Co-funded by the
Erasmus+ Programme
of the European Union

IMPROVING CYBERSECURITY READINESS OF THE EUROPEAN VOCATIONAL EDUCATION AND TRAINING SECTOR

CYBER.EU.VET

INTELLECTUAL OUTPUT IO3

TRAINERS TRAINING TOOLKIT

NGO NEST Berlin
AEII
tandemplus network
Latvian European Community Studies Association
COFAC
EOS
inerciadigital
meath partnership

Introduction

Les partenaires du projet CYBER.EU.VET ont élaboré cette boîte à outils pour la formation des formateurs - composée de 6 modules + matériels - à l'usage des enseignants et des formateurs du secteur de l'EFP. Chaque module comprend une partie théorique, des exemples pratiques et des tâches pour le travail en groupe. Le format de formation est ouvert à l'utilisation dans différents pays européens et doit être adapté aux besoins et conditions locales chaque fois que cela est nécessaire. Les ajustements peuvent porter principalement sur les exemples pratiques et les études de cas fournis par le format de formation.

LES PARTENAIRES ONT ÉLABORÉ LES MODULES DE FORMATION SUIVANTS ::

CYBERATTAQUES

Module 1

1. Aperçu du module

Groupe cible

- Éducateurs et formateurs en EFP
- Étudiants
- Représentants d'organisations ou d'initiatives pertinentes (ONG, autorités nationales et régionales, établissements d'enseignement) autorités nationales et régionales, établissements d'enseignement)

Module description

Compte tenu du nombre et de l'ampleur croissants des cyberattaques chaque année, notamment à la lumière des derniers événements économiques, politiques et sociaux (conséquences des restrictions Covid-19, conflit militaire en Ukraine, etc.), il est important de discuter plus fréquemment des cyberattaques réelles.

Par conséquent, l'objectif de ce cours est de fournir une compréhension fondamentale des cyberattaques et d'apprendre à réagir à d'éventuels incidents.

Le contenu de ce module couvre les aspects (unités) suivants :

- Définition et questions pertinentes
- Typologie
- Les incidents les plus réels (exemples pratiques)
- Comment se protéger des cyberattaques et comment réagir en cas d'incidents.
- A la fin de chaque unité, une activité pratique est prévue.

Objectifs d'apprentissage

- Fournir une compréhension fondamentale des questions liées aux cyberattaques.
- Comprendre les conséquences et les impacts des cyberattaques et menaces potentielles.
- Reconnaître et classer les formes les plus courantes de cyberattaques.
- Savoir comment réagir aux attaques - où signaler, si un incident se produit.
- Assurer des sources d'information et de littérature pour un apprentissage plus approfondi et plus détaillé, pour suivre les cyberattaques réelles et pour les moyens de protection.

Durée totale

Max 1,5 heures

CYBERATTAQUES

Module 1

Ce module sera présenté par le formateur sous forme de présentation PowerPoint partageant les connaissances théoriques accompagnées d'éléments plus visuels, d'exemples pratiques et d'exercices (20 minutes maximum + une activité pratique pour chaque unité).

Il est recommandé de préparer les présentations sur les modèles PPT adaptés au projet CYBER.EU.VET. Compte tenu des développements et des progrès rapides dans le domaine de la cybersécurité, il est recommandé de réviser continuellement les unités et, si nécessaire, d'ajuster le contenu en tenant compte des développements les plus récents dans le domaine de la cybersécurité.

En outre, il est recommandé aux formateurs d'adapter ce module aux besoins de l'EFP local et d'y inclure des exemples des sujets d'actualité dans la région. Ce module couvre principalement des exemples pratiques de la Lettonie ainsi que quelques exemples internationaux. Il est recommandé de se concentrer davantage sur l'unité 3 pour analyser et discuter d'exemples pratiques d'incidents, accompagnés de photos et de vidéos.

Unité 1 - Cyberattaques

Qu'est-ce que cela signifie ? Introduction au sujet

Activité didactique #1 - Théorie

DÉFINITION ET SIGNIFICATION

Cyberattaque (pl. cyberattaques) = tentative d'accès illégal et non autorisé à un ordinateur ou à un système informatique dans le but de l'endommager ou de lui nuire. Son objectif est de désactiver, perturber, détruire ou contrôler des systèmes informatiques ou d'altérer, bloquer, supprimer, manipuler ou voler des données contenues dans ces systèmes.

Avec l'apparition des restrictions Covid-19 et la nécessité de passer à un format de travail et d'apprentissage numérique, le nombre de cybermenaces et d'attaques a augmenté et la protection numérique est devenue plus importante.

Le terme "cyberattaque" est étroitement lié à des termes tels que "cybermenace" (possibilité qu'une attaque particulière se produise) et "cyberrisque".

Les cyberattaques les plus courantes : attaque par logiciel malveillant, hameçonnage, attaque de type "man-in-the-middle", attaque par mot de passe, attaque par déni de service, etc.

Types de communication des attaquants : contacts personnels, téléphone, courrier électronique, logiciels malveillants.

CYBERATTAQUES

Module 1

SOURCE : https://cert.lv/lv/2022/02/kiberuzbrukuma-riskam-paklauts-ikviens-interneta-lietotajs ; https://www.investopedia.com/terms/c/cybersecurity.asp.

Qui peut effectuer des cyberattaques ?

Une cyberattaque peut être lancée de n'importe quel endroit du monde par n'importe quel individu ou groupe utilisant une ou plusieurs stratégies d'attaque diverses, et peut viser des individus, des sociétés publiques ou privées (entreprises).

Pourquoi les cyberattaques se produisent-elles et que peuvent-elles provoquer ?

Les attaques dans l'environnement virtuel sont généralement liées à l'usurpation d'identité, l'acquisition de ressources informatiques, le vol et la falsification d'informations, l'accès à des secrets commerciaux, le chantage ou la diffamation. Les cyberattaques sont principalement conçues pour réaliser des gains financiers (par exemple, voler des numéros et des codes de cartes de crédit), perturber et se venger (par exemple, porter atteinte à la réputation d'une organisation).

Par exemple, des crises telles que Covid-19 ou le conflit militaire en Ukraine sont utilisées pour attirer l'attention des utilisateurs dans des courriels frauduleux et des annonces sur les médias sociaux.

STATISTIQUES

Le travail à distance forcé par la pandémie a manifestement augmenté les risques de cybersécurité et facilité de nouveaux types d'incidents. La plupart d'entre eux concernent également les établissements d'enseignement et devraient être pris en compte dans les activités d'éducation et de formation continue des éducateurs et des jeunes. Selon les informations analysées par Deloitte, 350 cyberattaques ont eu lieu en avril 2020 en Suisse, alors que la norme est de 100 à 150 cyberattaques - (phishing, sites web frauduleux, attaques directes contre des entreprises, etc.)

L'augmentation du travail à distance exige que l'on se concentre davantage sur la cybersécurité, en raison de l'exposition accrue aux cyberrisques. C'est ce qui ressort, par exemple, du fait que 47 % des individus tombent dans une arnaque de phishing alors qu'ils travaillent à domicile.

En Lettonie, par exemple, le plus grand nombre d'adresses IP uniques menacées a été détecté de février à avril 2020, lorsque la pandémie de Covid-19 a commencé (plus de 10 000 par mois) selon le CERT.LV (l'institution de réponse aux incidents de sécurité des technologies de l'information de Lettonie), qui publie mensuellement et annuellement des

données et un aperçu des incidents les plus pertinents appelés "Kiberlaikapstākļi" (Cyber Weather).

SOURCE : https://www2.deloitte.com/ch/en/pages/risk/articles/impact-covid-cybersecurity.html

OUTIL INTERACTIF : La carte des cybermenaces en direct (monde)

Activité d'apprentissage #1 - Activité pratique

Discussion avec les participants sur leur expérience des cyberattaques (10-15 min) :

1) Quels types de cyberattaques connaissez-vous ?

2) Avez-vous, ou vos parents/amis, déjà été victime d'une cyberattaque/incident cybernétique ? Comment s'est-il terminé ?

Unité 2 - Types de cyberattaques

Activité d'apprentissage #2 - Théorie

LES MÉTHODES (TYPES) DE CYBERATTAQUES LES PLUS COURANTES :

Un **malware** est un logiciel malveillant (vers, virus) qui est utilisé pour endommager les appareils (ordinateurs, téléphones, etc.) ou le réseau de l'utilisateur. Exemples de logiciels malveillants : Logiciels espions et chevaux de Troie, vers, virus, logiciels publicitaires, pourriels. Selon le type de code malveillant, les logiciels malveillants peuvent être utilisés par les pirates pour voler ou copier secrètement des données sensibles, supprimer des données, bloquer l'accès à des fichiers, perturber le fonctionnement du système ou le rendre inopérant [DigiCERT]. Les logiciels malveillants se propagent principalement à deux fins : obtenir des informations (logiciels malveillants d'espionnage qui transmettent des données à partir de l'appareil de la victime) ou réaliser des profits (logiciels de chiffrement ransomware qui chiffrent les données sur l'appareil de l'utilisateur et lui demandent ensuite une rançon) [CERT Report 2020].

Phishing ou escroquerie aux données personnelles - méthode dans laquelle un pirate envoie un courriel apparemment légitime demandant aux utilisateurs de divulguer des informations confidentielles. Les destinataires sont incités à télécharger le logiciel malveillant contenu dans l'e-mail en ouvrant un fichier joint ou un lien intégré. Il s'agit généralement de sites web qui ressemblent à de véritables entreprises et sur lesquels les utilisateurs doivent saisir leurs informations personnelles (compte bancaire, numéros de carte de crédit et mots de passe, y compris ceux des services d'authentification). L'escroquerie aux données peut également se faire par téléphone ou par messages WhatsApp [Investopedia].

Déni de service (DoS) - les pirates bombardent les serveurs d'une organisation de gros volumes de demandes de données simultanées jusqu'à ce que la cible ne puisse pas répondre ou tombe en panne, rendant ainsi les serveurs incapables de traiter les demandes légitimes. En conséquence, l'accès au service est impossible pour les utilisateurs du système. Les attaques DoS peuvent durer de quelques heures à plusieurs mois et peuvent coûter aux entreprises du temps et de l'argent pendant que leurs ressources et services sont indisponibles [Investopedia].

Attaque de l'homme du milieu - les attaquants s'insèrent secrètement entre deux parties, par exemple un utilisateur d'ordinateur individuel et une institution financière. Selon les détails de l'attaque réelle, ce type d'attaque peut être plus spécifiquement classé comme une attaque de type "homme dans le navigateur", "monstre du milieu" ou "machine du milieu". Dans ce cas, l'attaquant intercepte, supprime ou modifie les données lorsqu'elles sont transmises sur un réseau par un ordinateur, un smartphone ou tout autre appareil connecté [Investopedia, TechTarget].

Activité d'apprentissage #2 - Activité pratique

Discussion de groupe - quels types de caractéristiques indiquent des messages d'attaque/fraude ? (10 -15 min)

- Les participants disposent de 10 minutes pour noter les caractéristiques.
- Discussion des résultats

Unité 3 - Exemple de menaces et d'attaques

Comment identifier les menaces ?

Activité d'apprentissage #3 - Théorie

Exemples de cyberattaques (à la lumière de la guerre en Ukraine)

E-mails frauduleux en anglais appelant à soutenir l'une des parties au conflit militaire - l'Ukraine ou la Russie.

Le soutien peut être manifesté en achetant des votes et en votant de cette manière - il s'agit d'une fraude visant à voler les données des cartes de paiement des utilisateurs (voir écran d'impression)

VIDÉO - How scammers are hijacking Ukraine war charity donations (Comment les escrocs détournent les dons de charité pour la guerre en Ukraine) - BBC News

ARTICLE - 4 Types of Russia-Ukraine War Scams Targeting Consumers (4 types d'escroqueries liées à la guerre Russie-Ukraine ciblant les consommateurs)

Les exemples sont basés sur les principaux incidents survenus en Lettonie (2020-2021) et sur d'autres exemples internationaux (suivis d'exemples visuels)**.

(VEUILLEZ ADAPTER AUX BESOINS LOCAUX)

Malware

La situation du Covid-19 a été utilisée pour diffuser des tentatives de logiciels malveillants : par exemple, des courriels au nom de l'Organisation mondiale de la santé (OMS), indiquant que la pièce jointe contient les dernières informations sur le Covid-19 ; des liens vers des graphiques montrant la propagation du Covid-19, dont la fonctionnalité était de voler les données des utilisateurs ; des courriels malveillants adressés à des établissements de santé concernant la livraison d'équipements de protection du Covid-19, etc.

La propagation du logiciel malveillant le plus dangereux au monde, Emotet, à la fois sur les réseaux mondiaux et lettons, vise à voler des informations sensibles et provient généralement d'un courriel d'un contact déjà infecté. Emotet sert d'ouverture de porte pour d'autres ordinateurs, permettant un accès non autorisé à d'autres familles de logiciels malveillants. Plus de 200 entreprises lettones ont été infectées.

Phishing ou escroquerie aux données personnelles

La majorité des cas visaient l'escroquerie de données de messagerie et d'Office 365, l'acquisition d'une banque, d'un système de paiement international (y compris Smart-ID - outil d'authentification électronique
en Lettonie), de données d'accès, et l'escroquerie de données d'accès à des comptes sur des médias sociaux populaires (Facebook et Instagram). Le sujet Covid-19 était souvent utilisé pour attirer l'attention desutilisateurs dans des courriels frauduleux et des annonces sur les médias sociaux.

Pendant la pandémie, des tentatives intensifiées de fraude aux données ont été observées en utilisant les marques de fournisseurs de services de livraison de colis (Latvijas Pasts, DHL, Omniva, DPD, AliExpress, etc.),
des attaques innovantes ont été observées, par exemple une attaque sur les droits d'accès à Office 365 qui était difficile à détecter par des moyens techniques car aucune action malveillante n'a été menée sur l'appareil de la victime, mais les attaques ont été menées au sein d'Office 365.

VIDÉO Phishing (avec sous-titres en anglais)

Fraude

Tentatives de fraude intensives, y compris des attaques d'ingénierie sociale. La plupart des fraudes visaient à obtenir des données d'accès aux cartes de paiement des citoyens, des ressources financières, ainsi que des données d'accès au courrier électronique.

Les attaquants ont envoyé des courriels et des SMS frauduleux à la population, de la même façon que des appels téléphoniques frauduleux, le plus souvent en se faisant passer pour des représentants de banques ou de fournisseurs de services de messagerie. Plusieurs entreprises ont souffert de interférence commerciale (BEC), subissant une perte totale de près de 200 000 €.

La question de la livraison des marchandises a également fait l'objet de fraudes contre des vendeurs qui publiaient des informations sur la vente de marchandises sur des portails publicitaires. Se faisant passer pour des acheteurs intéressés et utilisant la plateforme de communication WhatsApp, les fraudeurs exprimaient le souhait d'acheter le produit, comme s'ils utilisaient les services d'une société de messagerie, et demandaient aux vendeurs de saisir les détails de la carte sur les faux sites Web d'Omniva, de DPD et, plus tard, de Latvijas Pasts, afin de révéler le code CVV et le solde.

Les attaquants ont utilisé des adresses de sites Web personnalisées (domaines) similaires aux adresses des sites Web originaux pour tromper le public.

Les attaquants ont également tenté d'obtenir des informations sur les cartes de paiement en envoyant des courriels leur demandant de demander un solde en bitcoins en s'inscrivant à un service frauduleux d'échange de crypto-monnaies.

Les tentatives les plus actives étaient des campagnes d'extorsion, dans lesquelles les pirates prétendaient avoir piraté l'appareil d'un utilisateur et obtenu du matériel compromettant pour lequel une rançon était fixée ; des loteries au nom des marques connues, proposant de gagner les tout derniers smartphones ou d'autres prix de valeur.

AUTRES EXEMPLES

Annonces trompeuses sur les médias sociaux - utilisant les noms de personnalités lettones célèbres à leur insu, les internautes étaient invités à investir dans des crypto-monnaies. Les escrocs

ont également passé des appels téléphoniques et ont tenté de persuader les gens d'investir.

Dans certains cas, des tentatives frauduleuses répétées

Dans certains cas, des tentatives frauduleuses répétées ont été observées, les victimes de la fraude financière se voyant proposer une aide pour récupérer leurs ressources perdues.

Escroqueries téléphoniques - en falsifiant les numéros de téléphone de différents établissements de crédit et en se faisant passer pour des représentants de banques, les escrocs, profitant de la méconnaissance du public sur les méthodes d'authentification supplémentaires, ont escroqué les ressources financières de plusieurs milliers d'utilisateurs, causant des pertes totales de centaines de milliers d'euros aux établissements de crédit lettons.

Les pirates s'adaptent également à la généralisation du travail à distance : ils prennent en compte le besoin des entreprises de passer rapidement à des conditions de travail à distance et de passer rapidement à une condition de travail à distance et de la mise en place de

circulation des documents électroniques, les pirates profitent de cette situation pour adapter leurs attaques - par exemple, un certain nombre de comptables d'entreprise ont reçu des courriels au nom du directeur ou d'un autre employé leur demandant d'effectuer un paiement urgent ou modifier le compte de paie.

Latvia and Lithuania detain 108 over multi-million euro call centre scam

Interférence dans la correspondance commerciale des entreprises - en compromettant les e-mails des entreprises ou de leurs partenaires de collaboration, les attaquants choisissent le moment opportun pour envoyer à l'une des parties une facture avec un compte modifié.

Messages d'escroquerie - les attaquants tentent d'intercepter les comptes WhatsApp en demandant qu'un code à six chiffres soit envoyé par erreur au numéro de téléphone du destinataire par erreur. Comme un message sera reçu des personnes figurant dans votre liste de contacts, certaines personnes transfèrent leur code, perdant ainsi l'accès à leur compte WhatsApp. L'utilisation d'une authentification à deux facteurs serait un moyen de protection contre une telle attaque.

EXEMPLE : l'utilisateur partage le code numérique avec un pirate.

EXEMPLE: SMS d'une banque locale avec un lien vers une fraude (exemple letton)

Courriels d'escroquerie - les fraudeurs se font passer pour un bureau de poste national (Latvijas Pasts) et demandent de payer pour la livraison d'un envoi prétendument retardé. Le lien fourni dans l'e-mail mène à un faux site web permettant d'obtenir des données frauduleuses sur les cartes de paiement (voir exemple letton).

Fausses boutiques en ligne - une activité particulièrement élevée a été observée pendant la période des fêtes de fin d'année au moyen d'annonces sur les médias sociaux et en raison des restrictions Covid-19 qui ont obligé les entreprises à vendre leurs produits en ligne.

EXEMPLES Les escrocs attirent les utilisateurs d'AliExpress vers de faux magasins en ligne (photo et cas d'escroquerie) ; Comment reconnaître une escroquerie

Arnaque romantique - les escrocs profitent des personnes à la recherche d'un partenaire romantique, souvent par le biais de sites de rencontres, d'applications ou de médias sociaux.

Ils jouent sur des déclencheurs émotionnels pour vous amener à fournir de l'argent, des cadeaux ou des informations personnelles.

EXEMPLE Enquête sur un arnaqueur romantique [par North Lab]

Attaques par déni de service (DoS et DDoS)

Des attaques DDoS contre des institutions publiques et municipales ont été enregistrées (par exemple, la Bibliothèque nationale, le Centre des systèmes d'information culturelle, etc.)

Des attaques DDoS prolongées ont perturbé une école. Des rapports similaires ont été reçus d'autres institutions éducatives au début de l'année scolaire. Les établissements d'enseignement ailleurs en Europe sont également confrontés à de tels défis.

En Europe comme en Lettonie, les incidents suivants sont devenus d'actualité - extorsion d'argent

tentatives visant principalement des institutions financières ou des entreprises du secteur privé (les attaquants ont effectué une série d'attaques à titre d'essai, menaçant de suspendre le fonctionnement des sites Web de l'entreprise ou d'autres ressources par le biais d'attaques jusqu'aux 2 Tb/s).

AUTRES TENDANCES

Appareils compromis et fuites de données

Les compromissions d'équipements peuvent toucher des particuliers, des entreprises, ainsi que des institutions publiques et municipales.

Cela peut se produire par un courrier électronique déjà compromis, ou par l'infection d'un appareil en ouvrant des pièces jointes ou des liens provenant de contacts apparemment familiers, tels que des collègues et des partenaires commerciaux; cela peut également se produire par l'intermédiaire de sites web compromis, par exemple via un plugin ou un système de gestion de contenu obsolète.

Comme ce fut le cas en 2020-2021, lorsque plusieurs institutions nationales ont temporairement perdu l'accès à leurs comptes de réseaux sociaux, des attaquants ayant pris le contrôle du profil d'un des administrateurs du compte.

Des rapports ont été déposés sur des effractions de réunions Zoom et MS Teams, résultant d'une mauvaise connaissance des mesures de protection disponibles (par ex. salle d'attente, accès limité depuis l'étranger, etc.)

Tentatives d'intrusion (toute attaque visant à compromettre les objectifs de sécurité d'une organisation) - après l'essor de l'activité de travail à distance des bots à la recherche de dispositifs vulnérables, mal configurés et/ou des mots de passe faibles pour les dispositifs connectés à un réseau (appareils fournis à la hâte par l'employeur, ordinateurs portables personnels qui ont commencé à être utilisés pour le travail, ainsi que des services RDP mal protégés avec des mots de passe faibles) a augmenté de manière significative

VIDEO Exemples d'intrusion

En savoir plus sur la détection d'intrusion

SOURCE CERT.LV et "Kiberlaikapstākļi" (Cyber Météo) ; Investopedia

Éléments supplémentaires

NOTE Considérez également les discussions sur d'autres méthodes sur les fausses informations et les informations frauduleuses, telles que deepfake et autres.

Activité d'apprentissage #3 - Activité pratique

A la fin de l'unité, un test Kahoot est organisé où les participants doivent détecter si les informations fournies sont frauduleuses et doivent identifier le type (méthode) de cybermenace.

threat: https://create.kahoot.it/details/421c14d4-9c70-47cb-94d5-e6c0174ef3a3

Unité 4 - Que faire en cas d'incident ?

Prévention et comment se préparer.

Activité d'apprentissage nº 4 - Théorie

QUELQUES CONSEILS ET ASTUCES POUR SE PROTÉGER

- Vérifiez toujours vos courriels avec soin et faites attention aux pièces jointes ou aux liens intégrés provenant de sources ou d'expéditeurs inconnus/suspicieux ; les messages qui semblent urgents et qui vous demandent de télécharger quelque chose ou d'effectuer une autre tâche ; les offres qui promettent de récompense qui semble trop belle pour être vraie.

VIDEO Clicker (Spaidonis) avec sous-titres en anglais

- Faites attention à l'orthographe de l'adresse URL. Les sites d'hameçonnage utilisent souvent des adresses Web qui ressemblent à un site officiel, mais qui contiennent une simple faute d'orthographe, comme le remplacement du "1" par un "l" Une orthographe incorrecte ou étrange est le signe d'une possible escroquerie.
- Utilisez des mots de passe forts et différents pour vos appareils, vos comptes de messagerie et vos comptes de médias sociaux. Pour plus de conseils, consultez le module CYBER.EU.VET sur les mots de passe (module 4).

- Dans la mesure du possible, ajustez vos paramètres pour utiliser l'authentification multifactorielle sur vos appareils. Par exemple, mot de passe et identification faciale ou empreinte digitale sur votre téléphone ; quant à Gmail, il dispose d'un tel paramètre, selon lequel lorsqu'un utilisateur se connecte à partir d'un nouvel appareil, après avoir saisi son nom d'utilisateur et son mot de passe, il reçoit une demande de confirmation de son identification à partir d'un autre appareil, généralement un téléphone.

vérification en deux étapes dans WhatsApp (pour les utilisateurs d'Android).

- N'effectuez pas de transactions sensibles sur les réseaux Wi-Fi publics non sécurisés des cafés et autres lieux publics similaires.
- Assurez-vous qu'au moins les données les plus importantes de votre appareil ont une copie de sauvegarde (dans le nuage ou sur un périphérique externe). Assurez-vous que vous pouvez restaurer les données nécessaires à partir des sauvegardes, et découvrez combien de temps cela prend.
- Mises à jour des logiciels - il est essentiel de suivre les mises à jour des logiciels et de les installer immédiatement. Le moindre retard d'une journée peut être critique.
- Utilisez un VPN. Les réseaux privés virtuels ajoutent une couche supplémentaire de protection à l'utilisation d'Internet à domicile. On ne peut pas compter uniquement sur eux pour prévenir les cyberattaques, mais ils peuvent constituer une barrière utile contre les cyberattaques.
- Suivez régulièrement l'actualité dans le monde des attentats et essayez de penser que les événements mondiaux, nationaux et locaux, tant politiques qu'économiques, mais aussi ceux liés à la souffrance globale (pandémies, conflits militaires) peuvent être utilisés comme sujet/"couverture" pour d'éventuelles cyberattaques..
- Supplémentaire (en letton) : Recommandations de CERT.LV à la lumière de l'aggravation de la situation géopolitique et de l'augmentation des cybermenaces en Europe : https://cert.lv/lv/2022/02/cert-lv-ieteikumi-saasinoties-geopolitiskajai-situacijai-eiropa-un-pieaugot-kiberdraudiem

Où signaler une cybermenace ou des incidents

- Votre lieu de travail, votre établissement d'enseignement - envoyez des captures d'écran, des photos ou des vidéos à la personne compétente de votre établissement (par exemple, le service informatique). Prévenez vos collègues et amis
- Institutions soutenant le cyberespace national (cas de la Lettonie) :

1. CERT.LV (aide à la résolution des incidents, surveillance du cyberespace, avertissements), Instruction comment transférer des e-mails frauduleux (en letton)
2. Police d'État
3. Centre letton pour un internet plus sûr (violations et contenus illicites sur l'internet, sécurité des enfants sur l'internet), et autres

SOURCES D'INFORMATION ET RÉALITÉS

Pour suivre l'actualité de la cybersécurité et des cybermenaces, **lisez régulièrement des ressources locales ou internationales** :
https://portswigger.net/daily-swig/cyber-attacks
https://www.euronews.com/tag/cyber-attack
OUCH! Newsletters - le principal bulletin d'information gratuit sur la sécurité, destiné à tout le monde.

Sites Internet pour la Lettonie (certaines informations sont également disponibles en anglais) **(VEUILLEZ VOUS ADAPTER AUX BESOINS LOCAUX)** https://www.esidross.lv/ https://cert.lv/lv/ (including, "Cyber Weather "(Kiberlaikapstākļi), instruction how to forward fraudulent e-mails (in Latvian)
https://drossinternets.lv/

Activité d'apprentissage #4 - Activité pratique

Discussion avec les participants : évaluation de l'utilité du module (activité de 5-10 min)

2. Résultats d'apprentissage pour le module

Connaissances

- Les apprenants auront une compréhension de base des principaux problèmes liés aux cyberattaques.
- Les apprenants auront un aperçu des incidents réels (à la lumière des événements mondiaux).
- Les apprenants sauront quelles sources d'information suivre pour les avertissements et l'actualité des menaces.

Skills

Les apprenants seront capables d'identifier et de classer les types courants de cybermenaces et de les expliquer.

Compétences

- Les apprenants seront capables de reconnaître une cybermenace potentielle et de savoir où signaler la menace.
- Les apprenants seront capables de choisir des outils et des techniques de base pour se protéger des cyberattaques.

3. Bibliographie

CERT.LV (Informācijas tehnoloģiju drošības incidentu novēršanas institūcija): https://cert.lv/lv

Covid-19 phishing examples: https://www.investopedia.com/articles/personal-finance/040115/watch-out-these-top-internet-scams.asp
Digicert, What are Malware, Viruses, Spyware, and Cookies? https://www.websecurity.digicert.com/security-topics/what-are-malware-viruses-spyware-and-cookies-and-what-differentiates-them

Fichtner, E. (2022), Cybersecurity 101: Intro to the Top 10 Common Types of Cybersecurity Attacks: https://www.datto.com/blog/cybersecurity-101-intro-to-the-top-10-common-types-of-cybersecurity-attacks

Information Technologies Security Incident Response Institutions (2021), CERT.LV Annual Report 2020: https://cert.lv/uploads/parskati/CERTLV-annual-report-2020_ENG.pdf
Informative report, Cybersecurity Strategy of Latvia 2019-2022 (in Latvian only): https://www.mod.gov.lv/sites/mod/files/document/kiberstrategija.pdf
Latvian Safer Internet Centre (Project-platform “Drossinternets.lv”): https://drossinternets.lv
LIKTA (Latvian Information and Communication Technologies Association): https://likta.lv/digitalas-parmainas-izglitiba/
Li, Y., Liu, Q (2021), A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments, Science Direct, Vol. 7, p. 8176-8186: https://www.sciencedirect.com/science/article/pii/S2352484721007289

Merriam-webster dictionary, cyberattack: https://www.merriam-webster.com/dictionary/cyberattack

Prat, M.K. (2021), Cyber-attack – definition: https://www.techtarget.com/searchsecurity/definition/cyber-attack
Simplilearn, Cyber Security Full Course 2022: https://youtu.be/yr1Psapupsc

CERT.LV (2022), IT drošības seminārs "Esi drošs" martā (in Latvian): https://cert.lv/lv/2022/02/it-drosibas-seminars-esi-dross-marta#Sanita_Vitola
Esi Drošs (2022), Kiberuzbrukuma riskam pakļauts ikviens interneta lietotājs (in Latvian): https://www.esidross.lv/2022/02/10/kiberuzbrukuma-riskam-paklauts-ikviens-interneta- lietotajs/

1. Aperçu du module

Groupe cible

- Enseignants en EFP
- Étudiants
- Représentants des institutions publiques actives dans les secteurs de l'éducation : municipalités, autorités régionales et nationales

Description du module

Aujourd'hui, les gens passent une grande partie de leur temps devant un écran. Les jeunes grandissent dans un monde où les nouvelles technologies sont nécessaires et le principal moyen de communication qu'ils utilisent est l'internet. Être présent sur les médias sociaux, par exemple, offre de nombreux avantages, mais aussi de nombreux risques. Il y a beaucoup de personnes qui ont été ou sont victimes d'intimidation.
Dans la plupart des cas, ils n'étaient pas conscients de cela ou des problèmes que cela peut causer dans leur vie. C'est pour ça que nous souhaitons utiliser ce module, pour comprendre ce qu'est la cyberintimidation et comment la prévenir.

Objectifs d'apprentissage

- Comprendre la cyberintimidation
- Savoir comment la détecter
- Effets de la cyberintimidation
- Une compréhension des principales conséquences
- Donner des techniques pour la prévenir et y faire face.

Durée totale

2 heures

Unité 1 - Comment détecter la cyberintimidation

Quels sont les effets ?

Cette unité sera délivrée par le formateur sous la forme d'une présentation PowerPoint dont le but est de partager connaissances théoriques accompagnées d'éléments plus visuels - de courtes vidéos et des cas réels de cyberintimidation résumant les informations des diapositives PowerPoint (30 minutes maximum).
Il est recommandé de préparer les présentations sur les modèles PPT personnalisés pour le projet CYBER.EU.VET.

Activité d'apprentissage 1

Le formateur présente aux apprenants un exposé dont le contenu est suggéré ci-dessous (30 minutes maximum) :
La cyberintimidation, bien que souvent associée au cyberharcèlement, est un problème très sérieux en soi et dont la prévalence a augmenté au cours des dernières années.

Comment détecter la cyberintimidation ?
La cyberintimidation peut être **difficile à reconnaître** car elle se déroule derrière des portes fermées ou dans un téléphone/ordinateur privé.
Voici quelques-uns des signes les plus courants, indiquant qu'une personne peut être victime de cyberintimidation :

- Est anormalement contrarié(e) s'il/elle ne peut pas utiliser l'ordinateur ou le téléphone ou après avoir utilisé l'ordinateur.
- Change rapidement d'écran ou ferme des programmes lorsque quelqu'un passe à proximité.
- Évite les discussions sur ce qu'il fait sur l'ordinateur.
- Il s'éloigne de sa famille ou de ses amis.
- Réticence à participer à des activités qu'il aimait auparavant.
- Baisse inexpliquée des résultats scolaires.
- Refuse d'aller à l'école.
- Signale de plus en plus souvent des symptômes de maladie.
- Montre des signes de dépression ou de tristesse.

Les effets de la cyberintimidation peuvent être dévastateurs pour les victimes. Elles peuvent ressentir diverses émotions négatives, comme la tristesse, la colère, la frustration et l'humiliation. Elles peuvent également se sentir isolées et seules, comme si elles n'avaient personne vers qui se tourner.

Les victimes peuvent également souffrir sur le plan scolaire, car elles sont trop gênées pour aller à l'école ou participer aux cours.
Dans certains cas, les victimes peuvent même envisager le suicide.
La cyberintimidation peut également avoir des effets négatifs sur les personnes qui en sont témoins.
Ils peuvent avoir peur, se sentir impuissants et tristes. Ils peuvent également avoir des problèmes de sommeil et d'alimentation, voire développer une anxiété ou une dépression.

Effets et conséquences de la cyberintimidation :
Lorsque le harcèlement se produit en ligne, on peut avoir l'impression d'être attaqué partout, même dans sa propre maison. Il peut sembler qu'il n'y ait pas d'échappatoire. Les effets peuvent durer longtemps et affecter une personne de nombreuses façons :

- **Mentalement :** se sentir bouleversé, embarrassé, stupide, voire effrayé ou en colère.
- **Emotionnellement :** se sentir honteux ou se désintéresser des choses que l'on aime.
- **Physiquement :** se sentir fatigué (par la perte de sommeil), ou ressentir des symptômes comme des maux d'estomac et de tête.

The feeling of being laughed at or harassed by others, can prevent people from speaking up or trying to deal with the problem. In extreme cases, cyberbullying can even lead to people taking their own lives.

VIDEO Words Hurt | Cyberintimidation court métrage

Effects:

- Maladie
- Dépression
- Isolement
- Colère
- Humiliation

Activité d'apprentissage 2

Discussion de groupe - Q&R ; évaluation et feedback (max. 10 minutes)
Maintenant que vous connaissez les signes les plus courants de quelqu'un qui est victime de cyberintimidation,

- Connaissez-vous quelqu'un dans cette situation ?
- Pourriez-vous l'aider ?

Unité 2 - Comment prévenir/arrêter la cyberintimidation

Activité d'apprentissage 1

Le formateur présente aux apprenants un exposé dont le contenu est suggéré ci-dessous (30 minutes maximum) :
La cyberintimidation est facilitée par la simplicité d'accès aux plateformes et aux appareils numériques. Souvent,
ceux-ci sont utilisés sans aucune surveillance. Cela fait de la cyberintimidation un problème incroyablement difficile à aborder. Prévenir cette pratique nécessiterait beaucoup de temps et de ressources pour surveiller efficacement chaque interaction en ligne.
S'il n'est souvent pas possible pour les de se débarrasser complètement des outils numériques, il existe des méthodes que les parents, parents, les étudiants et les éducateurs peuvent employer pour combattre le phénomène et réduire ses effets néfastes.

Pour les parents, un moyen efficace d'aborder le préjudice résultant de la cyberintimidation consiste simplement à discuter de ce problème avec leurs enfants.
Il est également important de discuter de la sécurité en ligne, de la confidentialité et de la gestion des mots de passe. Définissez des lignes directrices sur la manière dont les élèves doivent se comporter en ligne et demandez aux jeunes de parler ouvertement à leurs parents de tout préjudice qu'ils ont subis du fait de l'intimidation en ligne ou dans le
monde réel.
Les jeunes peuvent prévenir la cyberintimidation en faisant attention à ce qu'ils publient. Ils doivent éviter de partager leurs mots de passe et s'assurer que leurs paramètres de confidentialité en ligne les protègent.
Les élèves jouent un rôle important dans la prévention de la cyberintimidation. Si les jeunes qui connaissent les faits de la cyberintimidation remarquent que quelqu'un d'autre en est victime, ils peuvent en informer un adulte de confiance.
Ils doivent également faire preuve de gentillesse, de générosité et de soutien à l'égard de l'enfant qui est victime d'intimidation. Les enseignants, les éducateurs et les autres adultes de confiance doivent se joindre aux parents et aux jeunes pour combattre la cyberintimidation.
Souvent, ces personnes peuvent repérer des changements dans le comportement d'un enfant et peuvent aider à traiter le problème avant les parents.
La technologie et l'internet ne sont pas le problème. Ce sont les gens qui l'utilisent pour nuire aux autres qui
sont le vrai problème. Pour cela, il est important d'enseigner aux adolescents comment utiliser les médias sociaux en toute sécurité et de manière responsable, et leur faire prendre conscience de la manière d'agir s'ils sont victimes de cyberintimidation.

Que faire si vous êtes victime de cyberintimidation ?

- NE RÉPONDEZ ou COMMENTEZ PAS au message de cyberintimidation.
- BLOQUEZ les personnes concernées.
- DÉCONNECTEZ-VOUS du site où se déroule l'intimidation.
- Protégez vos MOTS DE PASSE et vérifiez vos CONTRÔLES DE CONFIDENTIALITÉ.
- GARDEZ tout. Faites des captures d'écran ou imprimez l'incident comme preuve.
- SIGNALEZ la cyberintimidation : presque tous les sites technologiques proposent une option permettant de signaler quelqu'un pour cyberintimidation.
- Dis à un ADULTE de confiance ce qui se passe ou contacte les forces de l'ordre.

Que dois-tu faire si tu es témoin d'une cyberintimidation ?

- Prévenez vos parents ou un adulte de confiance et demandez-leur conseil.
- Signalez la situation au fournisseur de la technologie, de l'application ou du média social.
- Si la situation implique des camarades de classe, informez vos professeurs.
- Montrez votre soutien à la personne qui subit les intimidations, par exemple en lui adressant un message gentil.

Engagez une action en justice : La calomnie et la diffamation sont toutes deux des crimes qui peuvent donner lieu à un procès.

Demandez de l'aide :

▪ Il est très difficile de faire face à la cyberintimidation tout seul.

VIDÉO L'histoire d'Emma : Cyberintimidation par un meilleur ami.

Comment puis-je m'éduquer ?

▪ Les organisations qui peuvent aider : Il y a de nombreuses organisations qui partagent des informations sur la cyberintimidation. Les sites Web ci-dessous créent et partagent un contenu qui est vraiment utile à toute personne anxieuse ou victime de cyberintimidation.

▪ Blogs et podcasts : suivre les blogs et podcasts qui traitent du sujet est un excellent moyen de rester à jour et d'obtenir les derniers conseils ou points de vue.

▪ Livres .

▪ Applications et logiciels : Il y a de nombreux produits qui permettent aux parents de limiter et/ou de surveiller l'activité en ligne de leurs enfants.

Il appartient à chaque parent de décider si ce type de surveillance est approprié en fonction de l'âge de l'enfant et de ses habitudes sur Internet. Certains logiciels détectent les propos susceptibles de constituer une forme d'intimidation. Il existe également des entreprises qui s'associent aux écoles pour permettre le signalement anonyme des incidents d'intimidation.

Activité d'apprentissage 2

Discussion de groupe - Q&R ; évaluation et feedback (max. 15 minutes)

Exercice d'écriture :
Décrivez une situation dans laquelle vous savez qu'il y a de la cyberintimidation. Cette situation peut être réelle ou fictive.
Pouvez-vous aider ? Comment ? Pourquoi ou pourquoi pas ? Explique ce que tu ressens.

2. Résultats d'apprentissage pour le module

Connaissances

- L'apprenant saura comment détecter le cyber-harcèlement et comment la victime le ressent et le vit.
- En comprenant les faits de cyberintimidation et en étant conscients des méthodes pour y remédier, les jeunes, adultes et éducateurs peuvent contribuer à créer un monde numérique meilleur et plus empathique.

Skills

- L'apprenant comprendra comment reconnaître qu'une personne est victime de cyberintimidation.
- L'apprenant sera capable de comprendre quel niveau de réponse et de soutien est nécessaire en fonction du scénario en question.

Compétences

- L'apprenant sera capable de reconnaître un épisode de cyberintimidation et d'y remédier immédiatement en utilisant les outils appropriés.
- L'apprenant sera capable d'identifier la meilleure méthode de soutien, et celle qui est la plus la plus adaptée au cas en question.

3. Bibliographie

https://socialmediavictims.org/cyberbullying/effects/
https://americanspcc.org/impact-of-cyberbullying/
https://www.unicef.org/end-violence/how-to-stop-cyberbullying
https://www.security.org/resources/cyberbullying-resources-books-podcasts/

1. Aperçu du module

Groupe cible

- Éducateurs de l'EFP
- Représentants des institutions publiques actives dans les secteurs de l'éducation : municipalités, autorités régionales et nationales

Description du module

Il s'agit d'un module de suivi de "Cyberbullying. Qu'est-ce que c'est ? Comment la détecter ? fournit aux groupes cibles les compétences nécessaires pour sensibiliser les gens à la cyberintimidation et pour fournir des techniques de prévention afin de ne pas devenir une victime de la cyberintimidation.

Objectifs d'apprentissage

- Comprendre l'importance de la prévention
- Sensibiliser à la cyberintimidation
- Sensibiliser aux techniques de prévention de la cyberintimidation

Durée totale

1 heure et demie

Unité 1 - Pourquoi prévenir la cyberintimidation ?

Cette unité sera fournie par l'éducateur sous forme d'une présentation PowerPoint qui comprendra des éléments théoriques et des éléments plus visuels tels que des films courts et des scénarios réels de cyberintimidation qui résumeront les informations contenues dans les diapositives PowerPoint (20 à 30 minutes respectivement pour chaque unité).
Nous vous recommandons de préparer les présentations sur les modèles de PPT adaptés au CYBER.EU.VET. La présentation est suivie d'une discussion de groupe, afin que chacun puisse réfléchir à ce qu'il a appris.

Activité d'apprentissage 1

Le formateur présente aux étudiants un exposé dont le contenu est suggéré ci-dessous (20 minutes maximum) :

Prévenir ou intervenir ?

Selon les recherches, les personnes qui sont victimes de cyberintimidation ont une variété de résultats négatifs, notamment des difficultés émotionnelles, physiques, mentales et scolaires. En outre, la cyberintimidation est une source importante de stress pour les jeunes. Les victimes sont psychologiquement blessées, honteuses et parfois effrayées par la cyberintimidation. Non seulement ils se reprochent le harcèlement et les abus qu'ils subissent, mais ils se sentent aussi extrêmement anxieux. En fait, selon une étude, plus de 35 % des personnes ciblées par les cyberintimidateurs présentaient des symptômes de stress.
Ce type d'intimidation peut être particulièrement nuisible car il est souvent très public. En général, de nombreuses personnes peuvent voir ce qui est écrit ou posté.
Il est difficile, voire impossible, d'effacer toutes les traces d'un message une fois qu'il a été publié en ligne.
Cela signifie que le harcèlement peut être permanent. Lorsqu'une personne est harcelée par d'autres personnes sur les médias sociaux, par SMS, par chat instantané et les publications de blogs, elles peuvent commencer à se sentir désespérées. Ils peuvent penser que le suicide est le seul moyen de mettre fin à leur souffrance. Les dangers de la cyberintimidation étant si sérieux, il est essentiel que les éducateurs de l'EFP enseignent ce problème à leurs élèves avant qu'il ne cause de réels dommages.
Faire de la prévention réduit les risques d'être exposé à la cyberintimidation.

Activité d'apprentissage 2

Discussion de groupe (max. 10 minutes)

Demandez à vos élèves :

- Pourquoi la prévention est-elle si importante dans la cyberintimidation ?
- Avez-vous déjà été informé sur la cyberintimidation ?
- Comment vous informez-vous habituellement sur les infractions de cyberintimidation ?

Unité 2 - Sensibilisation

Activité d'apprentissage 1

Le formateur fait une présentation aux étudiants avec le contenu suggéré suivant (max. 30 minutes) :
Il est essentiel de discuter avec les élèves de la manière d'utiliser les médias sociaux de façon sûre et responsable, en
détectant les auteurs de cyberintimidation et en apprenant ce qu'ils doivent faire s'ils sont victimes d'intimidation en ligne.

VIDÉO Cyberintimidation - Comment éviter les cyberabus

PENSER AVANT DE POSTER

Les élèves doivent prendre l'habitude de relire leur travail avant de le publier. Ils peuvent taper l'article dans la section notes de leur ordinateur ou de leur smartphone, puis le relire quelques heures plus tard pour décider de le publier ou non. Comme les cyberintimidateurs peuvent utiliser ce que vous publiez contre vous d'une manière ou d'une autre, vous serez moins enclin à dire quelque chose que vous regretterez plus tard ou qui pourrait être utilisé contre vous. Bien sûr, si quelqu'un veut utiliser quelque chose contre vous, il s'efforcera d'obtenir même l'information la plus insignifiante, mais vérifier avant de partager peut réduire la gravité de la cyber-attaque. Réfléchir avant de publier peut vous aider à maintenir une relation saine avec les médias sociaux.

ÊTRE PRUDENT AVEC LES APPAREILS PUBLICS

Les étudiants doivent également être prudents lorsqu'ils utilisent des appareils publics tels que les ordinateurs de l'université ou de la bibliothèque car quelqu'un pourrait en profiter de bien des façons. Les appareils publics peuvent être infectés par des programmes malveillants, tels que les enregistreurs de frappe (keyloggers).

Selon la plupart des sources, un enregistreur de frappe est un logiciel qui surveille et enregistre discrètement toutes les frappes au clavier. Ils peuvent être utilisés pour intercepter les mots de passe et d'autres informations personnelles saisies sur le clavier, ce qui constitue une menace majeure pour les utilisateurs, comme la remise de l'accès à vos comptes de médias sociaux à des cybercriminels. La chose la plus importante à savoir en ce qui concerne les enregistreurs de frappe est qu'ils ne peuvent souvent pas être détectés par les programmes antivirus, car il existe sur le marché de nombreux enregistreurs de frappe légitimes destinés au contrôle parental, à la sécurité des entreprises, etc.

VIDÉO Peut-être qu'un enregistreur de frappe vous espionne ?

Outre les programmes de surveillance spécialisés, il convient de rappeler aux élèves qu'ils doivent se déconnecter de leurs comptes, car ils risquent de les laisser involontairement ouverts et accessibles à ceux qui utiliseront les ordinateurs à côté de lui.

PROTECTION EN LIGNE

Il est essentiel d'utiliser des mots de passe forts partout pour lutter contre la cyberintimidation et d'autres activités frauduleuses.
eUn mot de passe fort est un mot de passe qui ne peut pas être facilement deviné ou compromis. Il doit être long, contenir une combinaison de chiffres, de caractères spéciaux et de lettres minuscules et majuscules, et ne doit en aucun cas contenir des informations évidentes telles que le nom, la date de naissance, etc.
En protégeant vos comptes, vous vous assurez que personne n'y a accès.

LA CYBERINTIMIDATION DOIT ÊTRE SIGNALÉE.

Assurez-vous que vos élèves comprennent l'importance de signaler les cas de cyberintimidation. Il ne s'agit pas seulement de détecter les cyberintimidateurs, mais aussi d'informer la plateforme de médias sociaux, le fournisseur d'accès à Internet et toute autre partie concernée. Pour mettre un terme au harcèlement, il peut même être nécessaire d'informer les autorités locales. Après avoir rempli tous les documents nécessaires, les élèves doivent prendre les mesures requises pour bloquer la personne ou le compte responsable de la cyberintimidation. Ils doivent également être conscients que, même après avoir bloqué l'auteur de l'infraction, celui-ci peut créer d'autres comptes pour approcher la victime. La bonne nouvelle concernant la cyberintimidation qui se produit en ligne est qu'elle peut généralement être enregistrée, préservée et présentée à quelqu'un qui peut aider. Les victimes devraient conserver cette preuve au cas où les choses deviendraient incontrôlables.

VIDÉO: IGNORER OU DÉNONCER UN CYBER-HARCELEUR

Activité d'apprentissage 2

Présentez aux étudiants l'étude de cas ci-dessous

Projet Erasmus+ YouProMe – www.youpromeproject.eu

Jessica est âgée de 18 ans. Elle vit avec ses deux parents, qui sont des professionnels et toujours occupés à travailler. Jessica est l'aînée de trois enfants. Il n'y a personne dans la famille avec de problèmes de santé connus. Elle étudie à l'école et est une élève studieuse. Elle est passionné de animaux et aime sortir avec ses amis. Elle a un petit ami. Jessica a un téléphone portable et utilise régulièrement les réseaux sociaux. Jessica a déclaré : "J'ai envoyé des photos à mon petit ami il y a quelques semaines. Je pensais qu'il était mon petit ami de toute façon, mais il les a montrées à son ami et son ami les a envoyées à tout le monde. L'école l'a découvert et maintenant la police a parlé à lui et à son ami. Je ne suis pas retournée à l'école depuis, mais tout le monde me traite de salope sur les réseaux sociaux. Je ne peux pas supporter quand ils me fixent, et je sais déjà ce qu'ils pensent. Même les filles ont une opinion similaire sur moi. La chose stupide c'est que tout le monde le fait, tout le monde envoie des photos, mais j'ai juste eu la malchance d'avoir un petit ami qui m'a trahi. Je ne ferai plus jamais confiance à personne. J'ai l'impression que tout est fini et qu'il n'y a pas de retour en arrière possible."

En conséquence, Jessica a été absente de l'école pendant un mois et refuse d'y retourner. Elle a abandonné toutes ses activités sportives à l'école. Sa mère a parlé avec l'éducateur sportif et a dit qu'elle était préoccupée par certaines des choses "sombres" que Jessica a dites. Jessica est désireuse de modifier sa présence en ligne et de retrouver sa confiance initiale. Jessica et sa famille ne sont pas au courant de l'aide disponible et de la meilleure façon de soutenir sa santé mentale, ni ne savent comment un travailleur social peut intervenir dans cette situation. Jessica a pris conscience des risques liés à l'utilisation abusive d'Internet et reconnaît qu'elle a besoin d'un soutien pour gérer sa santé mentale, car cela a influencé sa prise de décision.

Vous pouvez maintenant engager une conversation à partir de ces questions (30 minutes maximum) :

- Quels sont les risques présents ici ?
- Quels sont les services que vous devez faire intervenir ?
- Quel plan d'action suggérez-vous à Jessica et à sa mère ?

2. Résultats d'apprentissage pour le module

Connaissances

▪ L'apprenant comprendra l'importance de la prévention de la cyberintimidation.
▪ L'apprenant saura quels types de techniques sont disponibles pour éviter d'être victime de cyberbullying.

Skills

- L'apprenant sera capable de sensibiliser à la prévention de la cyberintimidation.
- L'apprenant sera capable d'enseigner des techniques de prévention importantes à ses élèves.

Compétences

- L'apprenant sera capable de mettre en œuvre des événements efficaces de sensibilisation contre la cyberintimidation
- En fonction de la situation, l'apprenant sera capable de déterminer le type d'aide nécessaire. d'assistance est nécessaire.

3. Bibliographie

https://www.verywellfamily.com/how-to-prevent-cyberbullying-5113808
https://anti-bullyingalliance.org.uk/sites/default/files/uploads/attachments/cyberbullying-and-send-module-final%281%29_1.pdf
https://securelist.com/keyloggers-how-they-work-and-how-to-detect-them-part-1/36138/
https://www.connectsafely.org/tips-to-help-stop-cyberbullying/

AUTHENTIFICATION ET MOT DE PASSE

Module 4

1. Aperçu du module

Groupe cible

- Educateurs de l'EFP
- Étudiants
- Représentants des institutions publiques actives dans les secteurs de l'éducation : municipalités, autorités régionales et nationales

Description du module

Les professionnels de l'EFP et leurs étudiants sont confrontés quotidiennement à différentes menaces de cybersécurité. Bien qu'il existe divers supports pédagogiques sur la cybersécurité disponibles en ligne, ils ne sont pas tous mis à jour, ou sont perçus par les apprenants comme trop basiques ou trop complexes.
Le contenu éducatif de ce module permettra aux apprenants d'acquérir les compétences et les connaissances nécessaires pour
améliorer leur compréhension de l'authentification et des mots de passe, afin de renforcer leur
capacité de formation, mais aussi d'améliorer leurs compétences afin d'éviter les attaques de cybersécurité. Mieux équipés, les éducateurs de l'EFP seront en mesure d'aider davantage leurs élèves à reconnaître les menaces quotidiennes en les évitant.

Objectifs d'apprentissage

- Améliorer la compréhension de l'authentification dans la cybersécurité.
- Enrichir la compréhension des différentes méthodes d'authentification.
- Enrichir la compréhension des principales caractéristiques des méthodes d'authentification les plus courantes.
- Comprendre les risques liés à l'absence d'utilisation de mots de passe complexes.
- Donner des techniques pour gérer facilement les mots de passe complexes.

Durée totale

2 heures

AUTHENTIFICATION ET MOT DE PASSE

Module 4

UNITÉ 1 - AUTHENTIFICATION

Cette unité sera présentée par le formateur sous la forme d'une présentation PowerPoint partageant des connaissances théoriques, accompagnée d'éléments plus visuels - de courtes vidéos résumant les informations contenues dans les diapositives PowerPoint (20 minutes maximum).
Il est recommandé de préparer les présentations sur les modèles de PPT adaptés au projet CYBER.EU.VET. Compte tenu de l'évolution et des progrès rapides dans le domaine de la cybersécurité, il est recommandé de réviser continuellement les unités et, si nécessaire, d'ajuster le contenu en tenant compte des développements les plus récents dans ce domaine. La présentation est suivie d'une discussion de groupe de 10 minutes afin de réfléchir au processus d'apprentissage et d'évaluer le niveau de compréhension du sujet par les apprenants, tout en créant une atmosphère de confiance, tout en créant un espace pour d'autres questions et un retour d'information.

Activité d'apprentissage 1

Le formateur fait une présentation dont le contenu est suggéré ci-dessous (20 minutes maximum) :

Qu'est-ce que l'authentification ?

Le processus d'authentification dans le contexte des systèmes informatiques signifie l'assurance et la confirmation de l'identité d'un utilisateur. Avant qu'un utilisateur ne tente d'accéder à des informations stockées sur un réseau, il doit prouver son identité et sa permission d'accéder aux données. Lorsqu'il se connecte à un réseau, un utilisateur doit fournir des informations de connexion uniques, notamment un nom d'utilisateur et un mot de passe. Cette pratique vise à protéger le réseau contre l'infiltration de pirates informatiques. Ces dernières années, l'authentification s'est élargie pour exiger davantage d'informations personnelles de l'utilisateur, par exemple des données biométriques, afin de garantir la sécurité du compte et du réseau contre ceux qui ont les compétences techniques pour profiter des vulnérabilités.

VIDÉO : QU'EST-CE QUE L'AUTHENTIFICATION ?

Pourquoi l'authentification est-elle importante ?

L'authentification est une étape cruciale pour assurer la sécurité des données des utilisateurs et pour prévenir et bloquer tout accès non autorisé aux données en ligne. Si l'authentification n'est pas sécurisée, le système peut être
facilement attaqué et piraté et les cybercriminels peuvent avoir accès aux données et informations stockées dans le système.

Ill est très important d'éviter que cela ne se produise et de s'assurer que les utilisateurs connaissent différentes méthodes d'authentification gratuites ou payantes pour empêcher tout accès non autorisé à leurs données personnelles ou professionnelles.
Pour les organisations et les entreprises, nous recommandons d'investir dans des outils d'authentification de haute qualité afin de protéger leurs données en ligne contre toute violation potentielle.

VIDÉO: CONSEIL HEBDOMADAIRE DE CYBERSÉCURITÉ - AUTHENTIFICATION

Méthodes courantes d'authentification par mot de passe

Compte tenu de l'évolution constante des différents types de cybermenaces et d'attaques, un large éventail de méthodes d'authentification différentes a été développé au cours des dernières années.
Voici quelques-unes des méthodes d'authentification les plus communes :

1. Authentification par mot de passe standard
2. Authentification à deux facteurs
3. Authentification par jeton
4. Authentification biométrique
5. Authentification par reconnaissance informatique
6. CAPTCHAS

1. AUTHENTIFICATION PAR MOT DE PASSE STANDARD

- Forme d'authentification la plus basique et la plus fréquemment utilisée :
- Requérir la saisie d'un nom d'utilisateur, accompagné d'un code secret ou d'un mot de passe qui permet d'accéder à un réseau, un compte ou une application.

Pour réduire le risque de compromission d'un mot de passe, les utilisateurs doivent choisir un mot de passe fort. Un gestionnaire de mots de passe ou un logiciel sécurisé peut contribuer à empêcher tout accès non autorisé aux données stockées en ligne.

2. AUTHENTIFICATION À DEUX FACTEURS (2FA)

- L'authentification à deux facteurs exige que les utilisateurs s'authentifient via quelque chose "qu'ils savent" et quelque chose "qu'ils ont". Un mot de passe sert de " quelque chose qu'ils connaissent ", et un objet physique spécifique tel qu'un smartphone sert de "quelque chose qu'ils ont".
- L'authentification à deux facteurs exige généralement que l'utilisateur saisisse son nom d'utilisateur, un mot de passe, et un code à usage unique qui a été envoyé à un dispositif physique (téléphone mobile, lecteur de carte, etc.).

3. AUTHENTIFICATION PAR TOKEN

- Les systèmes de token utilisent un dispositif physique spécialement conçu pour offrir une authentification à deux facteurs, et il est recommandé si vous préférez ne pas compter sur les téléphones portables.
- Il peut s'agir d'un dongle inséré dans la porte USB de votre appareil, ou peut-être d'une carte à puce avec une puce d'identification par radiofréquence ou de communication en champ proche.
- Pour assurer la sécurité d'un système de token, il est essentiel de veiller à ce que le dispositif d'authentification physique (c'est-à-dire le dongle ou la carte à puce) ne tombe pas dans de mauvaises mains.

4. AUTHENTIFICATION BIOMÉTRIQUE

▪ L'authentification biométrique s'appuie sur les caractéristiques physiques d'un utilisateur pour l'identifier. L'authentification biométrique peut utiliser les empreintes digitales, les scans de la rétine ou de l'iris, ou la reconnaissance faciale et vocale. Il s'agit d'une forme d'authentification hautement sécurisée, car deux individus n'ont pas les mêmes caractéristiques physiques. L'authentification biométrique est un moyen efficace de savoir précisément qui se connecte au système.

5. AUTHENTIFICATION PAR RECONNAISSANCE INFORMATIQUE

- La reconnaissance par ordinateur est une méthode d'authentification par mot de passe qui vérifie la légitimité d'un utilisateur en vérifiant qu'il se trouve sur un appareil particulier. Ces systèmes installent un petit plug-in logiciel sur l'appareil de l'utilisateur lors de sa première connexion réussie. Ce plug-in contient un marqueur de dispositif cryptographique. Lors de la prochaine connexion de l'utilisateur, le marqueur est vérifié pour s'assurer qu'ils sont sur le même appareil de confiance.
- Ce système est invisible pour l'utilisateur et ne nécessite aucune action d'authentification supplémentaire de leur part. Il lui suffit d'entrer son nom d'utilisateur et son mot de passe comme d'habitude et la vérification se fait automatiquement.
- Pour maintenir un niveau de sécurité élevé, les systèmes d'authentification par reconnaissance informatique doivent permettre les connexions à partir de nouveaux appareils en utilisant d'autres formes de vérification (ex. avec un code délivré par SMS).

6. CAPTCHAS

CAPTCHAs ne se concentrent pas sur la vérification d'un utilisateur particulier, contrairement à ce que les autres méthodes énumérées dans cet article. Les CAPTCHAs visent plutôt à déterminer si un utilisateur est humain, empêcher les tentatives d'intrusion dans les comptes par des ordinateurs (par exemple, les attaques par force brute).

Le système CAPTCHA affiche une image déformée de lettres et de chiffres, ou des images, et demande à l'utilisateur de taper ce qu'il voit. Comme les ordinateurs et les robots ont du mal à identifier correctement ces déformations, les CAPTCHA renforcent la sécurité en créant une barrière supplémentaire aux systèmes de piratage automatisés.

Activité d'apprentissage 2

Discussion de groupe - Questions et réponses, évaluation et retour d'information (10 minutes maximum)

Questions recommandées pour l'évaluation :

- Qu'est-ce que c'est l'authentification ?
- Pourquoi l'authentification est-elle importante ?
- Quelles sont les méthodes d'authentification les plus courantes actuellement utilisées et quelles sont leurs principales caractéristiques ?

UNITÉ 2 - MOT DE PASSE

Activité d'apprentissage 1

1. CE QUE VOUS NE DEVRIEZ PAS FAIRE

Diapositives avec des images qui illustrent les choses que les gens ne devraient pas faire, afin d'attirer l'attention du public.

ÉTUDES DE CAS

- "La police belge a affiché le mot de passe du WiFi. Cela a été montré à la télévision nationale"

https://www.reddit.com/r/cybersecurity/comments/cnkhft/the_belgian_police_have_a_post_it_with_the_wifi/

- Un mot de passe de l'agence d'urgence d'Hawaï était caché sur une photo publique, écrit sur un Post-it" - https://www.businessinsider.com/hawaii-emergency-agency-password-discovered-in-photo-sparks-security-criticism-2018-1
- "Quatre fuites embarrassantes de mots de passe en direct à la télévision" - https://www.itgovernance.co.uk/blog/four-embarrassing-password-leaks-on-live-tv

2. STATISTIQUES

Présentation de quelques statistiques :

- 81% des violations de données se produisent en raison d'une mauvaise sécurité des mots de passe.
- Mauvaises habitudes des employés en matière de mots de passe
- Le top 200 des mots de passe les plus courants.

3. L'IMPORTANCE D'UN MOT DE PASSE SÛR

L'anatomie d'un mot de passe inviolable

4. RÈGLES DE BASE

Décrire un ensemble de règles de base comme :

- Éviter d'utiliser les gestionnaires de mots de passe du navigateur ; c'est un moyen facile pour un " malware " d'y accéder.
- Ne partagez pas votre mot de passe.
- Mémorisez les mots de passe, ne les enregistrez pas sur papier ou numériquement
- Changez régulièrement les mots de passe.

(tous les deux mois au moins)

- Si possible, activez l'authentification à deux facteurs.
- Chaque mot de passe ne doit être utilisé que sur une seule plateforme.
- Changer le mot de passe d'origine lors de l'achat d'un appareil.
- Ne pas utiliser de mots courants . L'un des types d'attaque les plus fréquents est celui du "dictionnaire".

Règles pour un mot de passe plus sûr :

- Créer des mots de passe complexes : au moins 12 caractères, avec des majuscules et des minuscules, des chiffres et des caractères spéciaux. avec des chiffres et des caractères spéciaux
- N'utilisez pas de termes facilement " découvrables ", qui comprennent généralement : le nom, la ville de naissance, ou des des termes connus, le nom de l'animal de compagnie, le numéro d'immatriculation de la voiture, le numéro de téléphone portable, les anniversaires des membres de la famille, etc.

Mémorisez au lieu d'enregistrer :

- Créer une "clé" personnelle, qui fait partie de tous les mots de passe.
- Utiliser un dicton, des expressions courantes, ou quelque chose de facile à mémoriser.
- Par exemple, utilisez les deux premières lettres de chaque mot.
- Passez des majuscules aux minuscules et aux symboles.
- Ajouter quelque chose qui s'associe au site/outil

Activité d'Apprentissage 2

Exercice de groupe

Testez la longueur de votre mot de passe ! - https://www.passwordmonster.com

Ai-je déjà été craqué ? - https://haveibeenpwned.com/Passwords

Discussion et réactions (10 minutes maximum)

Questions recommandées pour l'évaluation :

- Combien d'années votre mot de passe résiste-t-il à une machine à algorithme de craquage normal ?
- Dois-je changer mon mot de passe ?

Activité d'apprentissage 3

Le formateur présente aux apprenants un exposé dont le contenu est suggéré ci-dessous (20 minutes maximum).
minutes) :

Que sont les gestionnaires de mots de passe ?

Des coffres-forts numériques
Permettent de stocker les informations d'identification et les notes de divers services.
Les coordonnées bancaires peuvent également être sauvegardées.
Une seule clé maîtresse
L'authentification biométrique peut être utilisée

Gestionnaires de mots de passe locaux

Sauvegarder les données sur l'appareil actuel.
Le fichier de mots de passe est crypté.
Chaque mot de passe doit être enregistré dans un fichier crypté distinct.
Ne peut être utilisé que sur un seul appareil.
Exemple comme KeePassXC

Gestionnaires de mots de passe en ligne

Les données sont stockées dans le nuage.
Permettent d'accéder aux informations d'identification et aux notes de divers services sur n'importe quel appareil.
Aucune installation requise
Une seule clé maîtresse
Les données sont cryptées de l'appareil au serveur.
Exemples de gestionnaires de mots de passe en ligne : Bitwarden, Latspass, Keeper et 1Password.

Activité d'apprentissage 4

Travaux pratiques en groupe

- Créer un mot de passe complexe
- Installez un gestionnaire de mots de passe sur votre ordinateur portable ou votre smartphone
- Activer l'AMF

Discussion et réactions (max. 10 minutes)

Questions recommandées pour l'évaluation :
A quel point cela a-t-il été difficile ?
Utiliserez-vous ces meilleures pratiques ?

2. Résultats d'apprentissage pour le module

Connaissances

- Comprendre la définition de l'authentification, son importance et les méthodes d'authentification les plus courantes et des méthodes d'authentification les plus courantes
- Comprendre les risques de ne pas utiliser des mots de passe complexes.
- Utiliser les meilleures pratiques de gestion des mots de passe personnels.

Skills

- Identifier et appliquer la méthode d'authentification la plus adéquate et la plus appropriée.
- Identifiez et appliquez la complexité de mot de passe la plus adéquate et la plus appropriée.

Compétences

- Percevoir l'importance de l'authentification.
- Décider de la méthode d'autorisation la plus appropriée pour différentes activités en ligne et les appliquer pour renforcer la sécurité en ligne
- Percevoir l'importance de l'utilisation de mots de passe complexes.
- Structurer les techniques de bonnes pratiques pour gérer les mots de passe personnels.

3. Bibliographie

https://www.sangfor.com/blog/cybersecurity/the-basics-of-authentication-in-cyber-security
https://www.passportalmsp.com/blog/which-password-authentication-method-works-best-businesses

MODULE DE FORMATION SUR LA SÉCURITÉ DU WI-FI

Module 5

1. Aperçu du module

Groupe cible

- Éducateurs en EFP
- Apprenants de l'EFP
- Parties prenantes publiques et privées intéressées par l'amélioration des connaissances et de la sensibilisation aux menaces de cybersécurité

Plan du module

Le présent module se concentre sur la mise en lumière des menaces réelles se connectant aux systèmes wifi publics, leur fonctionnement et, finalement, la manière de les prévenir.

Objectifs d'apprentissage

- Sensibilisation aux idées fausses concernant l'utilisation des réseaux wifi publics.
- Fournir des connaissances sur les menaces encourues par l'utilisation des réseaux wifi publics.

Durée totale

1 heure

Unité 1

Le module comprend des parties d'apprentissage vidéo et des discussions ouvertes. Plus précisément, dans un premier temps une première vidéo d'introduction sera présentée. Cette vidéo démontre, avec l'aide d'un expert, comment les réseaux publics sont un endroit risqué pour se connecter à l'internet. Néanmoins, cette première vidéo est très courte et ne permet pas de saisir l'essentiel du processus sous-jacent. Cette première partie se termine ensuite par une discussion entre les apprenants

Unité 2

Dans un deuxième temps, une vidéo plus spécifique sera prise en compte. Malgré sa manière informelle d'aborder le sujet, elle permet de mieux le comprendre. Une fois la vidéo terminée, l'animateur est invité à lancer une discussion entre les participants sur les risques des réseaux publics et, si possible, de partager leurs expériences personnelles.

Activité d'apprentissage 1

L'un des aspects sur lesquels ce module veut attirer l'attention est la facilité avec laquelle les menaces liées au wifi public sont mises en avant. Une activité d'apprentissage continu consiste à essayer d'appliquer les suggestions apprises à travers les contenus vidéo de ce module, du restaurant/bar où les participants où les participants prendront leur pause déjeuner, jusqu'à la gare et l'aéroport où s'arrêteront pour rentrer chez eux après la mobilité

2. Bibliographie

https://www.youtube.com/watch?v=4YbXXW3DLQM&ab_channel=Techquickie
https://www.youtube.com/watch?v=1OVTmrXGHyU&ab_channel=CBSBoston
https://www.kaspersky.com/resource-center/preemptive-safety/public-wifi-risks
https://goodspeed.io/blog/7-dangers-of-public-wifi.html
https://www.youtube.com/watch?v=NkNgW3TwMy8&ab_channel=TheModernRogue

L'UTILISATION DES RÉSEAUX SOCIAUX

Module 6

1. Aperçu du module

Groupe cible

- Educateurs de l'EFP
- Etudiants
- Représentants des institutions publiques actives dans les secteurs de l'éducation : municipalités, autorités régionales et nationales

Module Overview

Les réseaux sociaux en ligne (RSO) ont pris une place sans précédent dans les sphères professionnelle, éducative et privée de la vie quotidienne des gens, y compris celle des éducateurs de l'EFP et des enseignants, professionnelles, éducatives et privées, y compris celles des éducateurs de l'EFP et de leurs étudiants. Alors que les avantages d'une telle intégration ont été plus faciles à reconnaître et à adopter en tant que partie intégrante de l'éducation formelle et informelle les risques multiples qui y sont associés n'ont pas reçu l'attention qu'ils méritent et sont souvent ignorés par éducateurs eux-mêmes.

L'approche simpliste souvent utilisée à l'égard de la question multiforme de la sécurité des réseaux sociaux, ainsi que la complexité de certains matériels de formation disponibles, ne sont pas suffisent à créer la capacité requise pour prévenir et répondre aux menaces posées par l'utilisation de ces plateformes. Ce module tentera d'apporter aux apprenants un ensemble de connaissances de base et de renforcer leur capacité de formation, mais aussi d'améliorer leur propre approche de la sécurité des réseaux sociaux.

Objectifs d'apprentissage

- Comprendre les cyberrisques et les menaces associés à l'utilisation des réseaux sociaux
- Renforcer l'impact des processus de désinformation sur la sécurité des plateformes de CGU
- Identifier les différents types de menaces pour la cybersécurité
- Renforcer la capacité à prévenir et à répondre aux cybermenaces sur les médias sociaux
- Fournir des techniques pour gérer des mots de passe facilement complexes

Durée totale

2 heures

L'UTILISATION DES RÉSEAUX SOCIAUX

Module 6

Unité 1 - Menaces liées aux médias sociaux

Cette unité sera facilitée par l'utilisation d'une présentation Power Point et introduite par la lecture de titres d'actualité présentant des histoires très répandues de victimes de cybermenaces via les réseaux sociaux (photos de VIP volées, personnes ayant perdu la vie à cause de fausses nouvelles sur la vaccination, etc...)
Les histoires et le contenu seront adaptés au contexte et mis à jour en fonction des dernières découvertes.
La présentation est suivie d'une discussion en groupe de 10 minutes afin de réfléchir à l'apprentissage et d'évaluer la capacité des apprenants à comprendre le sujet, mais aussi de créer un espace pour d'autres questions et un retour d'information.

Activité d'apprentissage 1

Le formateur présente aux apprenants une présentation du contenu suggéré suivant (max. 20 minutes) :

Qu'est-ce qu'un réseau social en ligne ?

Un réseau social en ligne (RSE) est une structure sociale composée d'individus ou d'organisations, appelés nœuds, reliés par un ou plusieurs types spécifiques d'interdépendance, tels que l'amitié, l'intérêt commun, et l'échange de finances, de relations de croyances, de connaissances, ou le prestige. Les sites de réseaux sociaux tels que Facebook, Twitter, Instagram, etc. ne sont pas seulement utilisés pour communiquer ou interagir avec d'autres personnes dans le monde, mais aussi un moyen efficace de promotion des entreprises. Contrairement aux plateformes traditionnelles du web et des médias, les médias sociaux sont exclusivement dédiés à l'hébergement et à la distribution de contenus générés par les utilisateurs (CGU) selon des critères (algorithmes) basés sur les actions et les préférences exprimées par les utilisateurs eux-mêmes et enregistrées dans les données.
En ce sens, tous les utilisateurs sont des participants actifs à la durabilité des processus des réseaux sociaux.

Qu'est-ce qu'une menace liée aux médias sociaux ?

Une menace liée aux médias sociaux peut être tout ce qui compromet la sécurité d'un compte. Une cyber menace peut être à la fois intentionnelle et non intentionnelle, ciblée ou non, et elle peut et peut provenir de diverses sources, notamment de nations étrangères pratiquant l'espionnage et la guerre de l'information, des criminels, des pirates informatiques, des auteurs de virus, des employés mécontents et des sous-traitants qui travaillent au sein d'une organisation.

À quoi ressemble une menace liée aux médias sociaux

Les réseaux sociaux comptent un nombre considérable d'utilisateurs et stockent d'énormes quantités de données, ils sont des cibles naturelles pour les spammeurs, le phishing et les attaques malveillantes. D'ailleurs, les attaques sociales en ligne incluent l'usurpation d'identité, la diffamation, le harcèlement, l'atteinte à la dignité personnelle et la cyberintimidation. Les pirates créent de faux profils et imitent des personnalités ou des marques, ou calomnient un individu connu au sein d'un réseau d'amis.

Pour des raisons de protection de la vie privée, les profils d'utilisateurs ne doivent jamais publier et diffuser des informations sur le web. Les informations figurant sur les pages d'accueil personnelles peuvent contenir des données très sensibles telles que les dates de naissance, les adresses personnelles, portable personnels, etc. Ces informations peuvent être utilisées par des pirates informatiques qui utilisent des techniques d'ingénierie sociale pour tirer profit de ces informations sensibles et voler de l'argent.

Comment les menaces liées aux médias sociaux évoluent selon les plateformes

La manière dont une menace liée aux médias sociaux est mise en œuvre par un attaquant dépend de ses objectifs. Facebook permet aux utilisateurs de garder leurs images et leurs commentaires privés, Ainsi, un attaquant sera souvent ami avec les amis d'un amis d'un utilisateur ciblé ou envoie directement une demande d'ami à un utilisateur ciblé pour accéder à ses publications. LinkedIn est une autre cible commune des médias sociaux, connue pour la mise en réseau des entreprises. Si un attaquant cible une entreprise, LinkedIn est un excellent site de médias sociaux pour recueillir des d'affaires pour une attaque de phishing. Comme de nombreuses plateformes de médias sociaux affichent publiquement les utilisateurs, les attaquants peuvent collecter des données en silence, à l'insu de l'utilisateur. Certains attaquants d'accéder aux informations des utilisateurs en contactant les utilisateurs ciblés ou leurs amis.

Pourquoi est-il important de parler des menaces OSN ?

Au 30 décembre 2020, il y a près de 4 milliards d'utilisateurs dans le monde de l'Internet. Sur l'ensemble de la population totale sur Internet, on compte 2,7 milliards de clients dynamiques mensuels sur Facebook, 330 millions d'utilisateurs actifs sur Twitter et 320 millions d'utilisateurs actifs sur Pinterest. L'utilisation des sites de réseaux sociaux connaît une croissance exponentielle. Si on considère uniquement Facebook, sept nouveaux profils sont créés chaque seconde, 510 000 commentaires sont postés chaque 60 secondes, 298 000 statuts sont mis à jour, et 136 000 photos sont téléchargées dans le même temps. Puisqu'une énorme quantité de données est téléchargée, le risque de faille de sécurité est élevé. N'importe qui peut publier des contenus malveillants cachés dans des données multimédias ou dans des localisateur uniforme de ressource (URL - uniform resource locator). Il existe environ 83 millions de faux profils correspondant à des utilisateurs illégitimes ou à des professionnels effectuant des tests et des recherches. Environ 100 000 sites web sont piratés chaque jour.

Bien que certains sites de réseautage social comme Twitter ne permettent pas de divulguer des informations privées aux utilisateurs, certains attaquants expérimentés peuvent déduire des informations confidentielles en analysant les messages des utilisateurs et les informations qu'ils partagent en ligne. Les informations personnelles que nous partageons en ligne peuvent permettre aux cybercriminels d'obtenir nos adresses électroniques et nos mots de passe.

La valeur des données personnelles

Les réseaux de médias sociaux offrent souvent leurs services gratuitement. Les informations personnelles ne sont pas seulement la monnaie d'échange des réseaux de médias sociaux, mais aussi le principal objectif des cybermenaces sur les
sociaux. Il peut être facile de lancer une attaque car de nombreuses personnes communiquent généralement leurs informations sur les plateformes de médias sociaux. Les attaquants peuvent facilement collecter ces données et les utiliser à des fins lucratives. La collecte d'informations à voler n'est qu'un type de médias sociaux pour la reconnaissance. Le site informations postées sur les médias sociaux peuvent être utilisées pour obtenir des mots de passe ou se faire passer pour utilisateurs professionnels. Avec une liste de cibles, un attaquant pourrait alors passer en revue les comptes de médias sociaux à la recherche d'informations personnelles. Les informations personnelles peuvent aider l'attaquant à gagner la confiance de la cible dans le cadre d'une attaque par ingénierie sociale. Elles peuvent également être utilisées pour deviner les réponses aux questions de sécurité pour une prise de contrôle d'un compte ou être utilisées pour se rapprocher d'un utilisateur disposant de privilèges plus élevés. Les noms des animaux domestiques, les équipes sportives préférées et l'historique des études sont autant d'indices potentiels de mots de passe ou de réponses à des questions utilisées pour vérifier l'identité de l'utilisateur. questions utilisées pour vérifier l'identité de l'utilisateur afin de réinitialiser un mot de passe.

Pourquoi se renseigner sur les menaces OSN ?

Les interfaces et les processus conviviaux proposés par ces plateformes pourraient faire penser à des personnes ne possédant pas les connaissances ou les compétences requises pour accéder en toute sécurité à leurs services et à leurs contenus.

Education is key to stopping online social network threats. L'éducation est la clé pour mettre fin aux menaces des réseaux sociaux en ligne. La première étape consiste à éduquer les utilisateurs sur les dangers de divulguer trop d'informations en ligne au public. Même les comptes de médias sociaux définis comme privés peuvent être utilisés dans le cadre d'une attaque si l'attaquant obtient l'accès aux flux privés. Les utilisateurs ne doivent jamais publier d'informations privées
sur leurs comptes de médias sociaux ou des informations qui pourraient être utilisées dans le cadre d'une prise de contrôle du compte.

La deuxième étape consiste à éduquer les utilisateurs sur la manière dont les contenus numériques sont produits et distribués, et comment ils peuvent inciter les utilisateurs à agir en fonction des objectifs spécifiques pour lesquels le contenu a été créé.
Tous les contenus des médias sociaux sont créés et véhiculés par les utilisateurs en fonction de leurs différents objectifs personnels et/ou collectifs.
Pour ces raisons, certains de ces contenus ne sont pas toujours pratiques, vrais ou éthiques.
Enfin, les utilisateurs doivent être sensibilisés à l'utilisation et à la maintenance sûres des appareils par lesquels ils accèdent aux services de réseaux sociaux en ligne.
ils accèdent aux services de réseaux sociaux en ligne, car ceux-ci sont normalement des vecteurs de risques et intrusion. Certains points éducatifs à cet égard sont déjà illustrés dans d'autres modules de formation et incluent :

- Évitez de cliquer sur les publicités, en particulier les fenêtres pop-up qui demandent aux utilisateurs de télécharger un logiciel pour visualiser le contenu.
- Ne partagez pas vos mots de passe.
- Évitez les messages ou les publications sur les médias sociaux incitant à des actions rapides comme une technique d'ingénierie sociale.
- Ne pas accepter les demandes d'apparence amicale de personnes inconnues, même si l'utilisateur a plusieurs amis en commun.
- Évitez d'utiliser les sites de médias sociaux sur les hotspots wi-fi publics (un endroit courant pour les attaquants pour espionner les données en utilisant des attaques de type man-in-the-middle [mitm]).
- Changer régulièrement les codes d'accès et les mots de passe.

Activité d'apprentissage 2

Demandez aux apprenants de rechercher leur propre nom sur un moteur de recherche exploité par un média social ou sur Google, et d'énumérer toutes les informations privées qui peuvent être détectées par les multiples contenus trouvés (lieu et date de naissance, détails et informations sur les membres de la famille, adresses, numéros de téléphone, animaux domestiques, partenaires romantiques, loisirs et préférences). Invitez-les à réfléchir aux façons dont ces informations pourraient être utilisées contre eux.

Unité 2 - Type de menaces OSN

Activité d'apprentissage 1

Demande aux apprenants d'énumérer toute menace de sécurité qu'ils pensent pouvoir rencontrer sur les médias sociaux et demande-leur d'expliquer s'ils pensent que cette menace pouvait exister avant l'existence de l'OSN.

DIVERSES MENACES SUR LES RÉSEAUX SOCIAUX ET LES MÉDIAS EN LIGNE

Nous pouvons diviser les menaces OSN en trois catégories :

1. Les menaces conventionnelles comprennent les menaces que les utilisateurs connaissent depuis les premiers des réseaux sociaux.
2. Les menaces modernes sont des attaques qui utilisent des techniques avancées pour compromettre les comptes des utilisateurs.
3. Les attaques ciblées sont des attaques qui visent un utilisateur particulier.

MENACES CONVENTIONNELLES

Spam

Le spam est le terme utilisé pour les messages électroniques non sollicités en masse. Bien que le courrier électronique soit le conventionnel de diffusion du spam, les plates-formes de réseaux sociaux ont plus de succès dans la de spam. Les détails de communication des utilisateurs légitimes peuvent facilement être obtenus à partir des sites Web des entreprises, des blogs et des groupes de discussion. Il n'est pas difficile de convaincre le client ciblé de lire les messages de spam et de croire qu'il est protégé. La plupart des spams sont des publicités commerciales, peut également être utilisé pour collecter des informations sensibles auprès des utilisateurs ou peut contenir des virus, des logiciels malveillants ou des escroqueries.

Attaque de malware

Un malware est une application programmée qui est explicitement conçue pour contaminer ou accéder à un système informatique, généralement à l'insu de l'utilisateur.
Les logiciels malveillants peuvent utiliser la structure sociaux pour se propager par le biais d'URL partagées ou d'applications sous-OSN telles que des jeux électroniques ou des plugins.

Attaque par hameçonnage

Une attaque par hameçonnage est un type d'attaque d'ingénierie sociale au cours de laquelle l'agresseur peut acquérir des informations sensibles et confidentielles comme le nom d'utilisateur, le mot de passe et les détails de la carte de crédit d'un utilisateur par le biais de faux sites Web et d'e-mails qui semblent réels.

Dans le cas de l'OSN, un assaillant doit attirer le client vers une fausse page où il peut exécuter une attaque de phishing. Pour cela, l'agresseur utilise différentes méthodes d'ingénierie sociale. Par exemple, il peut envoyer un message à un utilisateur qui dit : "Vos photos personnelles sont partagées sur ce site Web vérifiez-les !". En cliquant sur cette URL, l'utilisateur est redirigé vers un faux site Web qui ressemble à un site de réseau social légitime.

MENACES MODERNES

Attaque par scripting intersite

Ce script est renvoyé à la victime par boomerang et est exécuté sur le navigateur. Des liens et des boutons attrayants sur des sites de médias sociaux populaires comme Twitter et Facebook peuvent inciter l'utilisateur à suivre des URL, ainsi que des alertes de virus pop-up et des publicités ou contenus multimédias prometteurs qui nécessitent de visiter un lien ou de cliquer sur un bouton pour être débloqués.
Certains utilisateurs peuvent être invités à copier et coller des JavaScript contenant des liens dans la barre d'adresse de leur navigateur.
Ces attaques peuvent soit voler des informations, soit agir comme des logiciels espions.
Elles peuvent également détourner des ordinateurs pour lancer des attaques sur des utilisateurs peu méfiants alors que le véritable auteur de l'attaque est caché derrière la machine compromise.

Attaque par clonage de profil

Dans cette attaque, l'agresseur clone le profil des utilisateurs grâce à des connaissances préalables ou à des informations recueillies en ligne. L'agresseur peut utiliser ce profil cloné dans la même ou dans une autre plateforme de réseau social pour créer une relation de confiance avec les amis de l'utilisateur réel. Une fois la connexion établie, l'attaquant amène les amis de la victime à croire à la validité du faux profil et à accéder avec succès à des informations confidentielles qui ne sont pas partagées dans leur espace public. Cette attaque peut également être utilisée pour commettre d'autres types de cybercrimes comme la cyberintimidation, le cyberharcèlement et le chantage.

Détournement d'identité

Dans le cas d'un détournement, l'adversaire compromet ou prend le contrôle du compte d'un utilisateur pour réaliser une fraude en ligne. Les sites ne disposant pas d'une authentification multifactorielle et les comptes avec des mots de passe faibles sont plus vulnérables au détournement, car les mots de passe peuvent être obtenus grâce au hameçonnage. Une fois le compte détourné, le pirate peut envoyer des messages, partager le lien , et modifier les informations du compte, ce qui compromet le contrôle de l'utilisateur sur son propre compte, ainsi que sa réputation.

Attaque par inférence

L'attaque par inférence déduit les informations confidentielles d'un manipulateur que l'utilisateur peut ne pas vouloir divulguer, à travers d'autres statistiques publiées par l'utilisateur sur un OSN. Elle utilise des procédures d'exploration de données sur des données visiblement disponibles comme la liste d'amis de l'utilisateur et la topologie du réseau.
Grâce à cette technique, un attaquant peut trouver les informations secrètes d'une organisation ou les informations géographiques et éducatives d'un utilisateur.

Sybil attack / Botnet

Dans l'attaque Sybil, un nœud revendique plusieurs identités dans un réseau. Elle peut être nuisible aux plateformes de sociales, car elles contiennent un grand nombre d'utilisateurs couplés par un réseau de pair à pair. Les pairs sont les cadres informatiques qui sont associés les uns aux autres par l'internet et peuvent partager des données sans besoin d'un serveur central. Ce réseau de machines peut également être appelé BotNet.
Une entité
en ligne peut créer plusieurs fausses identités et les utiliser pour diffuser des informations indésirables, des logiciels malveillants ou même affecter la réputation et la popularité d'une organisation. Par exemple, une enquête en ligne peut être manipulée à l'aide de diverses livraisons de protocoles Internet (IP) pour soumettre un nombre énorme de votes, et l'agresseur peut mettre en minorité un client authentique.
Une armée similaire peut par exemple partager un même message plusieurs fois et rendre son contenu viral.

Clickjacking

Le "clickjacking" est une procédure dans laquelle l'envahisseur trompe un utilisateur pour qu'il clique sur une page qui est différente de celle sur laquelle il avait l'intention de cliquer. L'attaquant exploite la vulnérabilité des navigateurs pour réaliser cette attaque. Il charge une autre page sur la page à laquelle l'utilisateur veut accéder, comme une couche transparente. Les deux variantes connues du clickjacking sont le likejacking
et le cursorjacking. La couche avant montre la substance avec laquelle le client peut être appâté.
Au moment où le client tape sur ce contenu, il appuie en fait sur le bouton "J'aime". Plus d'individus aiment le message, plus il se répand. Dans le cas du cursor jacking, un attaquant remplace le curseur actuel par une image de curseur personnalisée. Le curseur actuel est déplacé de la position actuelle de la souris. De cette manière, l'intrus peut inciter un consommateur à cliquer sur le site malveillant grâce à un positionnement astucieux des éléments de la page.

Attaque de désanonymisation

Sur un grand nombre de sites de réseautage social comme Twitter et Facebook, les utilisateurs peuvent cacher ou protéger leur identité réelle avant de publier des données en utilisant un alias ou un nom inventé. Mais si un tiers veut connaître la véritable identité de l'utilisateur, il peut le faire en suivant les cookies, les topologies de réseau, et l'inscription à un groupe d'utilisateurs pour découvrir l'identité réelle du client. Il s'agit une sorte de méthode d'extraction d'informations dans laquelle des informations mystérieuses sont croisées avec d'autres sources d'information afin de reconnaître à nouveau l'information inconnue. Un attaquant peut collecter des informations sur l'appartenance à un groupe d'un utilisateur en volant l'historique de son navigateur et en avec les données collectées. L'attaquant peut ainsi désanonymiser l'utilisateur qui visite le site web de cet attaquant.

MENACES CIBLÉES

Cyberintimidation

La cyberintimidation est l'utilisation de médias électroniques tels que les courriels, les chats, les conversations téléphoniques et les réseaux sociaux en ligne pour intimider ou harceler une personne. Contrairement à l'intimidation traditionnelle, la cyberintimidation est un processus continu puisqu'il est entretenu en permanence par les médias sociaux. L'agresseur envoie de manière répétée des messages d'intimidation, des remarques à caractère sexuel, des rumeurs, et parfois publie des photos ou des vidéos embarrassantes pour harceler une personne. Il peut également publier des informations personnelles ou privées de la victime, ce qui peut la mettre dans l'embarras ou l'humilier.

La cyberintimidation peut également être accidentelle, bien que la répétition de tels courriels, textes et messages en ligne sont rarement accidentels.

Cyber toilettage

Le cyber toilettage (aussi cyber grooming) consiste à établir une relation intime et émotionnelle avec la victime (généralement des enfants et des adolescents) dans l'intention d'imposer des abus sexuels ou mentaux. L'objectif principal de cette pratique est d'obtenir la confiance de l'enfant. Le but principal de la sollicitation en ligne est de gagner la confiance du jeune et de lui soutirer des informations intimes et individuelles. Les données sont souvent
voluptueuses par le biais de conversations, de photos et de vidéos à caractère sexuel, ce qui donne à l'attaquant un avantage pour menacer et faire chanter l'enfant.

Les agresseurs approchent souvent les adolescents ou les enfants par le biais d'une fausse identité sur des sites adaptés aux enfants, les rendant ainsi vulnérables et inconscients du fait qu'ils ont été attirés vers eux dans le but ultime de cyber toilettage. Cependant, la victime peut aussi déclencher sans le savoir le processus de " toilettage " lorsque lorsqu'elle reçoit des offres gratifiantes, par exemple de l'argent en échange de coordonnées ou de photos personnelles. L'anonymat et l'accessibilité des médias avancés permettent aux "groomers" d'approcher plusieurs jeunes simultanément, ce qui augmente de façon exponentielle les cas de cyber toilettage.

Cyberharcèlement

Le cyberharcèlement est l'observation d'une personne par le biais d'Internet, du courrier électronique ou d'un autre type de correspondance électronique, qui fait craindre la violence et porte atteinte à la paix mentale de cette personne. Elle implique l'atteinte au droit à la vie privée d'une personne. L'attaquant traque les informations personnelles ou confidentielles des victimes et les utilise pour les menacer par des messages continus et persistants tout au long de la journée. Ce comportement rend la victime exceptionnellement inquiète pour sa propre sécurité et déclenche chez elle un type de trouble, peur ou de perturbation. De nos jours, la plupart des individus partagent leurs informations personnelles, comme leur numéro de téléphone, leur lieu de résidence, leur région et leur emploi du temps, dans leur profil de réseau social, ainsi que dans leur vie privée, ainsi que l'endroit où ils vivent. Un agresseur peut recueillir ces données et les utiliser pour le cyberharcèlement.

Activité d'apprentissage 2

Demandez aux apprenants de travailler par deux et demandez-leur de se faire passer pour leur partenaire respectif pendant qu'ils les interviewent pendant 10 minutes.
Invitez-les à tenter leurs réponses en essayant d'obtenir les informations requises à partir de leur façon de s'habiller, des gadgets qu'ils portent sur eux et tout autre détail contextuel qu'ils pourraient trouver utile pour se faire passer pour eux.

Activité d'apprentissage 3

Demandez aux apprenants de faire défiler leurs flux de médias sociaux pendant 1 minute et de compter tous les call-to-actions, liens et boutons sur lesquels ils sont invités à cliquer. Invitez-les à une réflexion de groupe sur comment chacun de ces liens représente une menace potentielle et comment ils doivent décider quand et quand ne pas interagir avec le contenu.

Unité 3 - Conseils pour la protection des réseaux sociaux

Activité d'apprentissage 1

Distribuez à chaque apprenant une ou plusieurs cartes proposant des captures d'écran de publications (inventées) provenant de différentes plateformes et invitez-les à identifier les informations sensibles qu'ils peuvent obtenir à partir d'une seule publication et quelles menaces possibles peuvent provenir de cette publication.

L'UTILISATION DES RÉSEAUX SOCIAUX

Module 6

QU'EST-CE QUE LA PROTECTION DES MÉDIAS SOCIAUX

Les directives de protection des médias sociaux ont pour but d'empêcher tout accès non autorisé à vos comptes de médias sociaux, protéger votre identité en ligne contre les usurpations d'identité ou le vol de données, et protéger votre réseau contre les identités ou les contenus de médias sociaux malveillants.

Parce que les modalités et les objectifs des menaces OSN dépendent souvent du type de plateforme, certaines pratiques spécifiques pour prévenir les menaces doivent également être prises en compte en conséquence.

PRATIQUES GÉNÉRALES

Utiliser un mot de passe fort : pour maintenir la sécurité des comptes, les utilisateurs doivent choisir un mot de passe fort. Il ne doit pas être trop court, car les mots de passe courts peuvent être facilement devinés. Il doit être suffisamment long et doit contenir des valeurs alphanumériques et quelques caractères spéciaux.

Les utilisateurs ne doivent pas utiliser le même mot de passe que celui qu'ils utilisent pour d'autres comptes car si un attaquant parvient à connaître ce mot de passe, il peut compromettre tous les comptes de l'utilisateur.

Limiter le partage de la localisation : De nos jours, le partage de la localisation est devenu une tendance. De nombreux sites de sociaux ont également introduit une fonctionnalité de géolocalisation, qui marque automatiquement l'emplacement géographique d'un utilisateur lorsque celui-ci télécharge un contenu multimédia sur les médias sociaux.

L'utilisateur doit passer en mode manuel, afin que la géolocalisation ne soit pas automatique. Les utilisateurs doivent charger leur contenu multimédia en ligne avec beaucoup de précaution, car il peut contenir des métadonnées sensibles, et il est recommandé de passer la géolocalisation en mode manuel sur tous leurs appareils mobiles et comptes.

Soyez sélectif avec les demandes d'amis : il a été observé que de nombreux utilisateurs acceptent les demandes d'amis sans analyser le profil complet de l'auteur de la demande. Les gens acceptent généralement demandes d'amis sur la base d'amis communs. Si le demandeur a des amis communs, ils l'acceptent. Parfois, les attaquants rendent leur profil délibérément attrayant ou ils peuvent usurper l'identité d'un compte. Ainsi, si la personne qui envoie une demande d'ami est inconnue, il convient d'ignorer cette demande d'ami. Il peut s'agir d'un faux compte qui tente de dérober des informations sensibles.

Faites attention à ce que vous partagez : les utilisateurs doivent faire attention à leurs messages, car ils peuvent révéler leurs informations personnelles et parfois celles des autres personnes. De nombreuses organisations appliquent des règles strictes en matière de partage d'informations et de contenu multimédia. Il y a de nombreux cas de personnes licenciées pour avoir partagé des informations illégalement.

Cette situation peut être évitée si les employés sont bien informés des protocoles de l'organisation dans laquelle ils travaillent concernant les photos, vidéos et messages qu'ils publient en ligne. Le partage illégitime d'informations peut nuire à la réputation d'une organisation sur le marché, ainsi qu'à ses données et à sa propriété intellectuelle.

Faites attention aux liens et aux applications tierces : Des utilisateurs illégitimes peuvent accéder au compte d'une personne et obtenir des informations sensibles en partageant un lien malveillant.

De nos jours, les URL raccourcies deviennent très populaires sur diverses plateformes de médias sociaux. Ces URL raccourcies peuvent être obscurcies par un code ou un script malveillant. Ces scripts essaient de recueillir les informations personnelles et confidentielles d'un utilisateur, ce qui peut servir à violer la vie privée de cet utilisateur. En outre, les pirates peuvent profiter des vulnérabilités présentes dans une application tierce qui est intégrée à de nombreux réseaux sociaux populaires. Un exemple d'une telle application tierce est constitué par les jeux qui sont jouables sur les réseaux sociaux en ligne, et qui demandent les informations publiques d'un utilisateur pour utiliser leurs services. Ces informations peuvent être fournies à des personnes extérieures ou à des interventions de tiers. Pour éviter ce risque, les utilisateurs doivent être prudents lorsqu'ils installent des applications tierces dans leur profil.

Installez un logiciel de sécurité Internet : Certaines menaces dont le modèle est connu peuvent facilement être détectées par des antivirus. Des menaces telles que le cybergrooming, la cyberintimidation peuvent être détectées dans une certaine mesure en utilisant un logiciel antivirus.

PRATIQUES POUR LA PLATEFORME DE PARTAGE MULTIMÉDIA

Les réseaux professionnels sont principalement utilisés pour créer des contacts et accroître la visibilité auprès de des entreprises de recrutement potentielles. Ainsi, pour utiliser un réseau professionnel en toute sécurité, il convient d'examiner les détails fournis par les autres utilisateurs avant de les ajouter à sa liste de contacts. En général, un adversaire ne fournit pas beaucoup de détails sur sa carrière.

- Un utilisateur devrait vérifier s'il y a des fautes d'orthographe ou de grammaire dans le profil de quelqu'un, car si quelqu'un postule pour un emploi, il doit être très bien écrit et ne doit comporter de toute faute d'orthographe ou de grammaire. Il doit contenir des informations précises et bien présentées sur cette personne.
- Chercher la cohérence dans la carrière d'une personne peut être une bonne pratique si un utilisateur veut rester sécurité sur un réseau professionnel. Un profil qui change continuellement et définitivement sur une courte période de temps est la partie la plus utilisée par le fraudeur. Au moment où le fraudeur a besoin de cibler un type d'organisation ou un secteur vertical, il peut simplement ajouter une nouvelle position qui pourrait être pertinente pour ses cibles.

- Il faut également recouper les informations. Si une personne prétend être de l'entreprise de l'employeur, l'utilisateur peut vérifier l'annuaire de l'entreprise de l'employeur, l'utilisateur peut consulter l'annuaire de l'entreprise et ne doit pas hésiter à vérifier auprès du service des ressources humaines de l'entreprise.

Activité d'apprentissage 2

Demandez aux apprenants d'expliquer qui, selon eux, a accès au dernier post qu'ils ont publié sur leur OSN préféré. Enfin, aidez-les à vérifier leurs paramètres de confidentialité et à voir si ce qu'ils ont dit correspond à la vérité.
Ouvrez une discussion de groupe sur leurs résultats.

Activité d'apprentissage 3

Invitez les apprenants à regarder à nouveau les cartes qu'ils ont reçues au cours de l'activité d'apprentissage 1 de cette unité et demandez-leur s'ils peuvent identifier des risques supplémentaires dans les publications des médias sociaux présentées auparavant. Demandez-leur ce qu'ils feraient pour atténuer ces risques.

- Il faut également recouper les informations. Si une personne prétend être de l'entreprise de l'employeur, l'utilisateur peut vérifier l'annuaire de l'entreprise de l'employeur, l'utilisateur peut consulter l'annuaire de l'entreprise et ne doit pas hésiter à vérifier auprès du service des ressources humaines de l'entreprise.

Activité d'apprentissage 2

Demandez aux apprenants d'expliquer qui, selon eux, a accès au dernier post qu'ils ont publié sur leur OSN préféré. Enfin, aidez-les à vérifier leurs paramètres de confidentialité et à voir si ce qu'ils ont dit correspond à la vérité.
Ouvrez une discussion de groupe sur leurs résultats.

Activité d'apprentissage 3

Invitez les apprenants à regarder à nouveau les cartes qu'ils ont reçues au cours de **l'activité d'apprentissage 1** de cette unité et demandez-leur s'ils peuvent identifier des risques supplémentaires dans les publications des médias sociaux présentées auparavant. Demandez-leur ce qu'ils feraient pour atténuer ces risques.

2. Résultats d'apprentissage pour le module

Connaissances

- Cyber risques et menaces liés à l'utilisation des réseaux de médias sociaux.
- Sécurité des plateformes UGC (UGC = User Generated Content)

Skills

- Identification des différents types de menaces liées à la cybersécurité.

Compétences

- Prévenir et répondre aux cybermenaces sur les médias sociaux.
- Gérer des mots de passe complexes

3. Bibliographie

https://www.proofpoint.com/us/threat-reference/social-media-threats
https://www.digitalshadows.com/blog-and-research/how-cybercriminals-weaponize-social-media/
https://www.researchgate.net/publication/221663523_Cyber_Threats_In_Social_Networking_Websites
https://www.researchgate.net/publication/324860729_Social_Media_Security_Risks_Cyber_Threats_And_Risks_Prevention_And_Mitigation_Techniques

Co-funded by the
Erasmus+ Programme
of the European Union

YBER.VET.EU

AMÉLIORER LA PRÉPARATION À LA CYBERSÉCURITÉ DU SECTEUR EUROPÉEN DE L'ENSEIGNEMENT ET DE LA FORMATION PROFESSIONNELS

MATÉRIEL DE FORMATION

SENSIBILISATION À LA CYBERSÉCURITÉ MATÉRIEL DE FORMATION POUR LE SECTEUR DE L'EFP

NGO NEST Berlin
AEII
tandemplus network
Latvian European Community Studies Association
COFAC
EOS
inerciadigital
meath partnership

INTRO

De l'automne 2021, en lien avec le mois européen de la cybersécurité, au printemps 2022, les partenaires du projet CYBER.VET.EU ont organisé plusieurs GameJams dans les pays des partenaires. Les jeunes ont été impliqués en leur donnant l'opportunité d'être proches des sujets de cybersécurité et en leur fournissant de nouveaux outils.

L'objectif principal était de répondre au besoin de sensibilisation à la cybersécurité. Nous nous sommes tournés vers le processus de "gamification" afin d'obtenir une solution facile à adopter, rapide à mettre en œuvre, évolutive dans le temps et inclusive. Le processus de gamification, défini comme "l'application des mécanismes du jeu à des contextes non ludiques dans le but de susciter l'engagement et d'augmenter les niveaux de motivation", est un moyen éprouvé de maintenir les utilisateurs engagés dans des activités d'apprentissage, avec d'excellents résultats même sur une courte période grâce à l'exploitation du divertissement qui motive les participants à s'engager davantage avec le matériel et à pratiquer. En tant que tel, ce produit agira comme une combinaison de directives, de formation et de pratique, avec la caractéristique d'être facilement mis à jour lorsque du nouveau matériel doit être ajouté.

RÉSULTATS DES ACTIVITÉS / GAME JAMS

- Sensibilisation accrue à la sécurité numérique
- Sensibilisation accrue à la sécurité numérique au sein des communautés des participants (famille, amis, collègues)
- Réduction du taux de réussite des logiciels malveillants au sein des institutions
- Réduction du nombre de fuites de données
- Intérêt accru pour le secteur de la cybersécurité en tant qu'opportunité d'emploi.

AEII / INERCIA DIGITAL [ES]

ACTIVITES

Les activités les plus pertinentes menées par les partenaires espagnols AEII et Inercia Digital ont été les suivantes:

- Hackathon
- GameJams
- Journées d'information
- Conférence internationale
- Evénement de diffusion

RÉSULTATS

Les sessions GameJam en Espagne ont fourni des résultats utiles qui peuvent être consultés ici :https://www.youtube.com/watch?v=3QFI9iB0iJU&t=124s

SUR LE SCRATCH

https://scratch.mit.edu/projects/611211889/
Cybersécurité - Attaqué

https://scratch.mit.edu/projects/610354561/
en espagnol

https://scratch.mit.edu/projects/611201682/

https://scratch.mit.edu/projects/714361293/
en espagnol

https://scratch.mit.edu/projects/714362963/
en espagnol

https://scratch.mit.edu/projects/714362911/
sur le phishing - un remix

https://scratch.mit.edu/projects/606933322
sur le phishing - en anglais

AEII / INERCIA DIGITAL [ES]

GAME JAM

AEII / INERCIA DIGITAL [ES]

Hackathon

La cybersécurité dans l'éducation

Les partenaires espagnols AEII et Inercia Digital ont participé en ligne à un Hackathon du 20 au 22 octobre 2021, avec 47 participants, dont de nombreux experts en informatique. https://www.comprometidosporelfuturo.com/proyectos# soutenu par Boehringer Ingelheim en Espagne.

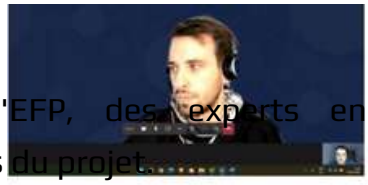
PROBLÈME À RÉSOUDRE

La cyberintimidation est l'un des principaux risques de l'internet pour les jeunes. Il est fréquent de trouver des messages au contenu offensant pour certaines personnes et que ceux-ci soient utilisés pour harceler et se moquer des victimes.

La cyberintimidation provoque souvent de graves perturbations chez les victimes, telles que le syndrome de stress post-traumatique, la dépression, les pensées et comportements suicidaires ou l'anxiété.

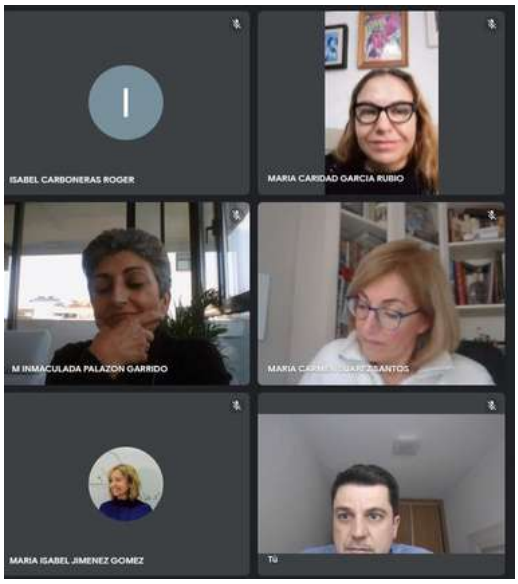
Ce défi consiste à étudier et à analyser les connaissances des jeunes en matière de sécurité, ainsi qu'à les sensibiliser aux risques qu'ils encourent dans leurs centres éducatifs et dans leur vie quotidienne.
Ce défi vise, par le biais de la gamification, à sensibiliser les élèves et les enseignants de la vie quotidienne aux questions liées à la sécurité dans l'utilisation des nouvelles technologies..

RÉSULTATS



- Jeu et animation liés à la cybersécurité dans l'enseignement
- Participation de l'administration publique, des écoles d'EFP, des experts en informatique, des enseignants, des étudiants et des partenaires du projet
- Création de courtes vidéos interactives

AEII / INERCIA DIGITAL [ES]



D'une manière générale, après avoir mené de nombreuses enquêtes, les connaissances en matière de cybersécurité des enseignants et des étudiants des centres de formation professionnelle sont encore faibles en Espagne. Pour cette raison, ce projet et d'autres similaires sont très pertinents en Espagne.

NGO NEST BERLIN [DE], EOS [IT] + IASIS [GR]

GAME JAM

L'ONG Nest Berlin, Extrafondente Open Source - EOS et IASIS ont organisé ensemble une session de GameJam en février 2022. La GameJam a débuté le samedi 12 et a duré 6 jours au total. Elle a vu les équipes nationales développer et travailler ensemble sur une ébauche de jeu (d'un jeu en ligne ou de plateau).

Un jury indépendant a été réuni et a été invité à évaluer le projet de jeu en suivant des directives communes et un modèle d'évaluation.

L'équipe gagnante a bénéficié d'un mentorat de 6 mois ainsi que de ressources techniques afin de poursuivre le développement de son idée de jeu.

A PROPOS DU JEU

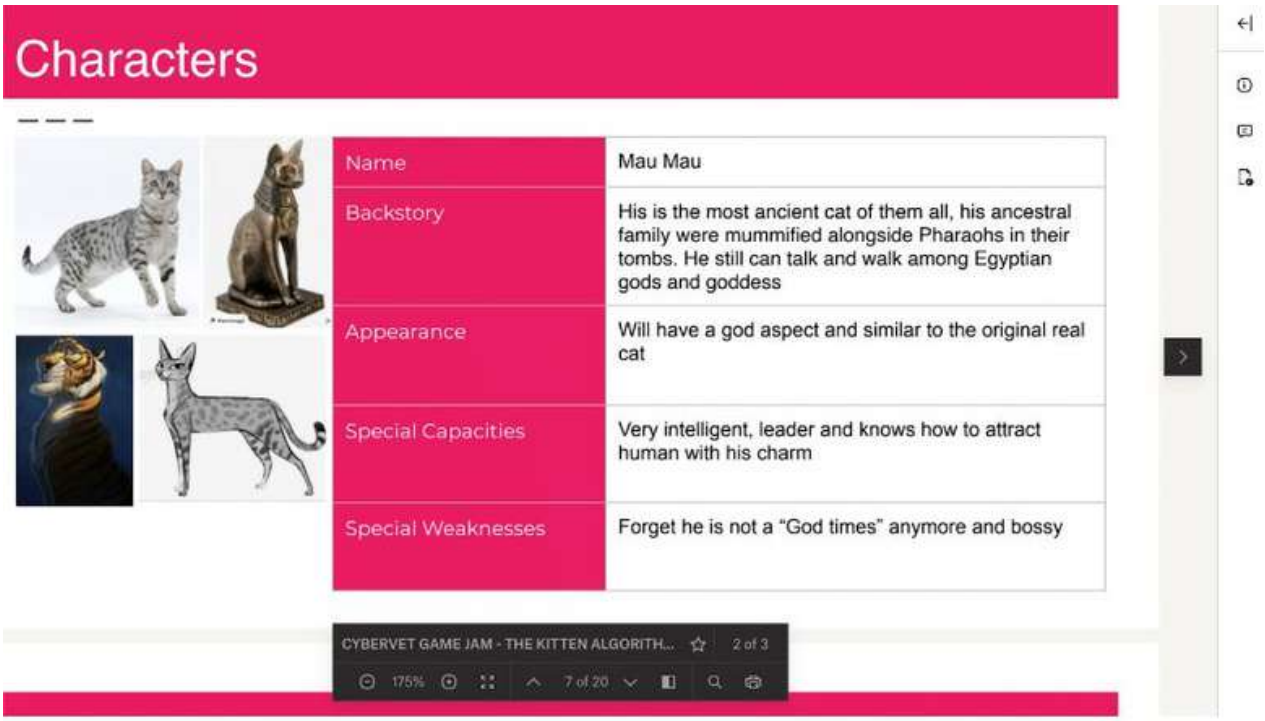
Il s'agit d'un jeu de société stratégique de 2 à 6 joueurs, qui se joue en 30 à 60 minutes. Dans ce jeu, vous devez tromper les humains pour les convaincre que vous êtes le meilleur chat et obtenir plus de prestige en obtenant le plus grand nombre possible de serviteurs des chats humains. Gardez l'œil ouvert, les autres chats patrons vont activement essayer de saboter votre chemin pour atteindre les humains et prendre la gloire pour eux-mêmes. Ne vous fiez pas à leurs jolis visages !

Vous perdez la partie si vous n'avez pas un nombre élevé d'humains comme serviteurs ou si le 10ème tour est terminé et qu'aucun des joueurs n'a au moins 4 humains sous son commandement.

La difficulté réside dans le fait qu'il y a 6 patrons qui essaient de tromper les humains pour qu'ils deviennent leurs serviteurs et qu'ils puissent les contrôler, mais tout le monde a le même objectif et certains pourraient même aider les humains à se libérer du contrôle du chat.

NGO NEST BERLIN [DE], EOS [IT] + IASIS [GR]

Mau Mau



LECSA (LV)

GAME JAM

Le partenaire LECSA de Lettonie a organisé un événement GameJam du 27 septembre au 1er octobre 2021. En raison des restrictions épidémiologiques et des différents lieux où se trouvaient les participants, l'événement a été organisé de manière hybride (sur place à l'école technique de Saldus et via la plateforme Zoom). Pendant l'événement, 6 équipes (4-5 personnes par équipe) ont été formées pour travailler sur le développement de prototypes de jeux. Pour obtenir des résultats tangibles, le concept de Game Jam prévoyait le développement de deux types de jeux : des jeux d'ordinateur et des jeux de société.

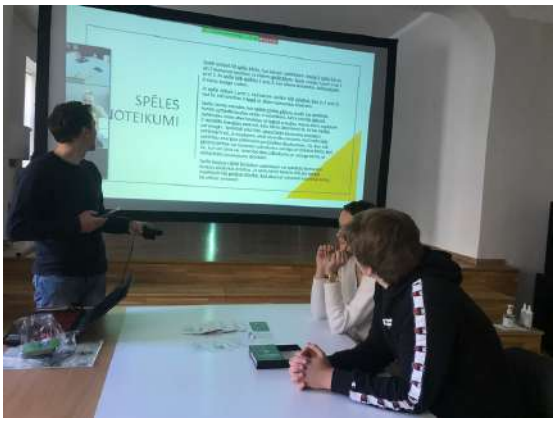
ACTIVITÉS

- Les mois d'août et septembre 2021 ont été consacrés à la planification et à l'organisation de l'événement (recherche d'experts en cybersécurité et en développement de jeux, diffusion d'informations aux participants potentiels, planification de l'agenda et définition des critères du jeu, etc.)
- Evénement multiplicateur - Actualité des cyberattaques (27.09.2021) : Introduction du projet CYBER.EU.VET et conférence sur les tendances en matière de cyberattaques avec M. Armins Palms, expert en cybersécurité du CERT.LV (institution de réponse aux incidents de sécurité informatique de la République de Lettonie).
- Nombre de participants : 26 personnes
- Lieu : École technique de Saldus (ville de Saldus) et plateforme ZOOM
- Annonce du Game Jame (27.09.2021) : définition et discussion sur les défis actuels de la cybersécurité (évaluation des besoins) ; formation des équipes, rencontre avec les mentors et discussion sur la suite du travail (atelier sur le moteur de jeu Unity), brainstorming sur l'idée et le concept du jeu.
- Activités de Game Jam en cours (28.09-30.09.2021) : les équipes ont travaillé sur le développement de prototypes, la consultation avec les mentors a été assurée, si nécessaire.
- Présentation de l'avancement (30.09.2021) : présentation des concepts de jeu et de l'avancement du travail pour recevoir les suggestions des mentors.
- Grande finale (01.10.2021) : quatre équipes ont présenté leurs résultats et les mentors ont fourni une évaluation. Une équipe, développant un jeu d'ordinateur, s'est retirée. Conclusion de l'événement et discussion informelle.
    - Nombre de participants : 30
    - Lieu : École technique de Saldus et plateforme ZOOM

LECSA (LV)

RÉSULTATS

1. prototype du jeu en ligne - Le Virus
2. Jeu de société - Cards About Security
3. Jeu de société - Cyberwar
4. Jeu de cartes compétitif - Cyber Mind



EXAMPLE Cyber Mind - Un jeu de cartes compétitif

Il s'agit d'un jeu de cartes éducatif avec des éléments de quiz. La tâche principale du jeu est d'enseigner les bases de la sécurité quotidienne sur Internet et ce à quoi les gens s'exposent en y faisant des bêtises. Il couvre des sujets tels que la sécurité sur Internet et la protection des données dans le contexte de l'utilisation des réseaux sociaux. À l'issue du jeu, les personnes (joueurs) devraient être capables de reconnaître les tentatives d'escroquerie dans la vie réelle.

Développé par l'équipe Veiksminieki (du letton : les gens qui réussissent), des étudiants de l'école technique de Saldus lors de la Game Jam en Lettonie (octobre 2021) :

Renars Ricards Hartmanis, Estere Ozoliņa, Sindija Diāna Valtere & autres.

Niveau : élémentaire (pour les débutants). Groupe cible : élèves, étudiants, enseignants et parents.

Le jeu contient : 50 cartes, 2 carnets de santé (pour compter la santé des joueurs), 2 dés et une carte de règle.

LECSA (LV)

GAME JAM

À PROPOS DE

Les tentatives de cyberattaques dans le monde augmentent chaque jour. Le gouvernement mondial a donc eu l'idée d'organiser un tournoi pour identifier les personnes qui présentent des cyberrisques et les contrer. Jeu éducatif permettant d'apprendre les principaux types de cyberattaques, les méthodes de prévention et d'élimination en se protégeant ou en protégeant son équipe et en contre-attaquant l'adversaire. Le but du jeu est d'éliminer toutes les vies de l'adversaire.

COMMENT JOUER/RÈGLES DU JEU

Nombre de joueurs : 2 ou 4 personnes (1 contre 1 ou 2 contre 2).
Chaque joueur ou équipe (à 2 contre 2) dispose de "100 vies" (Health=HP) au début du jeu.
Le décompte des points de vie se fait à l'aide de blocs-notes noirs ou d'autres notes disponibles. Désignez une personne distincte qui suivra et calculera la consommation d'énergie et de santé des joueurs, si possible. Sinon, les joueurs le font eux-mêmes.
Chaque joueur reçoit 5 cartes. Si le jeu se joue à 2 contre 2, les deux joueurs ont "une main commune" dans l'équipe ou 10 cartes ensemble.

Il existe trois types de cartes : Cartes d'attaque (rouge), Cartes de bouclier (jaune) et Cartes de vie ou de guérison (vertes).

Le jeu se joue en rounds. Le joueur/équipe qui obtient le plus grand nombre avec les dés commence la partie.

Chaque carte coûte de l'énergie. Au début de chaque tour, le joueur lance 2 dés pour définir une énergie qui est indiquée en haut de la carte (en bleu). Les cartes doivent être jouées de manière à ne pas dépasser le montant d'énergie obtenu.
Le joueur/équipe qui commence le tour peut attaquer (avec des cartes d'attaque), se protéger (cartes de bouclier) ou ajouter de la vie (cartes de guérison), tandis que les seconds peuvent uniquement utiliser les cartes d'attaque et de bouclier pour minimiser leur vulnérabilité en termes de vie.
Gardez à l'esprit que le nombre maximum de vies par joueur/équipe pendant le jeu peut être de 100 HP (par exemple, si la somme des vies et de l'énergie après le tour fait 110 HP au total, votre nombre de vies reste quand même de 100 HP).
Le jeu se termine dès qu'un joueur/équipe n'a plus de vies (0 vie).
Si le jeu n'a plus de cartes, vous devez à nouveau mélanger les cartes de la pile.

LECSA (LV)

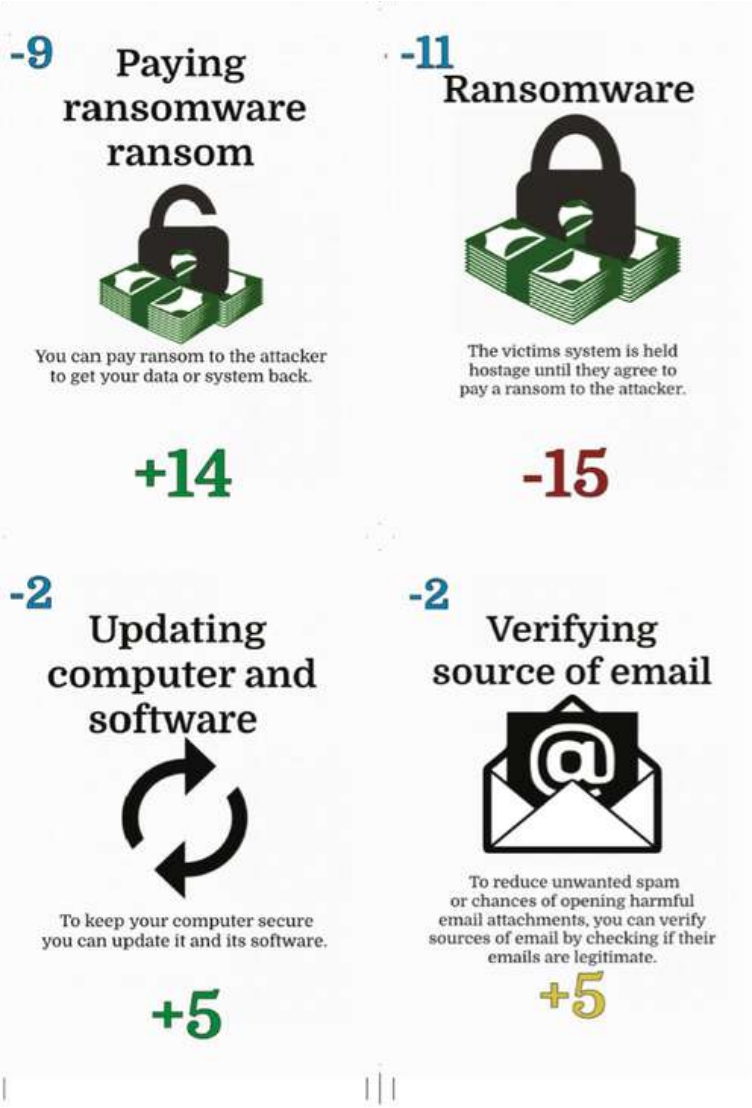
Exemples de cartes

En **bleu** – Energie

En **rouge** Cartes d'attaque

En **jaune** - Cartes de bouclier

En vert - Cartes de guérison



Exemple de calcul de la santé

EXEMPLE Cyberwar - Jeu de société

Développé par l'équipe Exodus (étudiants de l'école technique de Saldus), leader de l'équipe Valdemārs Šperbergs.

2-6 joueurs < - > Convient aux personnes âgées de 15 ans et plus.

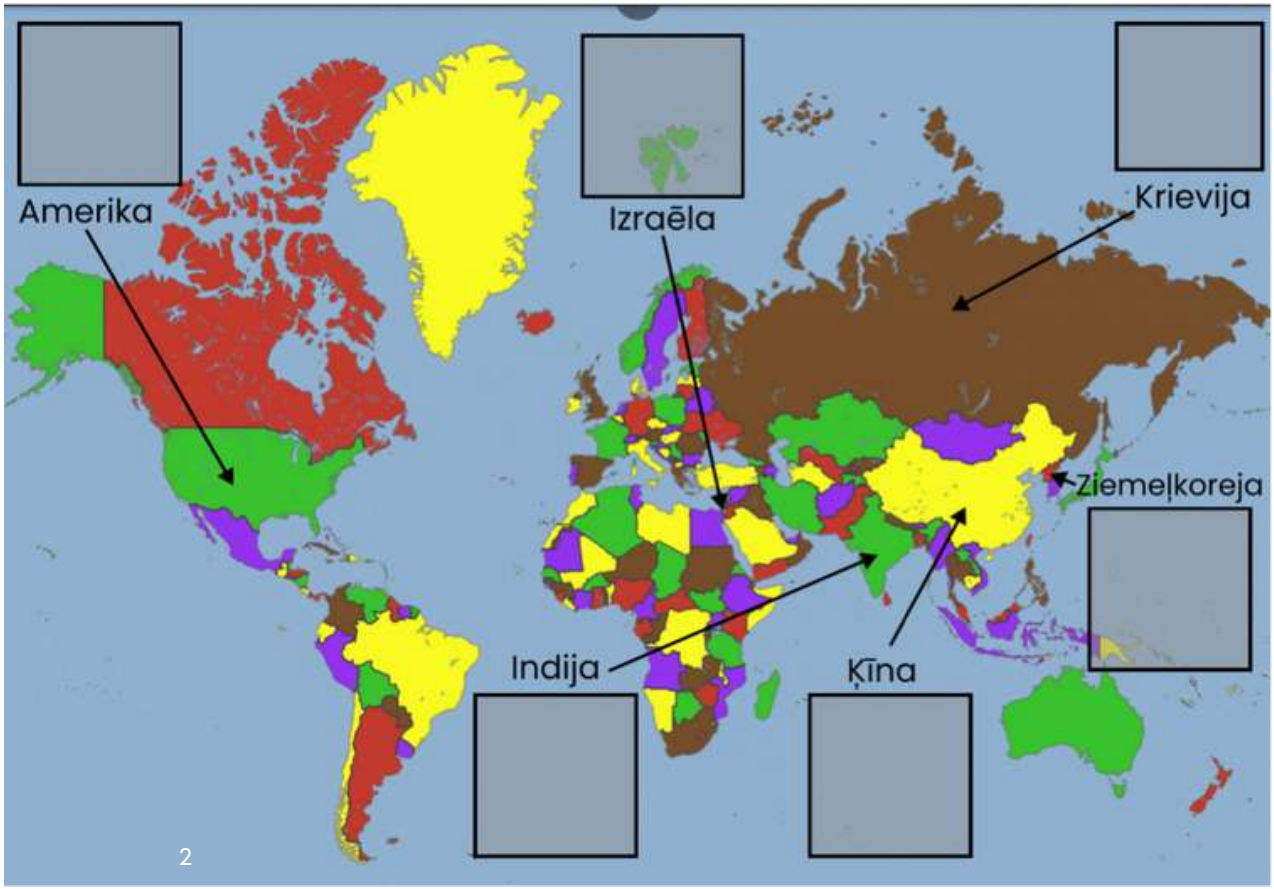
Un jeu de société qui met l'accent sur la tactique et l'aléatoire (le hasard).

Niveau : jeu éducatif pour ceux ayant une certaine compréhension sur la cybersécurité.

Le jeu contient : Une carte du monde, 2 dés, des serveurs, des cartes avec fonction "attaque", "défense" ou "réaction", une légende des vulnérabilités, un tableau avec les mouvements possibles pour chaque type de vulnérabilité.

À PROPOS DE

Le but du jeu est de protéger le pays représenté par le joueur et d'attaquer les autres pays pour gagner la cyber-guerre. Dans Cyberwar, chaque joueur doit choisir un pays à représenter. Chaque joueur dispose d'un serveur avec 3 vulnérabilités. Le but du joueur est de pirater les serveurs des autres pays en exploitant deux des trois vulnérabilités ou de corriger deux des trois vulnérabilités sur son propre serveur.



LECSA (LV)

COMMENT JOUER

Les joueurs choisissent le pays à représenter et placent un objet serveur à l'endroit désigné sur la carte. Chaque pays a ses propres bonus.

Chaque joueur tire au hasard (prend) 3 vulnérabilités - une de chaque niveau de difficulté, et les place face cachée à leur emplacement respectif sur leur champ serveur. Les vulnérabilités ne sont pas connues des joueurs.

Les vulnérabilités ont 3 niveaux de difficulté. Le niveau de difficulté détermine également le nombre de chiffres nécessaires pour exploiter une vulnérabilité (voir "Attaques"), ainsi que le nombre de coups nécessaires pour corriger la vulnérabilité (voir "Défense").

Le jeu se déroule en tours, les actions (mouvements) suivantes peuvent être effectuées - **Scanning, Attaque et Défense**. Les joueurs déterminent la séquence des joueurs en lançant deux dés.

Début

Chaque joueur reçoit 4 cartes au début de chaque tour. A la fin du tour, il est possible - de garder 2 cartes ou de les échanger contre des cartes existantes.

Le 1er tour est un tour de balayage où aucune carte d'attaque ou de défense n'est autorisée. Lors des tours suivants, les joueurs peuvent choisir de scanner ou d'attaquer ou d'essayer de réparer leurs vulnérabilités (voir Défense). Le jeu se poursuit tour après tour jusqu'à ce qu'une condition de victoire soit atteinte.

Numérisation

- L'attaquant choisit un pays pour scanner sa vulnérabilité (par exemple, "Je scanne un Russe de 2ème niveau de vulnérabilité").
- Le joueur effectue le scan - lance deux dés, applique les bonus de son pays représenté, compare avec le niveau de difficulté de la vulnérabilité + les bonus du pays de la victime.

Si l'attaquant obtient un nombre égal ou supérieur au niveau de difficulté de la vulnérabilité de la victime, il peut regarder la vulnérabilité scannée.

- Les bonus des pays ne sont pas ajoutés lorsque l'on se scanne soi-même.

Niveaux de difficulté

1er - le joueur doit obtenir au moins le numéro 4 (hors bonus du pays).

2ème - le joueur doit obtenir au moins le numéro 8 (sans les bonus du pays)

3ème - le joueur doit obtenir au moins le numéro 11 (sans les bonus du pays).

ATTAQUE

Le joueur nomme la cible de l'attaque (par exemple, "J'attaque une vulnérabilité russe de niveau 2") et révèle la carte d'attaque à tous les joueurs, en la plaçant à côté de la vulnérabilité.

Le joueur lance le dé pour voir si l'attaque fonctionne en comparant le résultat du dé à la difficulté de la vulnérabilité + les bonus (si le résultat du dé + les bonus correspondent ou dépassent la difficulté, l'attaque réussit).

Les attaques peuvent être repoussées en utilisant la carte de réaction prévue pour cette attaque. Chaque attaque a son propre type de réaction qui peut être jouée et son propre type de vulnérabilité pour laquelle elle fonctionne.

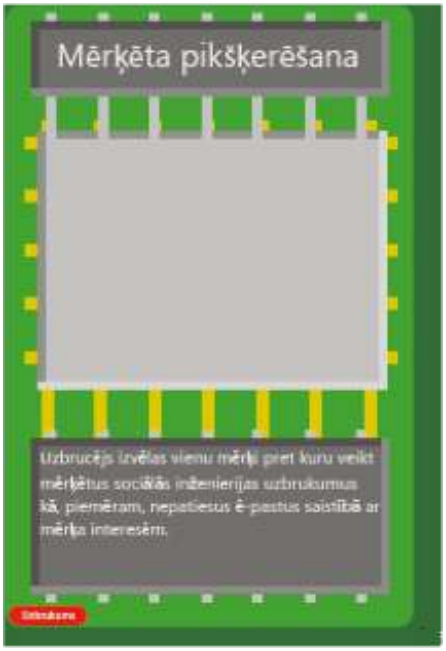
- Si l'attaque échoue ou est bloquée par une carte Réaction - les cartes Attaque et Réaction jouées restent sur la table jusqu'à la fin du prochain tour et empêchent les autres joueurs d'attaquer avec la même attaque pour la même vulnérabilité. Après le déplacement, les deux cartes retournent sur la pile.

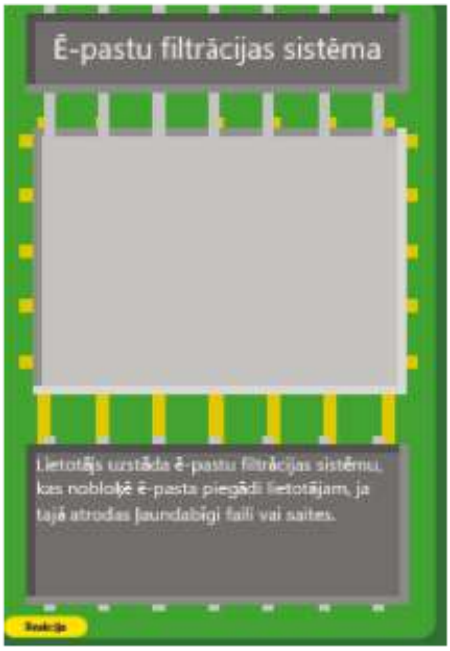
Niveaux de difficulté

1er - le joueur doit obtenir au moins le numéro 4 (hors bonus du pays).

2ème - le joueur doit obtenir au moins le numéro 8 (sans les bonus du pays)

3ème - le joueur doit obtenir au moins 11 (sans les bonus du pays).





LECSA (LV)

Défense

- Défense - choisir la bonne méthode contre une vulnérabilité particulière. Les cartes Réaction arrêtent (annulent) l'attaque entrante (et toutes les autres attaques visant la même vulnérabilité) pendant 1 tour.
- Pour annuler une attaque entrante, le joueur place une carte Réaction correspondant au type d'attaque (voir tableau des vulnérabilités) sur la carte d'attaque dès que l'attaque est jouée.
- Pour commencer à réparer une blessure, le joueur place une carte Défense à côté de la blessure à réparer.
- Les autres joueurs peuvent attaquer cette blessure pendant qu'elle est en défense (avant que le tour de défense ne soit terminé).
- Lorsque le joueur tente de réparer une blessure sur son serveur avec une carte Défense, celle-ci ne peut pas attaquer, mais peut essayer d'empêcher les attaques avec des cartes Réaction. Pour une réparation complète, il faut |niveau de difficulté + 1| tour. Les actions de balayage sont autorisées pendant la période de réparation.

Si la méthode de défense n'est pas correcte, le joueur saute 3 tours et ne peut pas utiliser de cartes de défense pendant cette période (les réactions et les actions de balayage sont autorisées).

Primes des pays

- USA : +2 en numérisation
- Russie : +2 pour les attaques
- Chine : +2 pour la défense contre les attaques
- Corée du Nord : +2 pour la défense contre les balayages
- Inde : +1 à toutes les attaques, -1 contre les attaques
- Israël : +3 dans toutes les attaques, -3 contre les attaques

Vulnérabilités par niveaux

Vulnerability	Attacks	Défense	Reaction
1st vulnerability level			
SSH server with username	Password guessing	Usage of the public key	Settings of Blocked Period
Administration Panel with User Name	Password guessing	Blocking external requests	Settings of Blocked Period
Untrained employee	Phishing campaigns	IT security trainings	Filtration system of e-mails; Implementation of e-mail SPAM list
Vulnerable SMB protocol	Exploitation of EternalBlue	Fixing vulnerability CVE-2017-0144	n/a
XSS vulnerability	Code injection; Code injection using Polyglot	Introductory synthesis	Introduction of the symbol blacklist

SQL injection	Code injection; Code injection using Polyglot	Introductory synthesis	Introduction of the symbol blacklist
Router panel with default username and password	Using default data	Complete replacement of authentication data	One session limit
2nd vulnerability level			
SSH server	Password guessing	Usage of the public key	Settings of Blocked Period
Administration Panel	Username guessing	Blocking external requests	Settings of Blocked Period
XSS vulnerability with filter	Code injection using Polyglot	Introductory synthesis	Introduction of the symbol blacklist
SQL injection with filter	Code injection using Polyglot	Introductory synthesis	Introduction of the symbol blacklist
Incompletely configured firewall	Packet fragmentation	Repair configuration	IDS implementation
WiFi network with WEP security	Packet Phishing	Using the WPA2 standard	RADIUS implementation
Busy CEO/boss	Phishing – catching the big fish	IT security trainings	Filtration system of e-mails; implementation of e-mail SPAM list
3rd vulnerability level			
Service failure	DDoS	IP address blocking and load limiting	Load balancers
Vulnerable OpenSSL program	Heartbleed exploitation	Repair of CVE-2014-0160	n/a
Vulnerable Print Spooler program	PrintNightmare exploitation	Repair of CVE-2021-36958	n/a
Buffer overflow vulnerability	Buffer overflow	Introduction of buffer limits	Increasing the buffer
Weak hashing algorithm	Decryption of the hash value	Improving the hash algorithm	Usage of a strong and long password
Lazy IT expert	Targeted phishing	IT security trainings	Filtration system of e-mails; implementation of e-mail SPAM list

LECSA (LV)

SSH serveris

SSH serveris ar lietotājvārdu

Administrācijas panelis

Administrācijas panelis ar lietotājvārdu

Neapmācīts darbinieks

Ievainojams SMB protokols

XSS ievainojums

SQL injekcija

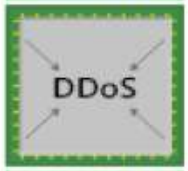
Rūtera panelis ar noklusējuma lietotājvārdu un paroli

XSS ievainojums ar filtru

SQL injekcija ar filtru

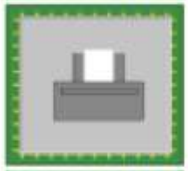
Nepilnīgi nokonfigurēts ugunsmūris

WiFi tīkls ar WEP drošību



Pakalpojuma atteices kļūda

Ievainojama OpenSSL programma

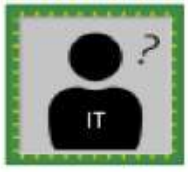


Ievainojama Print Spooler programma

Bufera pārpildes ievainojums

Vājš jaucējvērtības algoritms

Aizņemts priekšnieks



Slinks IT speciālists

LECSA (LV)

GAME JAM

LECSA (LV)

CONSEILS ET EXPÉRIENCES DU GAMEJAM EN LETTONIE

- Au cours de l'événement de deux jours, il n'est pas possible de développer un véritable jeu vidéo, mais plutôt un premier prototype, qui pourra ou non être développé en fonction de la motivation des participants.
- Des prix ou d'autres types d'avantages peuvent contribuer à impliquer davantage de participants et à garantir de meilleurs résultats (plus tangibles) à la fin (dans notre cas, des pizzas et des boissons ont été offertes à la fin de l'événement, ainsi qu'un soutien supplémentaire de la part des mentors (par exemple pour placer des jeux sur la plate-forme)).
- Les mentors sur les questions de développement de jeux et de cybersécurité jouent un rôle important dans la Game Jam en consultant et en aidant les participants.
- Planification à l'avance - il s'agit d'un événement assez complexe qui nécessite une planification minutieuse.
- Les organisateurs doivent tenir compte du fait que certaines équipes peuvent être exclues de la compétition (en raison du temps limité).

Veuillez consulter les posts FB avec les résultats de l'événement.:https://www.facebook.com/cybereuvetproject.eu/posts/138127645211214 https://www.facebook.com/saldustehnikums/posts/1780232175520378

L'événement a été organisé par LECSA en coopération avec la Commission européenne. Latvijas Universitāte | Ekonomikas un kultūras augstskola / EKA University of Applied Sciences | McĀbols | cert.lv | Coldwild Games | Saldus tehnikums!

MEATH PARTNERSHIP (IE)

ACTIVITÉS

- Réunion d'information sur l'évaluation des besoins avec les étudiants (formation au codage dans un établissement local d'enseignement pour adultes)
- GameJam de 2 jours (session d'information en ligne le 1er jour ; 2ème jour consacré au Game Jam)
- Événement multiplicateur - Matinée de sensibilisation à la cybersécurité

DESCRIPTION & RÉSULTATS

1) Réunion d'information sur l'évaluation des besoins avec les étudiants
(formation au codage dans un établissement local d'enseignement pour adultes)

Date : Octobre 2021

DESCRIPTION

Afin de diffuser le projet et d'identifier les principaux thèmes de la Game Jam, l'équipe de Meath Partnership a organisé une session d'information avec les étudiants d'une classe locale de formation au codage. Le partage d'informations sur la cybersécurité et la discussion sur les menaces les plus récentes ont été suivis d'une session de brainstorming où les étudiants ont été divisés en deux groupes afin de discuter des questions permettant d'identifier les sujets les plus intéressants à explorer pendant le Gamejam. Des informations supplémentaires sur le Gamejam et le projet CYBER.EU.VET ont également été partagées avec les participants ce jour-là.

EXEMPLE D'ÉVALUATION

YBER.VET.EU

Co-funded by the Erasmus+ Programme of the European Union

Needs assessment meeting guidelines

1. What do you know about cybersecurity?
2. Why do I need to be worried about it?
3. What are the biggest cybersecurity concerns/threats right now?
4. Do you know how to recognise those threats?
5. What is a cyber attack?
6. Can you give us an example of a cyber attack?
7. Can you give us, at least, 3 possible solutions to it?

MEATH PARTNERSHIP (IE)

RÉSULTATS

Grâce à cette activité, l'équipe de Meath Partnership a pu mieux comprendre les connaissances générales des élèves en matière de cybersécurité et de cybermenaces. Elle a également recueilli des informations qui ont été intégrées dans le processus de planification et de mise en œuvre du GameJam.

L'ÉVALUATION EN ACTION

2) Gamejam de 2 jours

(session d'information en ligne le 1er jour ; 2ème jour dédié au Game Jam)

DESCRIPTION

La première journée a été consacrée à l'accueil des participants, à la présentation du projet CYBER.EU.VET et à l'ouverture de la Game Jam, ainsi qu'au partage d'informations sur les deux sujets identifiés lors de la réunion d'évaluation des besoins. Les participants ont eu la possibilité de travailler individuellement ou en équipe. Ils ont également eu la possibilité de poser des questions ou d'obtenir des précisions sur les procédures liées au développement des jeux le deuxième jour.

Le deuxième jour était consacré au développement des jeux. Des membres de notre équipe et un expert en support informatique étaient disponibles via Zoom pour aider les participants pendant toute la durée de la Game Jam, de 9h à 21h.
Les participants ont été invités à télécharger leurs jeux sur la plateforme Itchio sous un profil créé dans le cadre de cet événement : CYBER.EU.VET : Cybersecurity Game Jam - itch.io

RÉSULTATS

Après que les participants ont partagé leurs ébauches de jeux avec l'équipe, un participant a décidé d'aller de l'avant et de télécharger le jeu pour une évaluation plus approfondie. Les autres participants ont décidé de ne pas soumettre leurs ébauches car elles n'en étaient qu'à leurs débuts.

Click or not click

Online interactive cybersecurity game

A short narrative driven game on raising awareness for cyber security threats. The game prompts players to make the right decision and avoid losing your security level.

Link: https://itch.io/jam/cybereuvet-cybersecurity-gamejam

Jeu interactif en ligne sur la cybersécurité :
https://itch.io/jam/cybereuvet-cybersecurity-gamejam

MEATH PARTNERSHIP (IE)

3) Événement multiplicateur - Matinée de sensibilisation à la cybersécurité

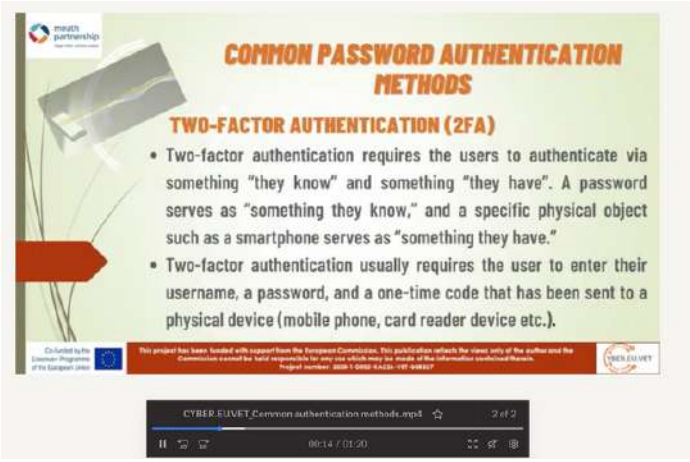
Date: Novèmbre 2021

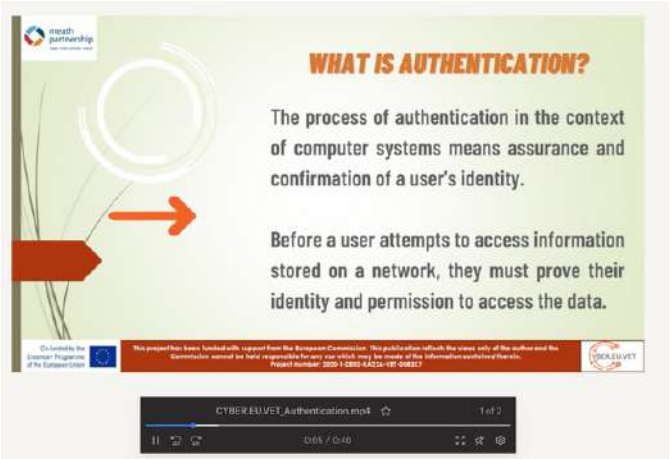
DESCRIPTION

L'événement multiplicateur a été organisé en ligne via Zoom afin de faire connaître le projet et ses activités. L'événement a été largement diffusé auprès d'une grande variété de parties prenantes intéressées ou impliquées dans la cybersécurité. L'événement a commencé par une présentation et une vue d'ensemble du projet et de la Game Jam, suivie d'une présentation et d'une discussion sur la cybersécurité et le partage d'informations pratiques sur la façon de rester en ligne (les cybermenaces actuelles et la façon d'éliminer les attaques possibles étaient possibles).

RÉSULTATS

L'événement multiplicateur a contribué à faire connaître le projet et a également permis de présenter à un public plus large les étapes franchies depuis le début du projet. Ce fut également une excellente occasion de partager des informations et des conseils pratiques en matière de cybersécurité avec les participants à l'événement.





COFAC / UNIVERSIDADE LUSÓFONA (PT)

GAME JAM

ACTIVITÉS

1) Cyber & Ethical Hacking post-graduation pour les futurs professionnels et les enseignants du marché Oct 2021 - Fév 2022 (en partenariat avec un cabinet de conseil local nommé Cybersec)

2) 2 Sessions GameJam organisées en janvier 2022 dans les écoles d'EFP :

Escola de Comércio de Lisboa - https://escolacomerciolisboa.pt

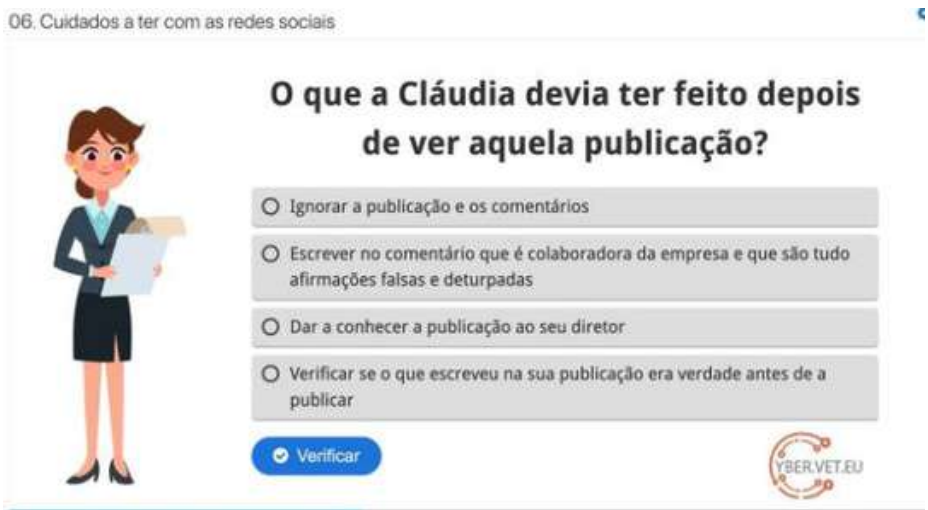
Escola Profissional Almirante Reis - https://www.epar.pt

3**)** cyberformation de trois demi-journées pour les élèves de l'enseignement secondaire en mars 2022 à l'Université Lusofona dans le cadre de l'événement Tecweb. - https://tecweb.ulusofona.pt

RÉSULTATS

Preuve du rapport de diffusion où l'on peut voir les différents tests qui ont été réalisés pendant une année civile (avril 2021 à avril 2022). Dans ce rapport, nous pouvons voir des captures d'écran de publications sur les réseaux sociaux, des affiches de différents événements, des questionnaires sur la sensibilisation à la cybersécurité (disponibles en portugais à l'adresse suivante https://docs.google.com/forms/d/e/1FAIpQLSeXACV_oeplRpTfbaC1NFKED76kRSYD6cT8cFMKjc7ohGMHZw/viewform).

DAu cours des Cyberjams, il a également été créé, sur la base des enquêtes de sensibilisation à la cybersécurité, une série de mini-jeux interactifs et conviviaux portant sur des situations simples.



TANDEM PLUS NETWORK – MEMBER IASIS [GR]

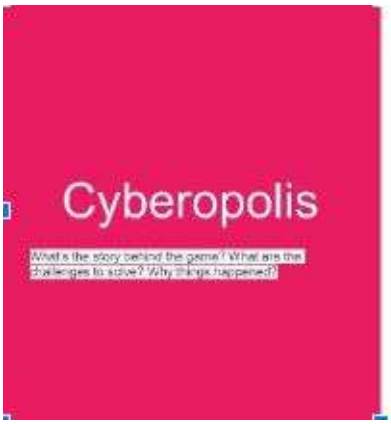
GAME JAM

Outil de conception de jeux (IASIS) - Cyberopolis

Ce jeu est un jeu de société destiné aux personnes intéressées par la cybersécurité, avec un maximum de 2-4 joueurs, et ses principaux aspects sont la confidentialité et l'intégrité des données; tandis que les sujets qu'il traite sont les logiciels malveillants, le phishing, les attaques basées sur le Web, les attaques d'applications Web, le spam, le vol d'identité, les DDoS et l'homme au milieu...

Voir l'image de ''Cyberopolis'' pour mieux comprendre les étapes à suivre pendant le jeu et les défis à résoudre.

Captures d'écran du jeu lors de la session GameJam où l'on peut constater le succès du jeu et le grand intérêt manifesté par les participants.



RÉSEAU TANDEM PLUS – MEMBRE IASIS [GR]

VIDEO - Prévention de la cyberintimidation

Cette vidéo développée par le partenaire grec rapproche les visiteurs des différentes manières de prévenir et de combattre la cyberintimidation.

YBER.EU.VET

Funded by
the European Union

DISCLAIMER

The European Commission support for the production of this publication does not constitute an endorsement of the contents which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Design
NGO Nest Berlin e.V.
Berlin, 2022

Co-funded by the
Erasmus+ Programme
of the European Union