863952 - A. S. DE VELAINE EN HAYE

Sensibilisation CyberMalveillance

ACTION

Nom de l'action
Sensibilisation CyberMalveillance

Date de l'action
22/04/2024

Public cible
Famille

Nombre de participants
26

Thème de l'action
Éducatif

Descriptif de l'action
Avec les Jeux Olympiques il faut savoir que le pays hôte devient la pays favoris des hackers, près de 450 millions de cyberattaques ont visé Tokyo en 2021, pour les jeux de Paris les experts s'attendent de huit à dix fois plus t'attaque. L'informatique et l'intelligence artificielle peuvent s'avérer d'excellent outils mais également devenir parfois dangereux. Nous avons sensibilisé nos jeunes à la bonne gestion des mots de passe, les risques des wifi partagés, mais nous avons décidé que cela n'était pas suffisant et nous avons décidé d'organisé une action PEF pour les parents durant laquelle nous reviendrons sur les risques de la cyber malveillance mais également nous expliquerons les bienfaits et méfaits de l'intelligence artificielle notre intervenant sera présent pour répondre à l'ensemble des questions. L'action se déroulera le 22/05/2024. L'action enfants & parents est disponible dans les photos. Actuellement nous avons déjà 26 participants. Afin de rendre disponible les informations nous avons créé une action PEF clé en main de toutes pièces afin de la proposer à d'autres clubs.

Commentaire
Sources utilisés pour le contenu de l'action : https://www.cybermalveillance.gouv.fr/, https://www.prodwaregroup.com/, https://www.cea.fr/

Photo(s)

OBJECTIF DE L'ATELIER

Sensibiliser
&
prévenir les
risques numériques

→ **Espace nécessaire**
1 demi terrain

→ **Encadrement souhaité**
1 éducateur

→ **Effectif idéal**
2 équipes de 4 à 8 joueurs

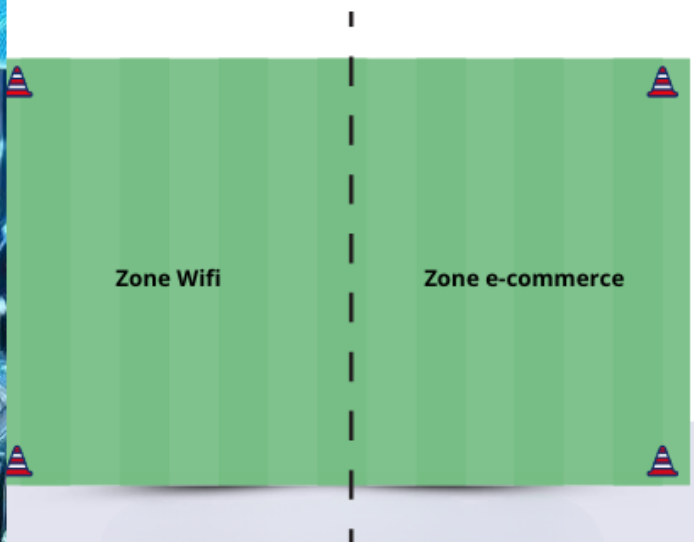
→ **Durée de l'action**
90 mn

→ OBJECTIFS

Adopter les bonnes pratiques & comprendre les risques liés au numérique.

→ MODÉLISATION DE L'ATELIER

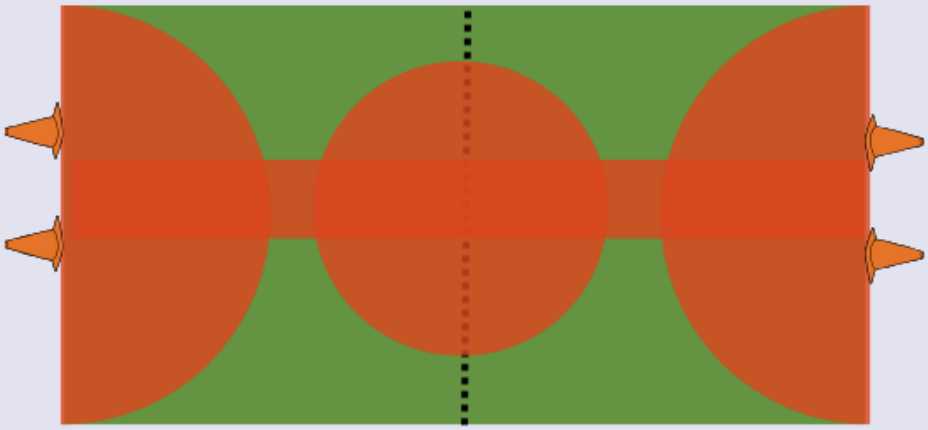
L'éducateur doit être muni d'un stylo et de la liste des participants afin de noter les mots de passe obtenu.



Au début de l'exercice l'éducateur demande à chaque joueur de choisir un mot de passe, en précisant qu'il ne doit le divulguer à personne avant la zone blanche. Dès lors l'objectif de l'éducateur sans que les joueurs le sachent c'est de récupérer un maximum de mots de passe l'équipe qui gagne et l'équipe qui a divulgué le moins de mots de passe.

Zone Wifi

15 mn



But de l'exercice

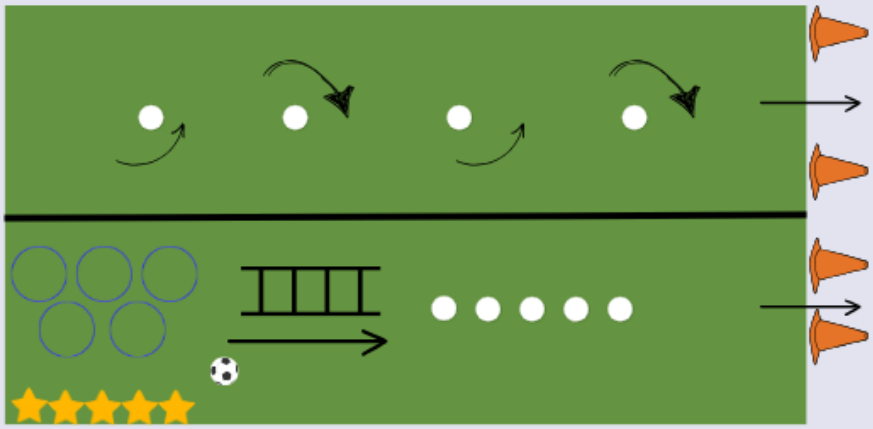
Les deux équipes doivent marquer un maximum de buts.
Par demi terrain, deux zones sont matérialisés une zone Wifi Public (en rouge) et une zone Wifi Privé (en vert), les joueurs s'affrontent en 4x4 ils peuvent marqués d'où ils veulent, mais si un joueur marque depuis la zone Wifi Public, il doit révéler son mot de passe à l'éducateur.

Variantes

L'éducateur peut ajouter des difficultés supplémentaires :
En jouant sur la taille des buts en cours de partie

Zone e-commerce

15 mn



But de l'exercice

Sur un durée de 10 mn, chaque équipe doit marquer un maximum de buts.
Les équipes passent l'une après l'autre, et pour chaque équipe les joueurs passent les uns après les autres. Le joueur effectue son parcours tente la frappe et revient au départ pour toucher son coéquipier qui seulement à ce moment là pourra partir.
Avant de marquer deux parcours de motricité sont proposés, un simple et rapide et un plus long et plus complexe, l'éducateur pourra s'il le souhaite positionner 5 étoiles sur le parcours le plus difficile. Le joueur a le choix soit il choisit le parcours simple mais doit donner son mot de passe à l'équipe adverse soit le parcours compliqué dans ce cas il peut garder son mot de passe secret.

Questionnaires :

15 mn

GÉRER SES MOTS DE PASSE

1/ Bonnes pratiques

Parmi les propositions, quelles sont les deux bonnes pratiques à mettre en œuvre pour assurer la sécurité de vos mots de passe ?

- ☐ **A** Les noter sur un post-it pour s'en souvenir
- ☐ **B** Choisir un mot de passe suffisamment complexe
- ☐ **C** Les confier à un tiers en cas de besoin
- ☐ **D** Utiliser un mot de passe différent pour chaque accès

2/ Vrai ou Faux

J'ai un mot de passe très sécurisé. Je peux donc l'utiliser sur tous mes comptes et services.

☐ **Vrai** ☐ **Faux**

3/ Cherchez l'intrus

Un mot de passe sécurisé :

- ☐ **A** est facile (suite logique, le prénom de mes enfants, ma date de naissance, etc.)
- ☐ **B** comporte 12 caractères mélangeant des majuscules, des minuscules, des chiffres et des caractères spéciaux
- ☐ **C** suit un moyen mnémotechnique

4/ Reliez les situations à leurs solutions

Je ne me souviens jamais de mes mots de passe	A ☐	☐ **1**	Je n'enregistre pas les mots de passe et me déconnecte après utilisation
Je soupçonne qu'un de mes comptes ait été piraté	B ☐	☐ **2**	Je fais confiance à Keepass, mon gestionnaire de mots de passe
Je travaille sur un ordinateur à la bibliothèque	C ☐	☐ **3**	Je change immédiatement de mot de passe

RÉPONSES

1/B et D – Vos mots de passe sont la porte d'entrée de vos appareils numériques et de l'accès à vos comptes, qui peuvent contenir des données sensibles. Protégez vos accès en utilisant un mot de passe complexe et unique pour chaque accès.

2/FAUX – Il vaut mieux utiliser un mot de passe différent et complexe pour chaque accès ou service. En effet, en cas de perte ou de vol d'un de vos mots de passe, vous limitez les risques d'accès frauduleux au seul compte lié à ce mot de passe.

3/A – Un mot de passe trop simple ou facile à deviner n'offre pas un niveau de sécurité suffisant, ce qui pourrait faciliter la tâche des cybercriminels.

4/A – 2 B – 3 C – 1

SÉCURITÉ DES APPAREILS MOBILES

1/ Bonnes pratiques

Parmi les propositions, quelles sont les deux bonnes pratiques à mettre en œuvre pour assurer au mieux la sécurité numérique de vos appareils mobiles ?

- ☐ **A** Je ne fais jamais fonctionner le Wifi et le Bluetooth en même temps
- ☐ **B** Je mets régulièrement mes appareils à jour
- ☐ **C** Je les verrouille avec un code d'accès difficile à deviner, en plus du code PIN
- ☐ **D** J'équipe mes appareils d'une coque et d'une protection d'écran

2/ Vrai ou Faux

Je n'ai pas besoin de faire des sauvegardes de mon téléphone.

☐ **Vrai** ☐ **Faux**

3/ Cherchez l'intrus

J'ai besoin d'une application mobile. Je la télécharge :

- ☐ **A** sur le site officiel du fournisseur
- ☐ **B** sur les magasins officiels d'applications comme Google Play ou App Store, par exemple
- ☐ **C** sur n'importe quel autre site

4/ Reliez les situations à leurs solutions

Je travaille régulièrement à l'extérieur	A ☐	☐ **1**	Je bloque ma ligne en appelant mon opérateur et mon téléphone en communiquant mon code IMEI et je dépose plainte
J'ai perdu ou je me suis fait voler mon téléphone	B ☐	☐ **2**	J'évite de me connecter à un réseau WiFi public
Je télécharge un jeu sur mon téléphone	C ☐	☐ **3**	Je n'autorise pas l'accès à mes photos, mes contacts et mes messages

RÉPONSES

1/B et C

2/FAUX – Votre appareil mobile contient de nombreuses données, comme votre répertoire de contacts, vos messages, vos photos et vidéos. En cas de perte, de panne ou de vol de votre appareil, vous pourriez ne plus retrouver vos données.

3/C – Seuls les sites ou les magasins officiels vérifient que les applications que vous installez ne sont pas piégées.

4/A – 2 B – 1 C – 3

Les informations clés sur les mots de passe

Utilisez un mot de passe différent pour chaque service

Ainsi en cas de perte ou de vol d'un mot de passe, seul le service concerné sera vulnérable. Dans le cas contraire, tous les services pour lesquels vous utilisez le même mot de passe compromis seraient piratables

Utilisez un mot de passe long et complexe

Une technique d'attaque répandue, dite par « force brute », consiste à essayer toutes les combinaisons possibles de caractères jusqu'à trouver le bon mot de passe. Réalisées par des ordinateurs, ces attaques peuvent tester des dizaines de milliers de combinaisons par seconde. Pour empêcher ce type d'attaque, il est admis q u ' un bon mot de passe doit comporter au minimum 12 signes mélangeant des majuscules, des minuscules, des chiffres et des caractères spéciaux.

Un technique pour créer un mot de passe solide :
La méthode des premières lettres :
Mon club préféré c'est l'ASVH je suis licencié depuis 2 ans
donne :
Mcpc'l'ASVHjsld2a

Utilisez un mot de passe impossible à deviner

Une autre technique d'attaque utilisée par les pirates est d'essayer de « deviner » votre mot de passe. Évitez donc d'employer dans vos mots de passe des informations personnelles qui pourraient être faciles à retrouver (sur les réseaux sociaux par exemple), comme le prénom de votre enfant, une date anniversaire ou votre groupe de musique préféré. Évitez également les suites logiques simples comme 123456, azerty, abcdef... qui font partie des listes de mots de passe les plus courants et qui sont les premières combinaisons qu'essaieront les cybercriminels pour tenter de forcer vos comptes.

Ne communiquez jamais votre mot de passe

Votre mot de passe doit rester secret. Aucune société ou organisation sérieuse ne vous demandera jamais de lui communiquer votre mot de passe par messagerie ou par téléphone. Même pour une « maintenance » ou un « dépannage informatique ». Si l'on vous demande votre mot de passe, considérez que vous êtes face à une tentative de piratage ou d'escroquerie.

N'utilisez pas vos mots de passe sur un ordinateur partagé

Les ordinateurs en libre accès que vous pouvez utiliser à l'école, dans une médiathèque et autres lieux publics peuvent être piégés et vos mots de passe peuvent être récupérés par un criminel. Si vous êtes obligé d'utiliser un ordinateur partagé ou qui n'est pas le vôtre, utilisez le mode de « navigation privée » du navigateur, qui permet d'éviter de laisser trop de traces informatiques, veillez à bien fermer vos sessions après utilisation et n'enregistrez jamais vos mots de passe dans le navigateur. Enfin, dès que vous avez à nouveau accès à un ordinateur de confiance, changez au plus vite tous les mots de passe que vous avez utilisés sur l'ordinateur partagé

Les informations clés sur les réseaux sociaux

Protégez l'accès à vos comptes

os comptes de réseaux sociaux contiennent des informations personnelles sensibles (identité, adresse postale ou de messagerie, numéro de téléphone, date de naissance, etc.), qui peuvent être convoitées par les cybercriminels. Pour vous assurer que personne ne puisse utiliser votre compte à votre insu ou usurper votre identité, protégez bien l'accès à votre compte en utilisant des mots de passe différents et suffisamment robustes. Si le service le propose, activez également la double authentification.

Vérifiez vos paramètres de confidentialité

Par défaut, les paramètres de visibilité de vos informations personnelles (numéro de téléphone, adresse email...) et de vos publications sont souvent très ouverts. Vos données peuvent ainsi être partagées à tous les abonnés du réseau social. Il est généralement possible de restreindre cette visibilité en réglant la configuration de votre compte, afin de garder la maîtrise de ce que les autres utilisateurs voient de vos informations et de vos activités. Vérifiez régulièrement ces paramètres de confidentialité qui peuvent être modifiés sans que vous ne le sachiez.

Maîtrisez vos publications

Les réseaux sociaux permettent de communiquer auprès d'une grande audience que vous ne pourrez jamais complètement maîtriser. Même dans un cercle que l'on pense restreint, vos publications peuvent vous échapper et être rediffusées ou interprétées au delà de ce que vous envisagiez. Ne diffusez pas d'informations personnelles ou sensibles qui pourraient être utilisées pour vous nuire. Faites également preuve de discernement lorsque vous évoquez votre travail car cela pourrait vous porter préjudice ainsi qu'à votre entreprise.

Faites attention à qui vous parlez

Les cybercriminels utilisent notamment les réseaux sociaux pour commettre des escroqueries et voler des informations personnelles ou professionnelles. Soyez vigilants, car à leur insu, vos "amis" ou contacts peuvent également vous envoyer ou partager des contenus malveillants, surtout s'ils se sont fait pirater leur compte sans le savoir. Quelques conseils supplémentaires : n'envoyez jamais d'argent à quelqu'un sans avoir vérifié son identité au préalable, n'envoyez jamais de photos ou vidéos intimes à des contacts virtuels qui pourraient en profiter pour vous faire chanter et méfiez vous des jeux concours, des gains inattendus, ou des « super affaires », qui peuvent cacher des escroqueries

Contrôlez les applications tierces

Certaines applications proposent d'interagir avec votre compte de réseau social. Il peut s'agir de jeux, de quiz, de programmes alternatifs pour gérer votre compte. Ces applications demandent des autorisations qu'il faut examiner avec attention car une fois données, ces applications peuvent avoir accès à vos informations personnelles, vos contacts, vos publications, vos messages privés... Ne les installez que depuis les sites ou magasins d'applications officiels, sinon vous risquez de donner l'accès à votre compte à un programme infecté par un virus. Si l'application vous semble trop intrusive dans les autorisations qu'elle demande, ne l'installez pas. Enfin, pensez à désinstaller ces applications ou en révoquer les droits si vous ne vous en servez plus.

Les informations clés sur les réseaux sociaux

Evitez les ordinateurs et le réseaux wifi

Utiliser un ordinateur en libre accès ou un réseau WiFi public est risqué car ils peuvent être piégés ou contrôlés par un cybercriminel. Lorsque vous vous connectez à votre compte de réseau social par ce moyen, vous pouvez vous faire voler votre mot de passe et donc vous faire pirater votre compte. Évitez dans la mesure du possible de renseigner des informations sensibles ou personnelles sur un matériel ou un réseau qui n'est pas le vôtre. Si vous y êtes contraint malgré tout, pensez à bien vous déconnecter de votre compte après utilisation pour empêcher que quelqu'un puisse y accéder après vous.

Faites preuve de discernement avec les infos publiées

Les réseaux sociaux sont de formidables et rapides outils d'information, mais n'importe qui peut aussi y publier n'importe quelle information, sans aucune vérification. Certaines informations peuvent donc être partiellement ou totalement fausses, parfois délibérément. Avec la puissance des réseaux sociaux, ces fausses informations (appelées « fake news » en anglais) peuvent avoir de graves conséquences sur les personnes qui en sont victimes. Aussi, avant de considérer ou relayer une information, efforcez vous d'en vérifier la véracité

L'Hameçonnage (phishing)

L'hameçonnage (phishing en anglais) est une technique frauduleuse destinée à leurrer l'internaute pour l'inciter à communiquer des données personnelles (comptes d'accès, mots de passe...) et/ou bancaires en se faisant passer pour un tiers de confiance. Il peut s'agir d'un faux message, SMS ou appel téléphonique de banque, de réseau social, d'opérateur de téléphonie, de fournisseur d'énergie, de site de commerce en ligne, d'administrations, etc.

Ne communiquez jamais d'informations sensibles par messagerie ou téléphone

aucune administration ou société commerciale sérieuse ne vous demandera vos données bancaires ou vos mots de passe par message électronique ou par téléphone

Avant de cliquer sur un lien douteux, positionnez le curseur de votre souris sur ce lien

(sans cliquer) ce qui affichera alors l'adresse vers laquelle il pointe réellement afin d'en vérifier la vraisemblance ou allez directement sur le site de l'organisme en question par un lien favori que vous aurez vous-même créé.

Vérifiez l'adresse du site qui s'affiche dans votre navigateur

r. Si cela ne correspond pas exactement au site concerné, c'est très certainement un site frauduleux. Parfois, un seul caractère peut changer dans l'adresse du site pour vous tromper. Au moindre doute, ne fournissez aucune information et fermez immédiatement la page correspondante.

Pour être conseillé en cas d'hameçonnage, contactez INFO ESCROQUERIES AU 0 805 805 817 (numéro gratuit).

LES RANÇONGICIELS

Un rançongiciel (ransomware en anglais) est un logiciel malveillant qui bloque l'accès à l'ordinateur ou à des fichiers en les chiffrant et qui réclame à la victime le paiement d'une rançon pour en obtenir de nouveau l'accès. La machine peut être infectée après l'ouverture d'une pièce jointe, ou après avoir cliqué sur un lien malveillant reçu dans des courriels, ou parfois simplement en naviguant sur des sites compromis, ou encore suite à une intrusion sur le système. Dans la majorité des cas, les cybercriminels exploitent des vulnérabilités connues dans les logiciels, mais dont les correctifs n'ont pas été mis à jour par les victimes.

Appliquez de manière régulière et systématique les mises à jour de sécurité du système et des logiciels installés sur votre machine

Tenez à jour l'antivirus

N'ouvrez pas les courriels, leurs pièces jointes et ne cliquez par sur les liens

Provenant de chaînes de messages, d'expéditeurs inconnus ou d'un expéditeur connu, mais dont la structure du message est inhabituelle ou vide

L'intelligence artificielle

Avantages de l'IA pour les enfants :

1. *Apprentissage personnalisé : L'IA peut aider à créer des programmes d'apprentissage personnalisés pour chaque enfant, en fonction de ses besoins et de son rythme d'apprentissage.*
2. *Jeux éducatifs : De nombreux jeux éducatifs utilisent l'IA pour aider les enfants à apprendre de manière ludique.*
3. *Aide aux devoirs : Des outils d'IA comme les assistants virtuels peuvent aider les enfants à faire leurs devoirs.*

Inconvénients de l'IA pour les enfants :

1. *Dépendance aux écrans : L'utilisation excessive de l'IA peut conduire à une dépendance aux écrans, ce qui peut avoir des effets négatifs sur la santé physique et mentale des enfants.*
2. *Vie privée : Les enfants peuvent ne pas comprendre les implications en matière de vie privée lorsqu'ils utilisent des outils d'IA.*
3. *Interaction sociale limitée : L'utilisation excessive de l'IA peut limiter les interactions sociales des enfants, ce qui est crucial pour leur développement émotionnel et social.*

Il est important de noter que l'IA est un outil, et comme tous les outils, son utilisation dépend de la façon dont nous l'utilisons. Il est donc essentiel d'enseigner aux enfants comment utiliser l'IA de manière responsable.