DE NAMUR

Nexova

1, rue devant les Hêtres | B-6890 Transinne, Belgique
Tel. : + 32 (0) 61 65 64 65 | Fax : + 32 (0) 61 65 64 61
Mail : info@eurospacecenter.be

www.eurospacecenter.be