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

IMPROVING CYBERSECURITY READINESS OF THE EUROPEAN VOCATIONAL EDUCATION AND TRAINING SECTOR

CYBER.VET.EU

INTELLECTUAL OUTPUT IO 3

HERRAMIENTAS PARA LA FORMACIÓN DE FORMADORES

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

INTRODUCCIÓN

Los socios del proyecto CYBER.EU.VET elaboraron este conjunto de herramientas para la formación de formadores -que consta de 6 módulos + materiales- para que lo utilicen los profesores y formadores del sector de la EFP. Cada módulo incluye una parte teórica, ejemplos prácticos y tareas para trabajar en grupo. El formato de formación está abierto a ser utilizado en diferentes países europeos y se adaptará a las necesidades y condiciones locales siempre que sea apropiado. Las adaptaciones podrían referirse principalmente a los ejemplos prácticos y los estudios de casos que ofrece el formato de formación.

LOS SOCIOS HAN DESARROLLADO LOS SIGUIENTES MÓDULOS DE FORMACIÓN:

CIBERATAQUES

MÓDULO 1

1. Resumen del módulo

Grupo objetivo

- Educadores y formadores de EFP
- Estudiantes
- Representantes de organizaciones o iniciativas relevantes (ONG, autoridades nacionales y regionales, instituciones educativas)

Descripción del módulo

Teniendo en cuenta el número y la magnitud crecientes de los ciberataques cada año, concretamente a la luz de los últimos acontecimientos económicos, políticos y sociales (consecuencias de las restricciones de Covid-19, conflicto militar en Ucrania, etc.), es importante debatir con más frecuencia los ciberataques reales.

Por lo tanto, el objetivo de la conferencia es proporcionar una comprensión fundamental de los ciberataques y aprender a reaccionar ante posibles incidentes.

El contenido de este módulo abarca los siguientes aspectos (unidades):

- Definición y cuestiones relevantes
- Tipología
- Los incidentes más reales (ejemplos prácticos)
- Cómo protegerse de los ciberataques y cómo reaccionar ante los incidentes

Al final de cada unidad está prevista una actividad práctica.

Objetivos de aprendizaje

Proporcionar una comprensión fundamental de las cuestiones relacionadas con los ciberataques.

- Comprender las consecuencias e impactos de los posibles ciberataques y amenazas.
- Reconocer y clasificar las formas más comunes de ciberataques.
- Saber cómo reaccionar ante los ataques: dónde informar, si se produce un incidente.
- Asegurarse de las fuentes de información y de la bibliografía para un aprendizaje más profundo y detallado, para seguir los ciberataques reales y las formas de protección.

Duración

Max 1,5 horas

CIBERATAQUES

Módulo 1

Este módulo será impartido por el formador en forma de presentación de PowerPoint en la que se compartirán los conocimientos teóricos acompañados de más elementos visuales, ejemplos prácticos y ejercicios (máx. 20 minutos + una actividad práctica por cada unidad). Se recomienda preparar las presentaciones en las plantillas de PPT adaptadas al proyecto CYBER.EU.VET. Teniendo en cuenta la rápida evolución y el progreso en el campo de la ciberseguridad, se recomienda revisar continuamente las unidades y, si es necesario, ajustar el contenido teniendo en cuenta los avances más recientes en este campo.
Además, se recomienda que los formadores adapten este módulo a las necesidades de su EFP local e incluyan ejemplos de incidentes de actualidad en la región. Este módulo abarca principalmente ejemplos prácticos de Letonia, así como algunos ejemplos internacionales. Se recomienda prestar mayor atención a la Unidad 3 para analizar y discutir ejemplos prácticos de incidentes, junto con imágenes y vídeos.

Unidad 1 - Ciberataques

¿Qué significa? Introducción al tema

Actividad de aprendizaje nº 1 - Teoría

Definición y significado

Ciberataque (pl. ciberataques) = intento de acceder ilegalmente y sin autorización a un ordenador o sistema informático con el fin de causarle daños o perjuicios. Su objetivo es inutilizar, interrumpir, destruir o controlar los sistemas informáticos o alterar, bloquear, borrar, manipular o robar los datos contenidos en estos sistemas.
Con la aparición de las restricciones de Covid-19 y la necesidad de pasar a un formato de trabajo y aprendizaje digital, el número de ciberamenazas y ataques ha aumentado y la protección digital se ha vuelto más importante.
El término "ciberataque" está estrechamente interrelacionado con términos como "ciberamenaza" (posibilidad de que se produzca un determinado ataque) y "ciberriesgo".
Los ciberataques más comunes: ataque de malware, ataque de phishing, ataque de hombre en el medio, ataque de contraseña, ataque de denegación de servicio y muchos más.
Tipos de comunicación de los atacantes: contactos personales, teléfono, correo electrónico, malware.

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

CIBERATAQUES

Módulo 1

¿Quién puede realizar ciberataques?

Un ciberataque puede ser lanzado desde cualquier lugar del mundo por cualquier individuo o grupo que utilice una o varias estrategias de ataque, y puede estar dirigido a individuos, empresas públicas o privadas (negocios).

¿Por qué se producen los ciberataques y qué pueden causar?

Los ataques en el entorno virtual suelen estar relacionados con la suplantación de identidad, la adquisición de recursos informáticos, el robo y la falsificación de información, el acceso a secretos comerciales, el chantaje o la difamación. Los ciberataques están pensados principalmente para obtener beneficios económicos (por ejemplo, el robo de números y códigos de tarjetas de crédito), trastornos y venganza (por ejemplo, para dañar la reputación de una organización)

Por ejemplo, crisis como la de Covid-19 o el conflicto militar en Ucrania se utilizan para atraer la atención de los usuarios en correos electrónicos fraudulentos y anuncios en las redes sociales.

ESTADÍSTICAS

El trabajo a distancia forzado por la pandemia ha aumentado obviamente los riesgos de ciberseguridad y ha facilitado nuevos tipos de incidentes. La mayoría de ellos son relevantes también para las instituciones educativas y deben ser tenidos en cuenta en las actividades de educación y formación de educadores y jóvenes.

Según la información analizada por Deloitte, en abril de 2020 se produjeron 350 ciberataques en Suiza, frente a una norma de 100 a 150 ciberataques (phishing, sitios web fraudulentos, ataques directos a empresas, etc.).

El aumento del trabajo a distancia exige una mayor atención a la ciberseguridad, debido a la mayor exposición al riesgo cibernético. Esto se desprende, por ejemplo, del hecho de que el 47% de las personas caen en una estafa de phishing mientras trabajan en casa.

En Letonia, por ejemplo, el mayor número de direcciones IP únicas amenazadas en Letonia se detectó de febrero a abril de 2020, cuando comenzó la pandemia de Covid-19 (más de 10.000 al mes), según el CERT.LV (la Institución de Respuesta a Incidentes de Seguridad de la Información de Letonia), que publica mensual y anualmente datos y una visión general de los incidentes más relevantes llamados "Kiberlaikapstākļi" (Cibertiempo).

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

Interactive t ool – **the live cyber threat map (world)**

Actividad de aprendizaje nº 1 - Actividad práctica

Debate con los participantes sobre su experiencia en materia de ciberataques (10-15 minutos):
1) ¿Qué tipo de ciberataques conoces?
2) ¿Has sufrido tú o tus parientes/amigos un ciberataque/ incidente cibernético? ¿Cómo terminó?

Unidad 2 - Tipos de ciberataques

Actividad de aprendizaje nº 2 - Teoría

Los métodos (tipos) más comunes de ciberataques:

Malware es un software malicioso (gusanos, virus) que se utiliza para dañar los dispositivos del usuario (ordenadores, teléfonos, etc.) o la red. Ejemplos de malware: Spyware y Troyanos, Gusanos, Virus, Adware, Spam. Dependiendo del tipo de código malicioso, el malware puede ser utilizado por los hackers para robar o copiar secretamente datos sensibles, borrar datos, bloquear el acceso a archivos, interrumpir las operaciones del sistema o hacer que los sistemas sean inoperables [DigiCERT].El malware se propaga principalmente con dos propósitos: obtener información (malware de espionaje que reenvía datos del dispositivo de la víctima) o para obtener un beneficio (ransomware de encriptación que cifra los datos del dispositivo del usuario y posteriormente se pide un rescate al usuario) [Informe del CERT 2020].

Phishing or estafas de datos personales – método en el que un hacker envía un correo electrónico aparentemente legítimo en el que pide a los usuarios que revelen información confidencial. Los destinatarios son engañados para que descarguen el malware contenido en el correo electrónico, ya sea abriendo un archivo adjunto o un enlace incrustado. Normalmente se trata de sitios web que parecen empresas reales y los usuarios tienen que introducir sus datos personales (cuenta bancaria, números de tarjeta de crédito y contraseñas, incluidas las de los servicios de autenticación). La estafa de datos puede realizarse también mediante una llamada telefónica o a través de mensajes de WhatsApp [Investopedia].

Denegación de servicio (DoS) – los hackers bombardean los servidores de una organización con grandes volúmenes de solicitudes de datos simultáneas hasta que el objetivo no puede responder o se bloquea, lo que hace que los servidores no puedan gestionar ninguna solicitud legítima. Como resultado, el acceso al servicio no es posible para los usuarios del sistema. Los ataques DoS pueden durar desde un

as horas hasta muchos meses y pueden costar a las empresas tiempo y dinero mientras sus recursos y servicios no están disponibles [Investopedia].

Man-in-the-Middle – los atacantes se interponen secretamente entre dos partes, por ejemplo, un usuario de ordenador individual y una institución financiera. Dependiendo de los detalles del ataque real, este tipo de ataque puede ser clasificado más específicamente como un ataque man-in-the-browser, ataque monster-in-the-middle o ataque machine-in-the-middle. En este caso, el atacante intercepta, borra o modifica los datos mientras se transmiten a través de una red por un ordenador, un smartphone o cualquier otro dispositivo conectado [Investopedia, TechTarget].

Actividad de aprendizaje nº 2 - Actividad práctica

Discusión en grupo - ¿Qué tipo de características indican sobre los mensajes de ataque/fraude? (10 -15 min)

- Los participantes disponen de 10 min para anotar las características
- Debate sobre los resultados.

Unidad 3 - Ejemplo de amenazas y ataques

¿Cómo identificar las amenazas?

Actividad de aprendizaje nº 3 - Teoría

Ejemplos de ciberataques (a la luz de la guerra en Ucrania)

- Correos electrónicos fraudulentos en inglés en los que se pide el apoyo a una de las partes del conflicto militar: Ucrania o Rusia. El apoyo se puede mostrar comprando votos y votando de esta manera - es un fraude cuyo objetivo es robar los datos de las tarjetas de pago de los usuarios (ver pantalla de impresión)
- VÍDEO - Cómo los estafadores están secuestrando las donaciones benéficas para la guerra de Ucrania - BBC News
- ARTÍCULO - 4 tipos de estafas por la guerra entre Rusia y Ucrania dirigidas a los consumidores

Ejemplos basados en los principales incidentes en Letonia (2020-2021) y otros ejemplos internacionales (seguidos de ejemplos visuales)

Malware

La situación de Covid-19 se utilizó para difundir intentos de malware: por ejemplo, correos electrónicos en nombre de la Organización Mundial de la Salud (OMS), en los que se indicaba que el archivo adjunto incluía la información más reciente sobre Covid-19; enlaces a gráficos que mostraban la propagación de Covid-19, cuya funcionalidad era robar datos de los usuarios; correos electrónicos maliciosos dirigidos a instituciones sanitarias en relación con la entrega de equipos de protección de Covid-19, etc.

CIBERATAQUES

Módulo 1

La propagación del malware más peligroso del mundo, Emotet, tanto en las redes mundiales como en las letonas, tiene como objetivo robar información sensible y suele originarse en un correo electrónico de un contacto ya infectado. Emotet sirve para abrir la puerta a otros ordenadores, permitiendo el acceso no autorizado a otras familias de malware. Más de 200 empresas letonas fueron infectadas.

Phishing o suplantación de identidad

La mayoría de los casos tenían como objetivo la estafa de datos de correo electrónico y de Office 365, la adquisición de datos bancarios, del sistema de pago internacional (incluyendo Smart-ID - herramienta de autenticación electrónica en Letonia), de datos de acceso, y la estafa de datos de acceso a cuentas en medios sociales populares (Facebook e Instagram). El tema de Covid-19 se utilizó a menudo para atraer la atención de los usuarios en correos electrónicos fraudulentos y anuncios en las redes sociales.

Durante la pandemia, se observaron intentos intensos de fraude de datos utilizando las marcas de proveedores de servicios de paquetería (Latvijas Pasts, DHL, Omniva, DPD, AliExpress, etc.)

También se observaron ataques innovadores, por ejemplo, un ataque a los derechos de acceso a Office 365 que fue difícil de detectar por medios técnicos, ya que no se llevaron a cabo acciones maliciosas en el dispositivo de la víctima, sino que los ataques se realizaron dentro de Office 365.

VIDEO Phishing (con subtítulos en inglés)

Fraude

Intentos intensos de fraude, incluyendo ataques de ingeniería social. La mayoría de los fraudes tenían como objetivo obtener los datos de acceso a las tarjetas de pago de los ciudadanos, los recursos financieros, así como los datos de acceso al correo electrónico. Los atacantes enviaron correos electrónicos y mensajes de texto fraudulentos a la población, así como realizaron llamadas telefónicas fraudulentas, la mayoría de las veces haciéndose pasar por representantes de bancos o proveedores de servicios de correo electrónico. Varias empresas sufrieron interferencias comerciales (BEC), sufriendo una pérdida total de casi 200.000 euros.

El tema de la entrega de bienes también fue objeto de intentos de fraude contra vendedores que publicaban información sobre la venta de bienes en portales de publicidad. Fingiendo ser compradores interesados y utilizando la plataforma de comunicación WhatsApp, los estafadores expresaban su deseo de comprar el producto, como si utilizaran los servicios de una empresa de mensajería, y pedían a los vendedores que introdujeran los datos de la tarjeta en los sitios web falsificados de Omniva, DPD y, posteriormente, Latvijas Pasts, para revelar tanto el código CVV como el saldo.

Los atacantes utilizaban direcciones de sitios web personalizados (dominios) similares a los originales para engañar al público.

Los atacantes también intentaron obtener la información de las tarjetas de pago enviando correos electrónicos en los que se les pedía que solicitaran un saldo de Bitcoin dándose de alta en un servicio fraudulento de intercambio de criptodivisas.
Los intentos más activos fueron las campañas de extorsión, en las que los hackers afirmaban haber hackeado el dispositivo de un usuario y obtener material comprometedor por el que se fijaba un rescate; los sorteos fraudulentos en nombre de las marcas conocidas, ofreciendo ganar los smartphones más nuevos u otros premios valiosos.

OTROS EJEMPLOS

Anuncios engañosos en las redes sociales – utilizando los nombres de personas famosas de Letonia sin su conocimiento, se invitaba a los internautas a invertir en criptodivisas. Los estafadores también hicieron llamadas telefónicas e intentaron persuadir a la gente para que invirtiera. En algunos casos, se observaron repetidos intentos fraudulentos en los que se ofrecía a las víctimas del fraude financiero ayuda para recuperar los recursos perdidos.

Estafas teleónicas – falsificando los números de teléfono de diferentes entidades de crédito y haciéndose pasar por representantes del banco, los estafadores, aprovechando el escaso conocimiento del público sobre los métodos de autenticación adicionales, defraudaron recursos financieros de varios miles de usuarios, causando pérdidas totales por valor de cientos de miles de euros a las entidades de crédito letonas.

Los piratas informáticos también se están adaptando a la difusión del trabajo a distancia: teniendo en cuenta la necesidad de las empresas de pasar rápidamente a una condición de trabajo a distancia y la implantación de la circulación de documentos electrónicos, los piratas informáticos aprovechan esta situación para adaptar sus ataques; por ejemplo, varios contables de empresas recibieron correos electrónicos en nombre del director o de otro empleado para realizar un pago urgente o cambiar la cuenta de la nómina.

Letonia y Lituania detienen a 108 personas por una estafa multimillonaria en centros de llamadas

interferencia en la correspondencia comercial de las empresas – al comprometer los correos electrónicos de las empresas o de sus socios colaboradores, los atacantes eligen un momento adecuado para enviar a una de las partes una factura con una cuenta modificada.

Mensajes de estafa – los atacantes intentan interceptar las cuentas de WhatsApp pidiendo un código de seis dígitos que se envía al número de teléfono del destinatario por error. Al recibir un mensaje de las personas de su lista de contactos, algunas personas transfieren sus códigos, perdiendo el acceso a su cuenta de WhatsApp. El uso de la autenticación de dos factores sería un medio de protección contra un ataque de este tipo.

EJEMPLO Cuando el usuario comparte el código de dígitos con el hacker (ver pantalla de impresión y artículo)
EJEMPLO SMS del banco local con enlace de fraude (ejemplo con SMS del banco SEB).

Correos electrónicos fraudulentos – los estafadores se hacen pasar por una oficina nacional de correos (Latvijas Pasts) y piden a los usuarios que paguen por la entrega de un supuesto envío retrasado. El enlace proporcionado en el correo electrónico conduce a un sitio web falso para obtener datos fraudulentos de la tarjeta de pago (véase la pantalla de impresión).

iendas oline falsas – Se ha observado una alta actividad específicamente durante la temporada de vacaciones por medio de anuncios en las redes sociales y debido a las restricciones de Covid-19 que obligaron a las empresas a vender sus productos online.
EJEMPLOS Los estafadores atraen a los usuarios de AliExpress a tiendas online falsas (imagen y caso de estafa); Cómo reconocer una estafa

Estafa romántica - los estafadores se aprovechan de las personas que buscan pareja romántica, a menudo a través de sitios web de citas, aplicaciones o redes sociales, haciéndose pasar por posibles compañeros. Se aprovechan de los estímulos emocionales para conseguir que les proporcionen dinero, regalos o datos personales.
EJEMPLO Historia de investigación sobre un estafador romántico [por North Lab]

Ataques de denegación de servicio (DoS y DDoS)
Se registraron ataques DDoS contra instituciones públicas y municipales (por ejemplo, la Biblioteca Nacional, el Centro de Sistemas de Información Cultural, etc.) Los ataques DDoS prolongados interrumpieron una escuela. Se recibieron informes similares de otras instituciones educativas al comienzo del año escolar. Las instituciones educativas de otros lugares de Europa también se enfrentan a estos problemas.
Tanto en Europa como en Letonia, los siguientes incidentes cobraron actualidad: intentos de extorsión monetaria dirigidos principalmente a instituciones financieras o empresas del sector privado (los atacantes realizaron una serie de ataques de prueba, amenazando con suspender el funcionamiento de los sitios web de las empresas u otros recursos mediante ataques de hasta 2 Tb/s).

OTRAS TENDENCIAS

Dispositivos comprometidos y fugas de datos

Los equipos comprometidos pueden afectar a particulares, empresas e instituciones estatales y municipales. Esto puede ocurrir a través de un correo electrónico ya comprometido, o la infección de un dispositivo al abrir archivos adjuntos o enlaces de contactos aparentemente familiares, como colegas y socios comerciales; también puede ocurrir a través de sitios web comprometidos, por ejemplo, a través de un plugin obsoleto o un sistema de gestión de contenidos obsoleto.

Como ocurrió en 2020-2021, cuando varias instituciones nacionales perdieron temporalmente el acceso a sus cuentas de redes sociales cuando los atacantes tomaron el control de uno de los perfiles de los administradores de las cuentas. Se registraron informes de intrusiones en reuniones de Zoom y MS Teams, como resultado del escaso conocimiento de las salvaguardias disponibles (es decir, sala de espera, acceso limitado desde el extranjero, etc.).

Intentos de intrusión (cualquier ataque que pretenda comprometer los objetivos de seguridad de una organización): tras el aumento de la actividad de trabajo remoto de los bots que buscan dispositivos vulnerables, mal configurados y/o contraseñas débiles para los dispositivos conectados a una red (dispositivos expedidos apresuradamente por el empleador, portátiles personales que empezaron a utilizarse para el trabajo, así como servicios RDP mal protegidos con contraseñas débiles) ha aumentado significativamente.

VIDEO Intrusion Examples

Más información sobre la detección de intrusiones

FUENTE CERT.LV and "Kiberlaikapstākļi" (Cyber Weather); Investopedia

- Elementos adicionales

NOTA Considere también las discusiones sobre otros métodos sobre información falsa y fraudulenta, como deepfake y otros.

Actividad de aprendizaje nº 3 - Actividad práctica

Al final de la unidad se organiza una prueba Kahoot en la que los participantes tienen que detectar si la información proporcionada es fraudulenta y tienen que identificar el tipo (método) de ciberamenaza.

Unit 4 - ¿Qué hacer en caso de incidente?

Prevención y cómo prepararse.

Actividad de aprendizaje nº 4 - Teoría

ALGUNOS CONSEJOS Y TRUCOS PARA LA PROTECCIÓN

- Revise siempre sus correos electrónicos con atención y esté atento a: archivos adjuntos o enlaces incrustados de fuentes o remitentes desconocidos/sospechosos; mensajes con sensación de urgencia que le pidan que descargue algo o realice alguna otra tarea; ofertas con una promesa de recompensa que parezca demasiado buena para ser cierta.

VIDEO Clicker (Spaidonis) con subtítulos en inglés

- Preste atención a la ortografía de la dirección URL. Los sitios de phishing suelen utilizar direcciones web que parecen similares a las de un sitio oficial, pero que contienen un simple error ortográfico, como la sustitución de un "1" por una "l". Una ortografía incorrecta o extraña es una señal de posible estafa.
- Utilice una contraseña fuerte y diferente entre sus dispositivos, cuentas de correo electrónico y cuentas de redes sociales. Para más consejos, consulte el módulo de CYBER.EU.VET sobre contraseñas (Módulo 4).
-

- Siempre que sea posible, ajusta tu configuración para utilizar la autenticación multifactor en tus dispositivos. Por ejemplo, contraseña y Face ID o huella dactilar en tu teléfono; Gmail, por su parte, tiene una configuración de este tipo, por la que cuando un usuario inicia sesión desde un nuevo dispositivo, tras introducir su nombre de usuario y contraseña, recibe una solicitud para confirmar su identificación desde otro dispositivo, normalmente un teléfono.

verificación en dos pasos en WhatsApp (para usuarios de Android).

- No realices transacciones sensibles en la Wi-Fi pública no segura de las cafeterías y otros lugares públicos similares.
- Asegúrate de que al menos los datos más importantes de tu dispositivo tienen una copia de seguridad (en la nube o en un dispositivo externo). Asegúrese de que puede restaurar los datos necesarios a partir de las copias de seguridad, y averigüe cuánto tiempo tarda.
- Actualizaciones de software: es crucial seguir las actualizaciones de software e instalarlas inmediatamente. Incluso un solo día de retraso puede ser crítico.
- Utilice una VPN. Las redes privadas virtuales añaden una capa más de protección al uso de Internet desde casa. No se puede confiar únicamente en ellas para evitar los ciberataques, pero pueden ser una barrera útil contra el ciberataque.
- Siga regularmente las noticias del mundo de los ataques e intente pensar que los acontecimientos globales, nacionales y locales, tanto políticos como económicos, pero también los relacionados con el sufrimiento global (pandemias, conflictos militares) pueden ser utilizados como tema/"tapadera" para posibles ciberataques.
- Adicional (en letón): Recomendaciones de CERT.LV ante el empeoramiento de la situación geopolítica y el aumento de las ciberamenazas en Europa: https://cert.lv/lv/2022/02/cert-lv-ieteikumi-saasinoties-geopolitiskajai-situacijai-eiropa-un-pieaugot-kiberdraudiem

Dónde informar sobre una amenaza o incidente cibernético

- Tu lugar de trabajo, institución educativa: envía capturas de pantalla, fotos o vídeos a la persona pertinente de tu institución (por ejemplo, el departamento de TI). Avisa a tus compañeros y amigos.

Instituciones de apoyo al ciberespacio nacional (caso de Letonia)

- CERT.LV (apoyo en la resolución de incidentes, vigilancia del ciberespacio, avisos), Instrucción sobre cómo reenviar correos electrónicos fraudulentos (en letón)

Policía estatal

- Centro letón para una Internet más segura (infracciones y contenidos ilegales en Internet, seguridad de los niños en Internet), y otros

FUENTES DE INFORMACIÓN Y ACTUALIDAD

Para seguir las noticias sobre ciberseguridad y ciberamenazas, lea regularmente recursos locales o internacionales:
https://portswigger.net/daily-swig/cyber-attacks https://www.euronews.com/tag/cyber-attack
OUCH! Boletines: el principal boletín gratuito de concienciación en materia de seguridad diseñado para todo el mundo.

Enlaces para Letonia (algunas informaciones también están disponibles en inglés):
https://www.esidross.lv/
https://cert.lv/lv/ (incluyendo, "Cyber Weather "(Kiberlaikapstākļi), instrucciones sobre cómo reenviar correos electrónicos fraudulentos (en letón)
https://drossinternets.lv/

Actividad de aprendizaje nº 4 - Actividad práctica

Debate con los participantes: evaluación de la utilidad del curso (actividad de 5-10 minutos)

2. Resultados de aprendizaje del módulo

Conocimiento

- Los alumnos tendrán una comprensión básica de los principales problemas de los ciberataques.
- Los alumnos tendrán una visión general de los incidentes reales (a la luz de los acontecimientos mundiales).
- Los alumnos sabrán qué fuentes de información deben seguir para conocer las alertas y la actualidad de las amenazas.

Habilidades

El alumno será capaz de identificar y clasificar los tipos más comunes de ciberamenazas y explicarlos.

Competencias

- Los alumnos serán capaces de reconocer una posible ciberamenaza y saber dónde denunciarla.
- El alumno será capaz de seleccionar herramientas y técnicas básicas para protegerse de los ciberataques.

3. Bibliografía

CERT.LV (Information Technology Security Incident Response Institution): 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.lvLIKTA (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. Resumen del módulo

Grupo objetivo

- Educadores de EFP
- Estudiantes
- Representantes de instituciones públicas activas en los sectores educativos: municipios, autoridades regionales y nacionales

Descripción del módulo

Hoy en día, la gente pasa gran parte de su tiempo delante de una pantalla. Los jóvenes crecen en un mundo en el que las nuevas tecnologías son necesarias y el principal medio de comunicación que utilizan es Internet. Estar en las redes sociales, por ejemplo, ofrece muchas ventajas, pero también muchos riesgos.. Hay mucha gente que ha sido acosada o está siendo acosada. En la mayoría de los casos, no eran conscientes de ello ni de los problemas que puede causar en sus vidas. Por esta razón, nos gustaría utilizar este módulo, para entender qué es el ciberacoso y cómo podemos prevenirlo.

Objetivos de aprendizaje

- Comprensión del ciberacoso.
- Saber cómo detectarlo
- Efectos del ciberacoso
- Comprender las principales consecuencias
- Dar a conocer las técnicas para prevenirlo y afrontarlo

Duración

2 horas

Unidad 1 - Cómo detectar el ciberacoso

¿Cuáles son los efectos?

Esta Unidad será impartida por el formador en forma de presentación de PowerPoint cuyo objetivo es compartir los conocimientos teóricos acompañados de elementos más visuales: vídeos cortos y casos reales de ciberacoso que resumen la información de las diapositivas de PowerPoint (máx. 30 minutos).
Se recomienda preparar las presentaciones en las plantillas PPT personalizadas para el proyecto CYBER.EU.VET.

Actividad de aprendizaje 1

El formador presenta a los alumnos una presentación con el siguiente contenido sugerido (máx. 30 minutos):
El ciberacoso, aunque a menudo se asocia con el ciberacoso, es un problema muy serio por sí mismo y cuya prevalencia ha aumentado en los últimos años.

¿Cómo detectar el ciberacoso?

El ciberacoso puede ser difícil de reconocer porque tiene lugar a puerta cerrada o en un teléfono/ordenador privado.
Aquí están algunos de los signos más comunes, de que alguien puede ser víctima de ciberacoso:

- Se altera de forma inusual si no puede usar el ordenador o el teléfono o después de usar el ordenador.
- Cambia rápidamente de pantalla o cierra los programas cuando alguien pasa por delante.
- Evita las discusiones sobre lo que está haciendo en el ordenador.
- Se aleja de la familia o de los amigos.
- Reticencia a participar en actividades que antes disfrutaban.
- Disminución inexplicable del rendimiento académico.
- Rechazo a ir a la escuela.

Las víctimas también pueden sufrir académicamente, ya que pueden sentirse demasiado avergonzadas para ir a la escuela o participar en clase. En algunos casos, las víctimas pueden incluso considerar el suicidio.

El ciberacoso también puede tener efectos adversos en quienes lo presencian. Pueden sentirse asustados, impotentes y tristes. También pueden tener problemas para dormir y comer e incluso desarrollar ansiedad y depresión.

Efectos y consecuencias del ciberacoso:

Cuando el acoso se produce en la red, puede parecer que te atacan por todas partes, incluso dentro de tu propia casa. Puede parecer que no hay escapatoria. Los efectos pueden durar mucho tiempo y afectar a la persona de muchas maneras:

- **Mentalmente:** sentirse molesto, avergonzado, estúpido, incluso con miedo o enfadado.
- **Emocionalmente:** sentirse avergonzado o perder el interés por las cosas que le gustan
- **Físicamente:** sentirse cansado (por la pérdida de sueño), o experimentar síntomas como dolores de estómago y de cabeza

La sensación de ser objeto de burla o acoso por parte de los demás, puede impedir que las personas hablen o intenten solucionar el problema. En casos extremos, el ciberacoso puede incluso llevar a las personas a quitarse la vida.

Efectos:

VIDEO Words Hurt | Cyberbully Short Film

- Enfermedad
- Depresión
- Aislamiento

Actividad de aprendizaje 2

Enfado

- Debate en grupo - Preguntas y respuestas; evaluación y retroalimentación (máx. 10 minutos)

Humillación

Ahora que conoces los signos más comunes de alguien que está siendo ciberacosado,

- ¿Conoces a alguien en esta situación?
- ¿Podrías ayudarles?

Unidad 2 - Cómo prevenir el ciberacoso

Actividad de aprendizaje 1

El formador presenta a los alumnos una presentación con el siguiente contenido sugerido (máx. 30 minutos):

El ciberacoso se ve facilitado por el fácil acceso a plataformas y dispositivos de medios digitales. A menudo, éstos se utilizan sin ninguna supervisión. Esto hace que el ciberacoso sea un problema increíblemente difícil de abordar. Prevenir esta práctica requeriría una gran cantidad de tiempo y recursos para supervisar eficazmente cada interacción en línea. Aunque a menudo no es posible deshacerse por completo de las herramientas digitales, hay métodos que padres, alumnos y educadores pueden emplear para combatir el fenómeno y reducir sus efectos nocivos.

Para los padres, una forma eficaz de abordar el daño resultante del ciberacoso es simplemente hablar del tema con sus hijos.
También es importante hablar de la seguridad en línea, la privacidad y la gestión de las contraseñas. Establezca directrices sobre cómo deben comportarse los estudiantes en línea e instruya a los jóvenes para que se sinceren con sus padres sobre cualquier daño que hayan sufrido a causa del acoso en línea o en el mundo real.
Los jóvenes pueden ayudar a evitar ser víctimas del ciberacoso siendo cautelosos con lo que publican. Deben evitar compartir sus contraseñas y asegurarse de que la configuración de su privacidad en línea los mantiene a salvo.
Los estudiantes desempeñan un papel importante en la prevención del ciberacoso. Si los jóvenes que conocen los hechos de ciberacoso observan que le ocurre a otra persona, pueden notificarlo a un adulto de confianza. También deben ser amables, generosos y solidarios con el niño que está siendo acosado. Los profesores, educadores y otros adultos de confianza deben unirse a los padres y a los jóvenes para combatir el ciberacoso. A menudo, estas personas pueden detectar cambios en el comportamiento de un niño y pueden ayudar a resolver el problema antes de que lo hagan los padres.
La tecnología e Internet no son el problema. El verdadero problema son las personas que la utilizan para dañar a otros. Por eso es importante enseñar a los adolescentes a utilizar las redes sociales de forma segura y responsable y a ser conscientes de cómo actuar en caso de sufrir ciberacoso.

¿Qué hacer si te están acosando cibernéticamente?

- NO CONTESTE ni comente el mensaje del ciberacoso.
- BLOQUEa a las personas implicadas.
- Salir del sitio donde se está produciendo el acoso.
- Asegura tus CONTRASEÑAS y comprueba tus CONTROLES DE PRIVACIDAD.
- GUARDA todo. Haz una captura de pantalla o imprime el incidente como prueba.

¿Qué hacer si ves que se produce ciberacoso?

- Denuncia el ciberacoso: casi todos los sitios tecnológicos tienen una opción para denunciar a alguien por ciberacoso.
- Comunícalo a tus padres o a un adulto de confianza y pídeles consejo.
- Comunica a un ADULTO de confianza lo que está ocurriendo o ponte en contacto con las fuerzas del orden.
- Denuncia la situación al proveedor de la tecnología, la aplicación o las redes sociales.
- Si la situación implica a compañeros de clase, informa a tus profesores.
- **Tomar medidas legales:** Tanto la calumnia como la injuria son delitos que pueden dar lugar a un juicio.
- Muestra tu apoyo a la persona acosada, por ejemplo, dirigiéndole un mensaje amable.

Pedir ayuda: Es muy difícil enfrentarse al ciberacoso en solitario.

VIDEO Emma's Story: Cyberbullied by a Best Friend

¿Cómo puedo educarme a mí mismo?

- Organizaciones que pueden ayudar: Hay muchas organizaciones que comparten información sobre el ciberacoso. Los sitios web que aparecen a continuación están creando y compartiendo contenido útil que es realmente útil para cualquier persona ansiosa por el ciberacoso o que lo esté sufriendo.
- Blogs y podcasts: mantenerse al día con los blogs y podcasts que se centran en el tema es una gran manera de mantenerse al día y obtener los últimos consejos o perspectivas.
- Libros.
- Aplicaciones y software: Existen numerosos productos que permiten a los padres restringir y/o supervisar la actividad en línea de sus hijos. Cada padre debe decidir si este tipo de control es adecuado en función de la edad de su hijo y de sus hábitos en Internet. Algunos incluso escanean el lenguaje que podría ser acosador. También hay empresas que se asocian con los colegios para permitir la denuncia anónima de incidentes de acoso.

Actividad de aprendizaje 2

Debate en grupo - Preguntas y respuestas; evaluación y retroalimentación (máx. 15 minutos)

Ejercicio de escritura:

Describe una situación en la que sepas que hay ciberacoso.

Puede ser real o ficticia.

¿Puedes ayudar? ¿Cómo? ¿Por qué o por qué no? Explica cómo te hace sentir esto.

2. Resultados de aprendizaje del módulo

Conocimiento

- El alumno sabrá cómo detectar el ciberacoso y cómo lo siente y experimenta la víctima.
- Comprendiendo los hechos del ciberacoso y conociendo los métodos para abordarlo, los jóvenes, los adultos y los educadores pueden ayudar a crear un mundo digital mejor y más empático.

Habilidades

- El alumno entenderá cómo reconocer cuando alguien está siendo víctima de ciberacoso.

El alumno será capaz de entender qué nivel de respuesta y apoyo es necesario dependiendo del escenario en cuestión.

Competencias

- El alumno será capaz de reconocer un episodio de ciberacoso y abordarlo inmediatamente utilizando las herramientas adecuadas.
- El alumno será capaz de identificar cuál es el mejor método de apoyo y cuál es el más adecuado para el caso en cuestión.

3. Bibliografía

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. Module Overview

Grupo objetivo

- Educadores de EFP
- Representantes de instituciones públicas activas en los sectores educativos: municipios, autoridades regionales y nacionales

Descripción del módulo

Este es un módulo de seguimiento de "Ciberacoso. ¿Qué es? ¿Cómo podemos detectarlo?" y proporciona a los grupos destinatarios las competencias necesarias para difundir la concienciación sobre el ciberacoso y proporcionar técnicas de prevención para no convertirse en víctima del ciberacoso.

Objetivos de aprendizaje

- Comprender la importancia de la prevención
- Difundir la concienciación sobre el ciberacoso
- Concienciar sobre las técnicas de prevención del ciberacoso

Duración

1,5 hora

Unidad 1 - ¿Por qué prevenir el ciberacoso?

Esta Unidad será proporcionada por el educador como una presentación de PowerPoint que incluirá tanto material teórico como elementos más visuales como películas cortas y escenarios de ciberacoso de la vida real que resumirán la información de las diapositivas de PowerPoint (20 a 30 minutos respectivamente en cada Unidad).
Recomendamos preparar las presentaciones en las plantillas PPT adaptadas al proyecto CYBER.EU.VET. La presentación va seguida de un debate en grupo, para que todos reflexionen sobre lo aprendido.

Actividad de aprendizaje 1

El formador presenta a los alumnos una presentación con el siguiente contenido sugerido (máx. 20 minutos):

¿Prevenir o intervenir?

Según las investigaciones, las personas que sufren ciberacoso tienen una serie de resultados negativos, como dificultades emocionales, físicas, mentales y académicas.
Además, el ciberacoso es una fuente importante de estrés para los jóvenes. Las víctimas se sienten psicológicamente heridas, avergonzadas y a veces asustadas como resultado del ciberacoso. No sólo se culpan a sí mismos por el acoso y el abuso que reciben, sino que también se sienten tremendamente ansiosos. De hecho, más del 35% de las personas que son objeto de ciberacoso presentan síntomas de estrés, según una investigación. Este tipo de acoso puede ser especialmente dañino porque suele ser muy público. Normalmente, muchas personas pueden ver lo que se escribe o se publica. Es difícil, si no imposible, borrar todo rastro de algo una vez que se ha publicado en línea. Esto significa que el acoso puede ser continuo.
Cuando las personas son acosadas por otros en las redes sociales, a través de mensajes de texto, chats instantáneos y publicaciones en blogs de forma frecuente, pueden empezar a sentirse desesperadas. Pueden sentir que el suicidio es la única forma de detener su sufrimiento. Dado que los peligros del ciberacoso son tan graves, es fundamental que los educadores de EFP enseñen a sus alumnos[AB1] este problema antes de que cause un daño real. Prevenir reduce los riesgos de estar expuesto al ciberacoso.

Actividad de aprendizaje 2

Debate en grupo (máx. 10 minutos)

Pregunte a sus alumnos:

- ¿Por qué es tan importante la prevención en el ciberacoso?
- ¿Te has informado alguna vez sobre el ciberacoso?

Cómo te sueles informar sobre los delitos de ciberacoso?

Unidad 2 - Difusión de la concienciación

Actividad de aprendizaje 1

El formador realiza una presentación a los alumnos con el siguiente contenido sugerido (máx. 30 minutos):
Es fundamental debatir con los alumnos cómo utilizar las redes sociales de forma segura y responsable, detectando a los agresores del ciberacoso y aprendiendo qué hacer si son acosados en línea.

VIDEO Cyberbullying - How to Avoid Cyber Abuse

PENSAR ANTES DE PUBLICAR

Los estudiantes deben acostumbrarse a leer su trabajo antes de publicarlo. Pueden escribir el post en la sección de notas de su ordenador o smartphone y volver a revisarlo unas horas después para decidir si lo publican o no. Como los ciberacosadores podrían utilizar lo que publicas en tu contra de alguna manera, estarás menos inclinado a decir algo de lo que luego te arrepientas o que pueda ser utilizado en tu contra. Seguro que si alguien quiere utilizar algo contra ti, se esforzará por conseguir hasta la información más insignificante, pero comprobarlo antes de compartirlo puede reducir la gravedad del ciberataque. Pensar antes de publicar puede ayudarte a mantener una relación sana con las redes sociales.

SÉ CUIDADOSO CON LOS DISPOSITIVOS PÚBLICOS

Los estudiantes también deben tener cuidado al utilizar dispositivos públicos, como los ordenadores de la universidad o de la biblioteca, ya que hay muchas formas de que alguien pueda aprovecharse de ello. Hay muchas posibilidades de que los dispositivos públicos se infecten con programas maliciosos, como los registradores de pulsaciones de teclas (keyloggers).

Un keylogger, según la mayoría de las fuentes, es una aplicación de software que supervisa y registra discretamente todas las pulsaciones de teclas. Pueden utilizarse para interceptar las contraseñas y otra información personal introducida a través del teclado, lo que supone una gran amenaza para los usuarios, como entregar el acceso a sus cuentas de redes sociales a los ciberdelincuentes. Lo más importante a tener en cuenta cuando se trata de keyloggers es que a menudo no pueden ser detectados por los programas antivirus, ya que hay muchos keyloggers legítimos disponibles en el mercado con fines de control parental, seguridad de la empresa, etc.

VIDEO Could a Keylogger Be Spying on You?

Aparte de los programas de control especializados, también hay que recordar a los estudiantes que deben cerrar la sesión de sus cuentas, ya que pueden dejarlas abiertas sin querer y a disposición de quienes vayan a utilizar los ordenadores de al lado.

PROTECCIÓN ONLINE

Es fundamental utilizar contraseñas seguras en todas partes cuando se trata de combatir el ciberacoso y otras actividades fraudulentas. Una contraseña fuerte es aquella que no puede ser fácilmente adivinada o comprometida. Una contraseña segura debe ser larga, contener una combinación de números, caracteres especiales y letras minúsculas o mayúsculas y no debe incluir en ningún caso información obvia como el nombre, la fecha de nacimiento, etc. Al proteger tus cuentas, te aseguras de que nadie tenga acceso a ellas.

HAY QUE DENUNCIAR EL CIBERACOSO.

Asegúrate de que tus alumnos entienden la importancia de denunciar el ciberacoso. Esto implica no sólo detectar a los ciberacosadores, sino también informar a la plataforma de medios sociales, al proveedor de servicios de Internet y a cualquier otra parte relevante. Para poner fin al acoso, puede que incluso tengan que informar a las autoridades locales. Después de haber presentado toda la documentación necesaria, los estudiantes deben tomar las medidas necesarias para bloquear al individuo o la cuenta responsable del ciberacoso. También deben ser conscientes de que, incluso después de bloquear al agresor, éste podría crear cuentas alternativas para acercarse a la víctima. La buena noticia en relación con el acoso que se produce en línea es que normalmente se puede grabar, conservar y presentar a alguien que pueda ayudar. Las víctimas deben guardar esa prueba por si las cosas se les van de las manos.

Video: Ignore or report a Cyber Bully

Actividad de aprendizaje 2

Presente a los alumnos el siguiente caso práctico

YouProMe Erasmus+ project – www.youpromeproject.eu

Jessica tiene 18 años. Vive con sus dos padres, ambos profesionales y siempre ocupados trabajando. Jessica es la mayor de tres hijos. No hay nadie en la familia con problemas de salud conocidos. Estudia en la escuela y es una estudiante muy trabajadora. Le apasionan los animales y le gusta salir con sus amigos. Tiene novio. Jessica tiene teléfono móvil y es usuaria habitual de las redes sociales.

Jessica informó: "Hace unas semanas le envié a mi novio unas fotos. Pensaba que era mi novio de todos modos, pero luego se las enseñó a su amigo y su amigo se las envió a todo el mundo. El colegio se enteró y ahora la policía ha hablado con él y con su amigo. No he vuelto a la escuela desde entonces, pero ahora todo el mundo me llama puta en las redes sociales. No soporto que me miren, y ya sé lo que piensan. Incluso las chicas tienen una opinión similar sobre mí. Lo estúpido es que todo el mundo lo hace, todo el mundo envía fotos, pero yo sólo tuve la mala suerte de tener un novio que me traicionó. No volveré a confiar en nadie. Siento que todo se ha acabado y que ya no hay vuelta atrás".

Como consecuencia, Jessica ha estado ausente de la escuela durante un mes y se niega a volver. Abandonó todas sus actividades deportivas escolares. Su madre ha hablado con el monitor deportivo y ha dicho que está preocupada por algunas de las cosas "oscuras" que Jessica ha estado diciendo. Jessica está deseando cambiar su presencia en Internet y recuperar la confianza inicial. Jessica y su familia no saben qué apoyo hay disponible y cómo apoyar mejor su salud mental, ni saben cómo puede mediar un monitor juvenil en esta situación. Jessica se ha dado cuenta del riesgo de hacer un mal uso de Internet y reconoce que necesita apoyo para gestionar su salud mental, ya que esto ha influido en su toma de decisiones.

Ahora puede iniciar una conversación basada en estas preguntas (máximo 30 minutos):

- ¿Qué riesgos hay aquí?
- ¿Qué servicios deberían involucrar?
- ¿Qué curso de acción sugieres a Jessica y a su madre?

2. Resultados del aprendizaje del módulo

Conocimiento

- El alumno comprenderá la importancia de prevenir el ciberacoso
- El alumno conocerá qué tipo de técnicas existen para evitar ser víctima del ciberacoso

Habilidades

- El alumno será capaz de difundir la prevención del ciberacoso
- El alumno será capaz de enseñar técnicas importantes de prevención a sus alumnos

Competencias

- El alumno será capaz de poner en marcha actos de sensibilización eficaces contra el ciberacoso
- En función de la situación, el alumno será capaz de determinar qué tipo de ayuda es necesaria.

3. Bibliografía

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/

AUTENTICACIÓN Y CONTRASEÑA

Módulo 4

1.Resumen del módulo

Grupo objetivo

- Educadores de EFP
- Estudiantes
- Representantes de instituciones públicas activas en los sectores educativos: municipios, autoridades regionales y nacionales

Descripción del módulo

Los profesionales de la EFP y sus alumnos se enfrentan a diario a diferentes amenazas de ciberseguridad. Aunque hay varios materiales educativos sobre ciberseguridad disponibles en línea, no todos están actualizados, o son percibidos por los alumnos como demasiado básicos o demasiado complejos.

El contenido educativo de este módulo dotará a los alumnos de habilidades y conocimientos para mejorar su comprensión de la Autenticación y las Contraseñas, con el fin de fortalecer su capacidad de formación, pero también para mejorar sus habilidades con el fin de evitar los ataques de ciberseguridad. Los educadores de EFP mejor equipados podrán apoyar aún más a sus alumnos para que reconozcan las amenazas diarias que les evitan.

Objetivos de aprendizaje

- Aumentar la comprensión de la autenticación en Ciberseguridad
- Aumentar la comprensión de los diferentes métodos de autenticación
- Aumentar la comprensión de las principales características de los métodos de autenticación más comunes
- Comprender los riesgos de no utilizar contraseñas complejas
- Dar a conocer las técnicas para gestionar fácilmente las contraseñas complejas

Duración

2 horas

AUTENTICACIÓN Y CONTRASEÑA

Módulo 4

Unidad 1 - Autenticación

Esta Unidad será impartida por el formador en forma de una presentación de PowerPoint en la que se compartirán los conocimientos teóricos acompañados de elementos más visuales: vídeos cortos que resuman la información de las diapositivas de PowerPoint (máximo 20 minutos).
Se recomienda preparar las presentaciones en las plantillas de PPT adaptadas al proyecto CYBER.EU.VET. Teniendo en cuenta la rápida evolución y el progreso en el campo de la ciberseguridad, se recomienda revisar continuamente las unidades y, si es necesario, ajustar el contenido teniendo en cuenta los avances más recientes en este campo.
La presentación va seguida de un debate en grupo de 10 minutos para reflexionar sobre el proceso de aprendizaje y evaluar el nivel de comprensión del tema por parte de los alumnos, al tiempo que se crea un espacio para nuevas preguntas y comentarios.

Actividad de aprendizaje 1

El formador realiza una presentación con el siguiente contenido sugerido (máx. 20 minutos):

¿Qué es la autenticación?
El proceso de autentificación en el contexto de los sistemas informáticos significa asegurar y confirmar la identidad de un usuario. Antes de que un usuario intente acceder a la información almacenada en una red, debe demostrar su identidad y su permiso para acceder a los datos. Cuando se conecta a una red, el usuario debe proporcionar una información de acceso única, incluyendo un nombre de usuario y una contraseña, una práctica diseñada para proteger una red de la infiltración de los hackers. La autenticación se ha ampliado en los últimos años para requerir más información personal del usuario, por ejemplo, la biométrica, para garantizar la seguridad de la cuenta y de la red frente a quienes tienen los conocimientos técnicos para aprovechar las vulnerabilidades.
Video: What is Authentication?

¿Por qué es importante la autenticación?
La autenticación es un paso crucial para mantener seguros los datos de los usuarios y para prevenir y bloquear cualquier acceso no autorizado a los datos en línea. Si la autenticación no es segura, el sistema puede ser fácilmente atacado y pirateado y los ciberdelincuentes pueden acceder a los datos y a la información almacenada en el sistema de ocurrir.

Es muy importante evitar que esto ocurra y asegurarse de que los usuarios conozcan los diferentes métodos de autenticación gratuitos o de pago para evitar cualquier acceso no autorizado a sus datos personales o profesionales. Para las organizaciones y empresas, recomendamos invertir en herramientas de autenticación de alta calidad con el fin de proteger sus datos en línea de cualquier posible infracción.

Video: Weekly Cybersecurity Tip - Authentication

Métodos habituales de autenticación de contraseñas

Teniendo en cuenta la naturaleza constantemente cambiante de los diferentes tipos de ciberamenazas y ataques, se ha desarrollado una amplia gama de métodos de autenticación diferentes en los últimos años.

Algunos de los métodos de autenticación más comunes son:

1. Autenticación con contraseña estándar
2. Autenticación de dos factores
3. Autenticación por token
4. Autenticación biométrica
5. Autenticación por reconocimiento informático
6. CAPTCHAS

1. AUTENTICACIÓN POR CONTRASEÑA ESTÁNDAR

- Forma de autenticación más básica y más frecuentemente utilizada:
- Requiere introducir el nombre de usuario, acompañado de un código secreto o contraseña que permite el acceso a una red, cuenta o aplicación.

Para reducir el riesgo de que una contraseña se vea comprometida, los usuarios deben elegir una contraseña segura. Un gestor de contraseñas seguro o un software pueden ayudar a evitar cualquier acceso no autorizado a los datos almacenados en línea.

2. AUTENTICACIÓN DE DOS FACTORES (2FA)

- La autenticación de dos factores requiere que los usuarios se autentiquen a través de algo que "saben" y algo que "tienen". Una contraseña sirve como "algo que saben", y un objeto físico específico, como un smartphone, sirve como "algo que tienen".
- La autenticación de dos factores suele requerir que el usuario introduzca su nombre de usuario, una contraseña y un código de un solo uso que se ha enviado a un dispositivo físico

3. AUTENTICACIÓN CON TOKEN

- Los sistemas de tokens utilizan un dispositivo físico construido a propósito para ofrecer la autenticación de dos factores, y se recomienda si se prefiere no depender de los teléfonos móviles.

- Puede ser un dongle que se inserta en el puerto USB de tu dispositivo, o quizás una tarjeta inteligente con identificación por radiofrecuencia o un chip de comunicación de campo cercano.

- Para mantener la seguridad de un sistema de tokens, es crucial garantizar que el dispositivo físico de autenticación (es decir, el dongle o la tarjeta inteligente) no caiga en manos equivocadas.

4. AUTENTICACIÓN BIOMÉTRICA

- La autenticación biométrica se basa en las características físicas del usuario para identificarlo. La autenticación biométrica puede hacer uso de huellas dactilares, escáneres de retina o iris, o reconocimiento facial y de voz. Se trata de una forma de autenticación muy segura, ya que no hay dos individuos con las mismas características físicas. La autenticación biométrica es una forma eficaz de saber con precisión quién se está registrando en el sistema.

5. AUTENTICACIÓN POR RECONOCIMIENTO INFORMÁTICO

- El reconocimiento informático es un método de autenticación de contraseñas que verifica la legitimidad de un usuario comprobando que se encuentra en un determinado dispositivo. Estos sistemas instalan un pequeño plug-in de software en el dispositivo del usuario la primera vez que se conecta con éxito. Este complemento contiene un marcador criptográfico del dispositivo. La próxima vez que el usuario se conecte, se comprueba el marcador para asegurarse de que está en el mismo dispositivo de confianza.

- Este sistema es invisible para el usuario y no requiere ninguna acción de autenticación adicional por su parte. Simplemente introducen su nombre de usuario y contraseña como siempre, y la verificación se produce automáticamente.

- Para mantener un alto nivel de seguridad, los sistemas de autenticación por reconocimiento informático deben permitir el inicio de sesión desde nuevos dispositivos utilizando otras formas de verificación (por ejemplo, la autenticación de dos factores con un código entregado por SMS).

6. CAPTCHAS

- CAPTCHAs no se centran en la verificación de un usuario concreto, a diferencia de lo que hacen los otros métodos enumerados en este artículo. En su lugar, los CAPTCHAs tienen como objetivo determinar si un usuario es humano, evitar los intentos de irrupción en las cuentas por parte de los ordenadores (por ejemplo, los ataques de fuerza bruta).

El sistema CAPTCHA muestra una imagen distorsionada de letras y números, o imágenes, y pide al

Actividad de aprendizaje 2

Debate en grupo - Preguntas y respuestas, evaluación y retroalimentación (máx. 10 minutos)
Preguntas recomendadas para la evaluación:

- ¿Qué es la autenticación?
- ¿Por qué es importante la autenticación?
- ¿Cuáles son los métodos de autenticación más comunes que se utilizan actualmente y cuáles son sus principales características?

Unidad 2 - Contraseña

Actividad de aprendizaje 1

1. THINGS YOU SHOULDN'T DO

Diapositivas con imágenes que ejemplifican las cosas que la gente no debe hacer, para entrar en la audiencia

ESTUDIOS DE CASO

- "La Policía belga lo ha publicado con la contraseña del WiFi puesta. Esto se mostró en la televisión nacional" - https://www.reddit.com/r/cybersecurity/comments/cnkhft/the_belgian_police_have_a_post_it_with_the_wifi/
- "Una contraseña de la agencia de emergencias de Hawái se escondía en una foto pública, escrita en una nota adhesiva" - https://www.businessinsider.com/hawaii-emergency-agency-password-discovered-in-photo-sparks-security-criticism-2018-1
- "Cuatro vergonzosas filtraciones de contraseñas en la televisión en directo" - https://www.itgovernance.co.uk/blog/four-embarrassing-password-leaks-on-live-tv

2. ESTADÍSTICAS

Presentación de algunas estadísticas:

- El 81% de las filtraciones de datos se producen por una mala seguridad de las contraseñas
- Malos hábitos de contraseñas de los empleados
- Las 200 contraseñas más comunes

AUTENTICACIÓN Y CONTRASEÑA

3. LA IMPORTANCIA DE UNA CONTRASEÑA SEGURA

La anatomía de una contraseña inhackeable

4. REGLAS BÁSICAS

Describir una serie de reglas básicas como:

- Evitar el uso de los gestores de contraseñas del navegador; es una forma fácil de que un "malware" acceda a ellas.
- No comparta su contraseña.
- Memorice las contraseñas, no las registre en papel ni digitalmenteCambie las contraseñas regularmente (cada dos meses como mínimo)
- Si es posible, activa la autenticación de dos factores
- Cada contraseña debe utilizarse en una sola plataforma
- Cambiar la contraseña original al adquirir un dispositivo
- No utilizar palabras comunes. Uno de los tipos de ataque más frecuentes es a través del "diccionario"

Reglas para una contraseña más segura:

- Crear contraseñas complejas: al menos 12 caracteres, con mayúsculas y minúsculas, con números y caracteres especiales
- No utilizar términos fácilmente descubribles, que suelen incluir: nombre, ciudad de nacimiento, o términos conocidos, nombre de la mascota, matrícula del coche; número de movil, cumpleaños de familiares, etc.
- Utiliza un refrán, expresiones comunes o algo fácil de memorizar
- Por ejemplo, utiliza las dos primeras letras de cada palabra
- Alternar entre mayúsculas, minúsculas y símbolos
- ¡Pruebe la longitud de su contraseña! - https://www.passwordmonster.com
- ¿Ya me han descifrado? - https://haveibeenpwned.com/Passwords

Memorizar en lugar de grabar:

- Crear una "clave" personal que forme parte de todas las contraseñas: Añadir algo que se asocie con el sitio/la herramienta

Actividad de aprendizaje 2

Ejercicio en grupo

Debate y comentarios (máx. 10 minutos)

Preguntas recomendadas para la evaluación:

- ¿Cuántos años resiste su contraseña una máquina normal de algoritmos de cracking?
- ¿Debo cambiar mi contraseña?

Actividad de aprendizaje 3

l formador presenta a los alumnos una presentación con el siguiente contenido sugerido (máx. 20 minutos):

¿Qué son los gestores de contraseñas?

- Cajas fuertes digitales
- Permiten almacenar credenciales y notas de diversos servicios
- También se pueden salvaguardar los datos bancarios

Gestores de contraseñas locales

- Una única llave maestra
- Se puede utilizar la autenticación biométrica
- Guardar los datos en el dispositivo actual
- El archivo de contraseñas está encriptado
- Cada contraseña debe guardarse en un archivo cifrado independiente

Gestores de contraseñas en línea

- Sólo se puede utilizar en un único dispositivo
- Ejemplo como KeypassXC
- Los datos se almacenan en la nube
- Permiten acceder a credenciales y notas de varios servicios en cualquier dispositivo
- No requiere instalación
- Una sola llave maestra
- Los datos se cifran desde el dispositivo hasta el servidor

Algunos ejemplos de gestores de contraseñas en línea son Bitwarden, Latspass, Keeper, 1Password

Actividad de aprendizaje 4

Grupo de trabajo

Crear una contraseña compleja

- Instalar un gestor de contraseñas en el portátil o en el smartphone

Activar MFA

Debate y retroalimentación (máx. 10 minutos)

Preguntas recomendadas para la evaluación:

¿Qué tan difícil fue?

¿Va a utilizar estas mejores prácticas?

2. Resultados del aprendizaje del módulo

Conocimiento

- Entender la definición de autenticación, su importancia y algunos de los métodos de autenticación más comunes
- Comprender los riesgos de no utilizar contraseñas complejas
- Utilizar las mejores prácticas en la gestión de las contraseñas personales

Habilidades

- Identificar y aplicar el método de autenticación más adecuado y apropiado
- Identificar y aplicar la complejidad de la contraseña más adecuada y apropiada

Competencias

- Percibir la importancia de la autentificación
- Decidir el método de autorización más adecuado para las distintas actividades en línea y aplicarlo para mejorar la seguridad en línea
- Percibir la importancia de utilizar contraseñas complejas
- Estructurar las técnicas de mejores prácticas para gestionar las contraseñas personalesy

3. Bibliografía

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

1. Module Overview

Grupo objetivo

- Educadores de EFP
- Alumnos de EFP
- Partes públicas y privadas interesadas en mejorar el conocimiento y la concienciación sobre las amenazas a la ciberseguridad

Esquema del módulo

El presente módulo se centrará en arrojar luz sobre las amenazas reales que se conectan a los sistemas wifi públicos, cómo funcionan y, finalmente, cómo prevenirlas.

Objetivos de aprendizaje

- Concienciar sobre las ideas erróneas en relación con el uso de las redes wifi públicas
- Proporcionar conocimientos sobre las amenazas que conlleva el uso de las redes wifi públicas

Duración

1 hora

Unidad 1

El módulo comprende tanto partes de aprendizaje en vídeo como debates abiertos. En concreto, inicialmente se proyectará un primer vídeo introductorio. Este vídeo demuestra, con la ayuda de un experto, cómo las redes públicas son un lugar arriesgado para conectarse a Internet. Sin embargo, este primer vídeo es muy corto y no permite captar gran parte del proceso por debajo. Esta primera parte concluye con un debate entre los alumnos.

Unidad 2

En segundo lugar, se tendrá en cuenta un vídeo más específico. A pesar de su manera informal de abordar el tema, sin duda transmite una mejor comprensión del asunto. Una vez realizado el vídeo, se pide al facilitador que plantee un debate entre los participantes sobre los riesgos de las redes públicas y, si es posible, que compartan sus experiencias personales.

Actividad de aprendizaje 1

Uno de los aspectos sobre los que este módulo quiere llamar la atención es la facilidad con la que se plantean estas amenazas de wifi público. Una actividad de aprendizaje continuo es intentar aplicar las sugerencias aprendidas a través de los contenidos de vídeo de este módulo, desde el restaurante/bar donde los participantes harán la pausa para comer hasta la estación de tren y el aeropuerto donde los participantes dejarán de volver a casa después de la movilidad

2. Bibliografía

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

EL USO DE LAS REDES SOCIALES

Módulo 6

1. Module Overview

Grupo objetivo

- Educadores de EFP
- Estudiantes
- Representantes de instituciones públicas activas en los sectores educativos: municipios, autoridades regionales y nacionales;

Resumen del módulo

Las redes sociales en línea (RSL) han asumido un espacio sin precedentes en las esferas profesional, educativa y privada de la vida cotidiana de las personas, incluidas las de los educadores de EFP y sus alumnos. Mientras que los beneficios de dicha integración han sido más fáciles de reconocer y adoptar como un componente integral de la educación formal e informal, los múltiples riesgos asociados a ella no han recibido la debida atención y a menudo son ignorados por el propio educador.
El enfoque simplista que a menudo se utiliza con respecto a la multifacética cuestión de la seguridad en las redes sociales, así como la complejidad de algunos de los materiales de formación disponibles, no son suficientes para crear la capacidad necesaria para prevenir y responder a las amenazas que plantea el uso de estas plataformas.

Este módulo tratará de proporcionar a los alumnos una serie de conocimientos básicos y de reforzar su capacidad de formación, pero también de mejorar su propio enfoque personal de la seguridad en las redes sociales.

Objetivos del aprendizaje

- Comprender los ciberriesgos y las amenazas asociadas al uso de las redes sociales
- Fortalecer el impacto de los procesos de desinformación en la seguridad de las plataformas UGC
- Identificar los diferentes tipos de amenazas a la ciberseguridad
- Fortalecer la capacidad de prevención y respuesta a las ciberamenazas en las redes sociales
- Ofrecer técnicas para gestionar fácilmente contraseñas complejas

Duración

2 horas

Unidad 1 - Amenazas de las redes socales

Esta Unidad se facilitará mediante el uso de una presentación en Power Point y se introducirá mediante la lectura de titulares de noticias que ofrezcan historias generalizadas de víctimas de ciberamenazas a través de las redes sociales (fotos de VIP robadas, personas que perdieron la vida a causa de noticias falsas sobre la inmunización, etc.)
Las historias y el contenido se ajustarán para que sean relevantes para el contexto y se actualicen a los últimos descubrimientos.
La presentación irá seguida de un debate en grupo de 10 minutos para reflexionar sobre el aprendizaje y evaluar la capacidad de los alumnos para comprender el tema, pero también para crear un espacio para nuevas preguntas y comentarios.

Actividad de aprendizaje 1

El formador presenta a los alumnos el siguiente contenido sugerido (máx. 20 minutos):

¿Qué es una red social en línea?

Una red social en línea (OSN) es una estructura social formada por individuos u organizaciones denominados nodos, conectados por uno o más tipos específicos de interdependencia, como la amistad, el interés común y el intercambio de finanzas, relaciones de creencias, conocimientos o prestigio. Los sitios de redes sociales como Facebook, Tweeter, Instagram, etc. no sólo se utilizan para comunicarse o interactuar con otras personas a nivel mundial, sino que también son una forma eficaz de promoción empresarial. A diferencia de las plataformas web y de medios de comunicación tradicionales, las redes sociales se dedican exclusivamente a albergar y distribuir contenidos generados por los usuarios (UGC) según criterios (algoritmos) basados en las acciones y las preferencias expresadas por los propios usuarios y registradas en los datos. En este sentido, todos los usuarios son participantes activos en los procesos de sostenibilidad de las redes sociales.

¿Qué es una amenaza en las redes sociales?

Una amenaza en las redes sociales puede ser cualquier cosa que comprometa la seguridad de una cuenta. Una ciberamenaza puede ser tanto intencional como no intencional, dirigida o no dirigida, y puede provenir de una variedad de fuentes, incluyendo naciones extranjeras dedicadas al espionaje y la guerra de la información, criminales, hackers, escritores de virus, empleados descontentos y contratistas que trabajan dentro de una organización.

ómo es una amenaza en las redes sociales

Dado que las redes sociales tienen un enorme número de usuarios y almacenan enormes cantidades de datos, son objetivos naturales para los spammers, el phishing y los ataques maliciosos. Además, los ataques sociales en línea incluyen el robo de identidad, la difamación, el acoso, la lesión de la dignidad personal y el ciberacoso. Los hackers crean perfiles falsos e imitan a personalidades o marcas, o calumnian a un individuo conocido dentro de una red de amigos.

La preocupación por la privacidad exige que los perfiles de los usuarios nunca publiquen y distribuyan información en la red. La información de las páginas personales puede contener datos muy sensibles, como fechas de nacimiento, direcciones de casa, números de móvil personales, etc. Esta información puede ser utilizada por piratas informáticos que utilizan técnicas de ingeniería social para obtener los beneficios de dicha información sensible y robar dinero.

Cómo cambian las amenazas de las redes sociales en las distintas plataformas

La forma en que un atacante lleva a cabo una amenaza en las redes sociales depende de sus objetivos. Facebook permite a los usuarios mantener sus imágenes y comentarios privados, por lo que un atacante suele hacerse amigo de los amigos de un usuario objetivo o enviar directamente una solicitud de amistad a un usuario objetivo para acceder a sus publicaciones. LinkedIn es otro objetivo común de las redes sociales, conocido por sus redes de negocios. Si un atacante tiene como objetivo una empresa, LinkedIn es un sitio de redes sociales excelente para recopilar correos electrónicos empresariales para un ataque de phishing. Dado que muchas plataformas de redes sociales muestran públicamente las publicaciones de los usuarios, los atacantes pueden recopilar datos de forma silenciosa sin que el usuario lo sepa. Algunos atacantes tomarán medidas adicionales para acceder a la información del usuario poniéndose en contacto con los usuarios objetivo o con sus amigos.

¿Por qué es importante hablar de las amenazas de OSN?

A fecha de 30 de diciembre de 2020, hay casi 4.000 millones de usuarios en el panorama de Internet. Del total de la población en Internet, hay 2.700 millones de clientes dinámicos mensuales en Facebook, 330 millones de usuarios activos en Twitter y 320 millones de usuarios activos en Pinterest.

El uso de las redes sociales está creciendo exponencialmente. Si nos fijamos sólo en Facebook, cada segundo se crean siete nuevos perfiles, se publican 510.000 comentarios en cada 60, se actualizan 298.000 estados y se suben 136.000 fotos en el mismo tiempo. Dado que se sube una gran cantidad de datos, existe un alto riesgo de que se produzca una brecha de seguridad. Cualquiera puede publicar contenido malicioso oculto dentro de datos multimedia o con localizadores uniformes de recursos (URL) acortados. Hay unos 83 millones de perfiles falsos que corresponden a usuarios ilegítimos o a profesionales que hacen pruebas e investigaciones. Alrededor de 100.000 sitios web son hackeados diariamente.

unque algunas redes sociales como Twitter no permiten revelar información privada a los usuarios, algunos atacantes experimentados pueden inferir la información confidencial analizando las publicaciones de los usuarios y la información que comparten en línea. La información personal que compartimos en línea podría dar a los ciberdelincuentes lo suficiente para conseguir nuestro correo electrónico y nuestras contraseñas.

El valor de los datos personales

Las redes sociales suelen ofrecer sus servicios de forma gratuita. La información personal no sólo es la moneda de cambio de las redes sociales, sino también el principal objetivo de las ciberamenazas en los medios sociales.

Puede ser fácil lanzar un ataque porque muchas personas suelen dar su información personal a las plataformas de medios sociales. Los atacantes pueden recopilar fácilmente estos datos y utilizarlos para obtener beneficios.

Recoger información para robar es sólo un tipo de medios sociales para el reconocimiento. La información publicada en las redes sociales podría utilizarse para obtener contraseñas o suplantar a usuarios de empresas.

Con una lista de objetivos, un atacante podría revisar las cuentas de las redes sociales en busca de información personal. La información personal puede ayudar al atacante a ganarse la confianza del objetivo en un ataque de ingeniería social. También puede utilizarse para adivinar las respuestas a las preguntas de seguridad para una toma de posesión de la cuenta o para acercarse a un usuario con mayores privilegios. Los nombres de las mascotas, los equipos deportivos favoritos y el historial educativo son todas las pistas potenciales de la contraseña o las respuestas a las preguntas utilizadas para verificar la identidad del usuario para restablecer una contraseña.

¿Por qué informarse sobre las amenazas de las redes sociales?

Las interfaces y los procesos fáciles de usar que ofrecen estas plataformas podrían haber aludido a personas sin los conocimientos o la habilidad necesarios para acceder de forma segura a sus servicios y contenidos.

La educación es la clave para detener las amenazas de las redes sociales en línea.

El primer paso es educar a los usuarios sobre los peligros de revelar demasiada información en línea al público. Incluso las cuentas de redes sociales configuradas como privadas podrían ser utilizadas en un ataque si el atacante consiguiera acceder a los contenidos privados. Los usuarios nunca deben publicar información corporativa privada en sus cuentas de redes sociales o información que pueda ser utilizada en una toma de posesión de la cuenta.

El segundo paso es educar a los usuarios sobre cómo se producen y distribuyen los contenidos digitales, y cómo pueden impulsar las acciones de los usuarios hacia los objetivos específicos para los que se han creado los contenidos. Todos los contenidos de los medios sociales son creados y vehiculados por los usuarios en función de sus diferentes objetivos personales y/o colectivos. Por estas razones, algunos de estos contenidos pueden no ser siempre convenientes, verdaderos o éticos.

Por último, hay que educar a los usuarios en el uso y mantenimiento seguro de los dispositivos a través de los cuales acceden a los servicios de las redes sociales online, ya que normalmente son vectores de riesgos e intrusiones. Algunos puntos educativos en este sentido ya están ilustrados en otros módulos de formación y serían:

- Evitar hacer clic en los anuncios, especialmente en las ventanas emergentes que instruyen a los usuarios a descargar software para ver el contenido.
- No compartir las contraseñas.
- Evitar mensajes o publicaciones en redes sociales que insten a realizar acciones rápidas como técnica de ingeniería social.
- No aceptar solicitudes de aspecto amigable de personas desconocidas aunque el usuario tenga varios amigos en común
- Evitar el uso de sitios de medios sociales en puntos de acceso wi-fi públicos (un lugar común para que los atacantes husmeen los datos mediante ataques man-in-the-middle [mitm])
- Cambie regularmente los códigos de acceso y las contraseñas.

Actividad de aprendizaje 2

Pida a los alumnos que busquen sus propios nombres en un motor de búsqueda operado por las redes sociales o en Google, y que hagan una lista de toda la información privada que puede detectarse por los múltiples contenidos que se encuentran (lugar y fecha de nacimiento, detalles e información sobre miembros de la familia, direcciones, números de teléfono, mascotas, parejas románticas, aficiones y preferencias). Invítales a pensar en las formas en que esta información podría ser utilizada en su contra.

Unidad 2 - Tipo de amenazas OSN

Actividad de aprendizaje 1

Pide a los alumnos que enumeren cualquier amenaza a la seguridad que crean que podrían encontrar en los medios sociales y pídeles que expliquen si creen que esa amenaza podría existir antes de que existiera la red social.

DIVERSAS AMENAZAS EN LAS REDES SOCIALES Y MEDIOS DE COMUNICACIÓN EN LÍNEA

Podemos dividir las amenazas de OSN en tres categorías:

- Las amenazas convencionales incluyen las amenazas que los usuarios han estado experimentando desde los primeros días de las redes sociales.
- Las amenazas modernas son ataques que utilizan técnicas avanzadas para comprometer las cuentas de los usuarios.
- Los ataques dirigidos son ataques que se dirigen a algún usuario en particular.

AMENAZAS CONVENCIONALES

Spam

Spam es el término utilizado para los mensajes electrónicos masivos no solicitados. Aunque el correo electrónico es la forma convencional de propagar el spam, la plataforma de redes sociales tiene más éxito en la propagación del spam. Los datos de comunicación de los usuarios legítimos pueden obtenerse fácilmente de los sitios web de las empresas, los blogs y los grupos de noticias. No es difícil convencer al cliente objetivo de que lea los mensajes de spam y confíe en que está protegido. La mayor parte del spam es publicidad comercial, también puede utilizarse para recopilar información sensible de los usuarios o puede contener virus, malware o estafas.

Ataque de malware

El malware es una aplicación programada que se desarrolla explícitamente para contaminar o acceder a un sistema informático, normalmente sin el conocimiento del usuario. El malware puede utilizar la estructura de las redes sociales para propagarse a través de URLs compartidas o aplicaciones secundarias de OSN, como juegos electrónicos o plugins.

Phishing

Un ataque de phishing es un tipo de ataque de ingeniería social en el que el agresor puede adquirir información sensible y confidencial como el nombre de usuario, la contraseña y los datos de la tarjeta de crédito de un usuario a través de sitios web y correos electrónicos falsos que parecen ser reales.

In el caso de OSN, un asaltante necesita atraer al cliente a una página falsa donde pueda ejecutar un ataque de phishing. Para ello, el agresor utiliza diferentes métodos de ingeniería social. Por ejemplo, puede enviar un mensaje a un usuario que diga: "tus fotos personales están compartidas en este sitio web, por favor, compruébalo". Al hacer clic en esa URL, el usuario es redirigido a un sitio web falso que parece una red social legítima.

AMENAZAS MODERNAS

Ataque de scripting cruzado

El cross-site scripting es un vector de ataque muy frecuente entre los infiltrados. Fundamentalmente, el ataque ejecuta un JavaScript malicioso en el navegador de la víctima mediante diferentes técnicas. El navegador puede ser secuestrado con un solo clic de un botón que puede enviar un script malicioso al servidor. Este script se devuelve a la víctima y se ejecuta en el navegador. Los enlaces y botones atractivos de las redes sociales más populares, como Twitter y Facebook, pueden engañar al usuario para que siga las URL, así como las alertas emergentes de virus y los anuncios prometedores o los contenidos multimedia que requieren visitar un enlace o hacer clic en un botón para ser desbloqueados. Algunos usuarios pueden ser invitados a copiar y pegar enlaces con JavaScript en la barra de direcciones de su navegador. Estos ataques pueden robar información o actuar como software espía. Estos ataques también pueden secuestrar ordenadores para lanzar ataques a usuarios desprevenidos mientras el verdadero autor del ataque se oculta tras la máquina comprometida.

Ataque de clonación de perfiles

En este ataque, el agresor clona el perfil de los usuarios gracias al conocimiento previo o a la información recopilada en línea. El atacante puede utilizar este perfil clonado en la misma o en otra plataforma de red social para crear una relación de confianza con los amigos del usuario real. Una vez establecida la conexión, el atacante engaña a los amigos de la víctima para que crean en la validez del perfil falso y accedan con éxito a información confidencial que no comparten en sus perfiles públicos. Este ataque también puede utilizarse para cometer otros tipos de ciberdelitos como el ciberacoso, el ciberacoso y el chantaje

Hijacking (secuestro)

En el hijacking, el adversario compromete o toma el control de la cuenta de un usuario para llevar a cabo un fraude en línea. Los sitios sin autenticación multifactor y las cuentas con contraseñas débiles son más vulnerables al hijacking, ya que las contraseñas pueden obtenerse a través del phishing. Una vez secuestrada una cuenta, el secuestrador puede enviar mensajes, compartir el enlace malicioso y cambiar la información de la cuenta, todo lo cual compromete el control del usuario sobre su propia cuenta, así como su reputación.

Ataque de inferencia

El ataque de inferencia infiere la información confidencial de un manipulador que el usuario puede no querer revelar, a través de otras estadísticas que pone el usuario en alguna OSN. Utiliza procedimientos de minería de datos sobre datos visiblemente disponibles como la lista de amigos del usuario y la topología de la red. Mediante esta técnica, un atacante puede encontrar información secreta de una organización o información geográfica y educativa de un usuario.

Sybil attack / Botnet

En el ataque Sybil, un nodo reivindica múltiples identidades en una red. Puede ser perjudicial para las plataformas de redes sociales, ya que contienen un gran número de usuarios que se acoplan a través de una red de pares. Los pares son las estructuras informáticas que se asocian entre sí por medio de Internet y pueden compartir registros directamente sin necesidad de un servidor central. Esta red de máquinas también puede llamarse BotNet. Una entidad online puede crear varias identidades falsas y utilizarlas para distribuir información basura, malware o incluso afectar a la reputación y popularidad de una organización. Por ejemplo, se puede manipular una encuesta web utilizando varias entregas de Protocolo de Internet (IP) para enviar un enorme número de votos, y el agresor puede superar a un cliente genuino. Un ejército similar puede, por ejemplo, compartir un mismo mensaje varias veces y hacer que su contenido sea viral.

Clickjacking

El clickjacking es un procedimiento en el que el invasor engaña a un usuario para que haga clic en una página diferente a la que pretendía. El atacante aprovecha la vulnerabilidad de los navegadores para realizar este ataque. Carga otra página sobre la página a la que el usuario quiere acceder, como una capa transparente. Las dos variantes conocidas del clickjacking son el likejacking y el cursorjacking. La capa frontal muestra la sustancia con la que se puede cebar al cliente. En el momento en que el cliente pulsa sobre ese contenido, en realidad pulsa el botón de "me gusta". Cuantos más individuos les guste la publicación, más se difundirá. En el robo del cursor, un atacante sustituye el cursor real por una imagen de cursor personalizada. El cursor real se desplaza de su posición real del ratón. De esta manera, el intruso puede engañar a un consumidor para que haga clic en el sitio malicioso con un posicionamiento inteligente de los elementos de la página.

Ataque de desanonimización

En bastantes sitios de redes sociales como Twitter y Facebook, los usuarios pueden ocultar o proteger su identidad real antes de publicar cualquier dato utilizando un alias o nombre inventado. Pero si un tercero quiere averiguar la identidad real del usuario, puede hacerlo rastreando las cookies, las topologías de red y la inscripción en grupos de usuarios para descubrir la identidad genuina del cliente. Es una especie de método de minería de información en el que la información misteriosa se cruza con otras fuentes de información para volver a reconocer la información desconocida. Un atacante puede recoger información sobre la pertenencia a un grupo de un usuario robando el historial de su navegador y combinando este historial con los datos recogidos. De este modo, el atacante puede desanonimizar al usuario que visita el sitio web del atacante

AMENAZAS DIRIGIDAS

Ciberacoso

El ciberacoso es el uso de medios electrónicos como correos electrónicos, chats, conversaciones telefónicas y redes sociales en línea para intimidar o acosar a una persona. A diferencia del acoso tradicional, el ciberacoso es un proceso continuo, ya que se mantiene continuamente a través de las redes sociales. El agresor envía repetidamente mensajes intimidatorios, comentarios sexuales, publica rumores y, a veces, fotos o vídeos vergonzosos para acosar a una persona. También puede publicar información personal o privada de la víctima, causando vergüenza o humillación. El ciberacoso también puede producirse de forma accidental, aunque los patrones repetidos de este tipo de correos electrónicos, textos y publicaciones en línea rara vez son accidentales.

Cyber grooming

El cyber grooming consiste en establecer una relación íntima y emocional con la víctima (normalmente niños y adolescentes) con la intención de obligarla a cometer abusos sexuales o mentales, El punto principal del cyber grooming es adquirir la confianza del joven y a través de la cual se puede obtener información íntima e individual del niño. Los datos suelen ser de naturaleza voluptuosa a través de conversaciones sexuales, fotos y vídeos que dan al atacante una ventaja para amenazar y chantajear al niño. Los agresores suelen acercarse a los adolescentes o a los niños a través de identidades falsas en sitios adaptados a los niños, dejándolos vulnerables y sin saber que se han acercado a ellos con el objetivo final del ciberacoso. Sin embargo, la víctima también puede iniciar el proceso de grooming sin saberlo cuando recibe ofertas gratificantes, por ejemplo, dinero en efectivo a cambio de datos de contacto o fotografías personales suyas. El anonimato y la accesibilidad de los medios de comunicación avanzados permiten a los groomers acercarse a varios jóvenes simultáneamente, lo que aumenta exponencialmente los casos de cyber grooming.

yberstalking

El cyberstalking es la observación de un individuo por medio de Internet, el correo electrónico o algún otro tipo de correspondencia electrónica que provoca miedo a la violencia e interfiere en la paz mental de ese individuo. Supone la invasión del derecho a la intimidad de una persona. El agresor rastrea la información personal o confidencial de las víctimas y la utiliza para amenazarlas mediante mensajes continuos y persistentes a lo largo del día. Esta conducta hace que la víctima esté excepcionalmente preocupada por su propia seguridad y le provoca un tipo de problema, miedo o perturbación. Hoy en día, la mayoría de las personas comparten su información personal, como el número de teléfono, el lugar de residencia, la zona y el horario en su perfil de las redes sociales, así como su ubicación en vivo. Un agresor puede reunir estos datos y utilizarlos para el ciberacoso.

Actividad de aprendizaje 2

Pida a los alumnos que trabajen en parejas y pídales que se hagan pasar por su respectivo compañero mientras lo entrevistan durante 10 minutos. Invítelos a que intenten sus respuestas tratando de obtener la información requerida a partir de su forma de vestir, los artilugios que llevan consigo y cualquier otro detalle contextual que les resulte útil para hacerse pasar por ellos.

Actividad de aprendizaje 3

Pida a los alumnos que recorran sus redes sociales durante 1 minuto y cuenten todas las llamadas a la acción, los enlaces y los botones en los que se les invita a hacer clic. Invítelos a reflexionar en grupo sobre cómo cada uno de esos enlaces representa amenazas potenciales y cómo deben decidir cuándo y cuándo no interactuar con el contenido.

Unidad 3 - Consejos para la protección de las redes sociales

Actividad de aprendizaje 1

Distribuya a cada alumno una o varias tarjetas en las que se propongan capturas de pantalla de publicaciones (inventadas) de medios sociales de diferentes plataformas e invíteles a identificar qué información sensible pueden obtener de la publicación única y qué posibles amenazas pueden derivarse de esa publicación.

EL USO DE LAS REDES SOCIALES

Módulo 6

QUÉ ES LA PROTECCIÓN DE LAS REDES SOCIALES

Las directrices de protección de las redes sociales tienen como objetivo evitar el acceso no autorizado a sus cuentas de redes sociales, proteger su identidad en línea de la suplantación de identidad o el robo de datos, y proteger su red de identidades o contenidos maliciosos en las redes sociales.

Dado que las modalidades y los objetivos de las amenazas de las redes sociales suelen depender del tipo de plataforma, también deben tenerse en cuenta algunas prácticas específicas para prevenir las amenazas.

PRÁCTICAS GENERALES

Utilizar una contraseña fuerte: para mantener la seguridad de las cuentas, los usuarios deben elegir una contraseña fuerte. No debe ser demasiado corta, ya que las contraseñas cortas pueden ser fácilmente adivinadas. Debe ser lo suficientemente larga y debe contener valores alfanuméricos con algunos caracteres especiales.

Los usuarios no deben utilizar la misma contraseña que utilizan para otras cuentas, ya que si de alguna manera un atacante llega a conocer esa contraseña, puede comprometer todas las cuentas de ese usuario.

Limitar el uso compartido en la ubicación: Hoy en día, compartir la ubicación se ha convertido en una tendencia. Muchas redes sociales han introducido la función de geoetiquetado, que etiqueta automáticamente la ubicación geográfica de un usuario cuando éste sube cualquier contenido multimedia a las redes sociales. Los usuarios deben subir sus contenidos multimedia en línea con mucho cuidado, ya que pueden contener metadatos sensibles, y se recomienda cambiar el geoetiquetado a modo manual en todos sus dispositivos móviles y cuentas.

Ser selectivo con las solicitudes de amistad: se ha observado que muchos usuarios aceptan solicitudes de amistad sin analizar el perfil completo del solicitante. La gente suele aceptar las solicitudes de amistad basándose en los amigos comunes. Si el solicitante tiene algunos amigos en común, lo aceptan. A veces los atacantes hacen su perfil atractivo deliberadamente o pueden suplantar una cuenta. Por eso, si la persona que envía una solicitud de amistad es desconocida, hay que ignorarla. Podría tratarse de una cuenta falsa que intenta robar información sensible.

Ten cuidado con lo que compartes: los usuarios deben tener cuidado con sus publicaciones, ya que pueden revelar su información personal, y a veces también la de otros. Muchas organizaciones mantienen normas estrictas para compartir información y contenido multimedia. Hay muchos informes de personas que han sido despedidas de su trabajo por compartir información ilegalmente.

Esta situación puede evitarse si los empleados están bien informados sobre los protocolos de la organización en la que trabajan en relación con las fotos, vídeos y mensajes que publican en línea. Compartir información de forma ilegítima puede perjudicar la reputación de una organización en el mercado, así como sus datos y su propiedad intelectual.

Tenga cuidado con los enlaces y las aplicaciones de terceros: Los usuarios ilegítimos pueden acceder a la cuenta de alguien y obtener información sensible compartiendo un enlace malicioso. Hoy en día, las URL acortadas se están haciendo muy populares en varias plataformas de medios sociales. Estas URLs acortadas pueden estar ofuscadas con códigos o scripts maliciosos. Estos scripts intentan recopilar la información personal y confidencial de un usuario, lo que puede servir para violar la privacidad de dicho usuario. Además, los hackers pueden aprovecharse de las vulnerabilidades presentes en una aplicación de terceros integrada en muchas redes sociales populares. Un ejemplo de este tipo de aplicaciones de terceros son los juegos que se pueden jugar en las redes sociales en línea, y que piden la información pública de un usuario para consumir sus servicios. Esta información puede ser proporcionada a personas ajenas o a intervenciones de terceros. Para evitar este riesgo, los usuarios deben tener cuidado al instalar aplicaciones de terceros en su perfil.

Instalar software de seguridad en Internet: Algunas amenazas cuyo patrón es conocido pueden ser fácilmente detectadas a través de antivirus. Amenazas como el cyber grooming, el cyberbullying pueden ser detectadas hasta cierto punto mediante el uso de software antivirus.

PRÁCTICAS PARA LA PLATAFORMA DE INTERCAMBIO MULTIMEDIA

- No se debe publicar información sensible en las fotos o en los pies de foto. Exponer demasiada información privada en un perfil puede ser peligroso.
- Se debe evitar compartir la ubicación actual en las redes sociales. Los servicios de geoetiquetado que ofrecen las diferentes plataformas multimedia deben desactivarse manualmente.
- Si una aplicación no se utiliza durante mucho tiempo, es mejor revocar el acceso a esa aplicación. Hay muchas aplicaciones de terceros que utilizan las cuentas de las redes sociales para iniciar sesión. Por cuestiones de seguridad y privacidad, hay que permitir el acceso sólo a las aplicaciones de confianza.
- Activa la autenticación en dos pasos para todas tus cuentas de redes sociales siempre que sea posible. Esto proporciona una capa adicional de seguridad a la cuenta. En caso de que un adversario descubra la contraseña de un usuario, seguirá necesitando un segundo factor para

PRÁCTICAS PARA LOS FOROS DE DEBATE

- Hay que prestar atención al hacer clic en los enlaces proporcionados por diversas fuentes. Puede tratarse de algún sitio sospechoso que intenta obtener las credenciales del usuario.
- Los usuarios deben vigilar siempre la URL del sitio. Los sitios dañinos pueden parecer irresistiblemente indistinguibles de los reales. Sin embargo, la URL puede contener pequeñas incoherencias, como una ligera variación en la ortografía (por ejemplo, un "0" en lugar de una "o", indiscernible si se lee rápidamente) o un nombre de dominio alternativo.
- Tenga cuidado con las comunicaciones en las que se pide al cliente que actúe con rapidez, se le ofrece algo que parece poco realista o se le solicita información personal.

PRÁCTICAS PARA LAS PLATAFORMAS DE CONEXIÓN SOCIAL

- Los usuarios deben conocer la configuración de privacidad y seguridad de las diferentes plataformas de redes sociales, y utilizarlas.Cada plataforma ofrece secciones de configuración y privacidad destinadas a limitar quién y qué grupos pueden ver diversos aspectos del perfil del usuario. La configuración de privacidad proporcionada por los sitios como configuración predeterminada no debe dejarse sin modificar.
- Cuantos más detalles se proporcionen, más fácil será para un adversario utilizar esa información para robar la identidad o cometer otros ciberdelitos. Por lo tanto, el intercambio de información debe ser limitado.
- Antes de aceptar una solicitud de amistad, hay que comprobar completamente el perfil del solicitante. Se pueden crear diferentes grupos para compartir diferentes tipos de información, como un grupo diferente para colegas y familiares

PRÁCTICAS PARA LAS REDES PROFESIONALES

- Las redes profesionales se utilizan principalmente para crear contactos y aumentar la visibilidad ante posibles empresas de contratación, por lo que, para utilizar una red profesional de forma segura, hay que comprobar los datos proporcionados por otros usuarios antes de añadirlos a la lista de contactos. Por lo general, un adversario no proporciona muchos detalles sobre su carrera.
- Un usuario debe comprobar si hay errores ortográficos o gramaticales en el perfil de alguien, porque si alguien está solicitando un trabajo, debe estar muy bien escrito y no debe tener ningún error ortográfico o gramatical. Debe contener información precisa y bien presentada sobre esa persona.
- Comprobar la coherencia de la carrera de una persona puede ser una buena práctica si un usuario quiere mantenerse seguro en una red profesional. Un perfil que cambia continua y definitivamente en un corto espacio de tiempo es la parte más utilizada como reclamo por el invasor. En el momento en que el defraudador necesita dirigirse a un tipo de organización o vertical, puede simplemente añadir un nuevo puesto que podría ser pertinente para sus objetivos.

- También hay que contrastar la información. Si una persona dice ser de la empresa del empleador, el usuario puede consultar el directorio de la empresa y no debe dudar en verificar con el departamento de recursos humanos de la empresa.

Actividad de aprendizaje 2

Pida a los alumnos que expliquen quién creen que tiene acceso al último post que han publicado en su OSN favorita. Por último, ayúdeles a comprobar su configuración de privacidad y a ver si lo que han dicho se corresponde con la verdad. Abra un debate en grupo sobre sus conclusiones.

Actividad de aprendizaje 3

Invite a los alumnos a mirar de nuevo las tarjetas que han recibido durante la Actividad de Aprendizaje 1 de esta Unidad y pregúnteles si pueden identificar riesgos adicionales en las publicaciones de medios sociales presentadas anteriormente. Pregúnteles qué harían para mitigar esos riesgos.

2. Resultados del aprendizaje del módulo

Conocimiento

- Riesgos y amenazas cibernéticas asociadas al uso de las redes sociales
- Seguridad de las plataformas UGC (UGC = User Generated Content)

Habilidades

- Identificar los diferentes tipos de amenazas a la ciberseguridad

Competencias

- Prevenir y responder a las ciberamenazas en las redes sociales
- Gestionar contraseñas complejas

3. Bibliografía

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

CYBER.VET.EU

IMPROVING CYBERSECURITY READINESS OF THE EUROPEAN VOCATIONAL EDUCATION AND TRAINING SECTOR

MATERIALES DE FORMACIÓN

CYBERSECURITY AWARENESS TRAINING MATERIAL FOR THE VET SECTOR

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

INTRODUCCIÓN A LOS MATERIALES DE FORMACIÓN

JORNADAS DE JUEGOS

INTRODUCCIÓN

Desde el otoño de 2021, relacionado con el Mes Europeo de la Ciberseguridad, hasta la primavera de 2022, los socios del proyecto CYBER.VET.EU organizaron varias GameJams en los países de los socios. Los jóvenes participaron dándoles la oportunidad de acercarse a los temas de ciberseguridad y proporcionándoles nuevas herramientas.

El objetivo principal de esta salida intelectual era resolver la necesidad de una mayor concienciación sobre la ciberseguridad. Se recurrió al proceso de "gamificación" para obtener una solución fácil de adoptar, rápida de implementar, escalable en el tiempo e inclusiva. El proceso de gamificación, definido como "la aplicación de la mecánica de los juegos a contextos no lúdicos con el objetivo de inducir el compromiso y elevar los niveles de motivación", es una forma demostrada de mantener a los usuarios comprometidos con las actividades de aprendizaje, con grandes resultados incluso en periodos cortos de tiempo gracias a la explotación del entretenimiento que motiva a los participantes a comprometerse más con el material y a practicar. Así pues, este producto actuará como una combinación de directrices, formación y práctica, con la característica de ser fácilmente actualizable cuando haya que añadir nuevo material.

RESULTADOS DE LAS ACTIVIDADES / JORNADAS DE JUEGO

- Mayor concienciación sobre la seguridad digital
- Aumento de la concienciación sobre seguridad digital entre las comunidades de los participantes (familia, amigos, colegas).
- Reducción de la tasa de éxito del malware en las instituciones
- Reducción de las fugas de datos
- Aumento del interés por el sector de la ciberseguridad como oportunidad laboral.

AEII / INERCIA DIGITAL [ES]

ACTIVIDADES

Las actividades más relevantes realizadas por los socios españoles AEII e Inercia Digital fueron:

- Hackathon
- Jornadas de juegos
- Jornadas informativas
- Conferencia internacional
- Evento de difusión

RESULTADOS

Las sesiones de GameJam en España proporcionaron algunos resultados útiles que pueden consultarse aquí:

https://scratch.mit.edu/projects/611211889/

https://scratch.mit.edu/projects/611201682/ https://www.youtube.com/watch?v=3QFI9iB0iJU&t=124s

AEII / INERCIA DIGITAL [ES]

GAME JAM

Gamejam in Cyber.EU.VET

20 visualizaciones Fecha de estreno: 3 dic 2021 The main objective of CYBER.EU.VET is to strengthen the European VET capacity to recognize and manage cybersecurity threats (e.g. ...más

0 No me gusta Compartir Descargar Guardar ...

Gamejam in Cyber.EU.VET

20 visualizaciones Fecha de estreno: 3 dic 2021 The main objective of CYBER.EU.VET is to strengthen the European VET capacity to recognize and manage cybersecurity threats (e.g. ...más

0 No me gusta Compartir Descargar Guardar ...

AEII / INERCIA DIGITAL [ES]

Hackathon

Ciberseguridad en la educación

Los socios españoles AEII e Inercia Digital participaron online en un Hackathon del 20 al 22 de octubre de 2021, con 47 participantes, muchos de ellos expertos en informática. https://www.comprometidosporelfuturo.com/proyectos# apoyado por Boehringer Ingelheim en España.

PROBLEMA A RESOLVER

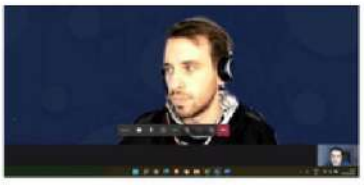
El ciberacoso es uno de los principales riesgos de Internet para los jóvenes. Es habitual encontrar posts con contenido ofensivo hacia algunas personas y que éstos sean utilizados con el fin de acosar y burlarse de las víctimas.

El ciberacoso suele provocar graves alteraciones en las víctimas, como trastorno de estrés postraumático, depresión, pensamientos y conductas suicidas o ansiedad.

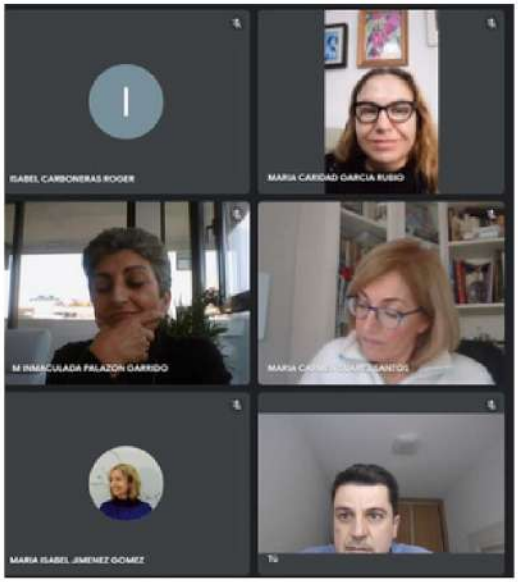
Este reto consiste en estudiar y analizar lo que los jóvenes saben sobre seguridad, así como concienciarles de los riesgos que corren en sus centros educativos y en su vida diaria.
Este reto busca, a través de la gamificación, la mayor concienciación de alumnos y profesores en el día a día en temas relacionados con la seguridad en el uso de las nuevas tecnologías.

RESULTADOS

- Juego y animación vinculados a la ciberseguridad en la educación
- Implicación de la administración pública, centros de FP, expertos en informática, profesores, alumnos y socio del proyecto
- Creación de vídeos cortos interactivos



AEII / INERCIA DIGITAL [ES]



En general, después de realizar numerosas encuestas, los conocimientos de ciberseguridad de los profesores y alumnos de los centros de FP siguen siendo bajos en España. Por ello, este proyecto y otros similares son muy relevantes en España.

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

JORNADA DE JUEGOS

La ONG Nest Berlin, Extrafondente Open Source - EOS e IASIS realizaron conjuntamente una sesión GameJam en febrero de 2022. La GameJam comenzó el sábado 12 y duró 6 días en total. En ella, los equipos nacionales desarrollaron y trabajaron juntos en un borrador de juego (de un juego online o de mesa).
Se reunió un jurado independiente al que se le pidió que evaluara el proyecto de juego siguiendo unas directrices comunes y una plantilla de evaluación.
El equipo ganador recibió una tutoría de 6 meses, así como recursos técnicos para seguir desarrollando la idea de juego.

SOBRE EL JUEGO

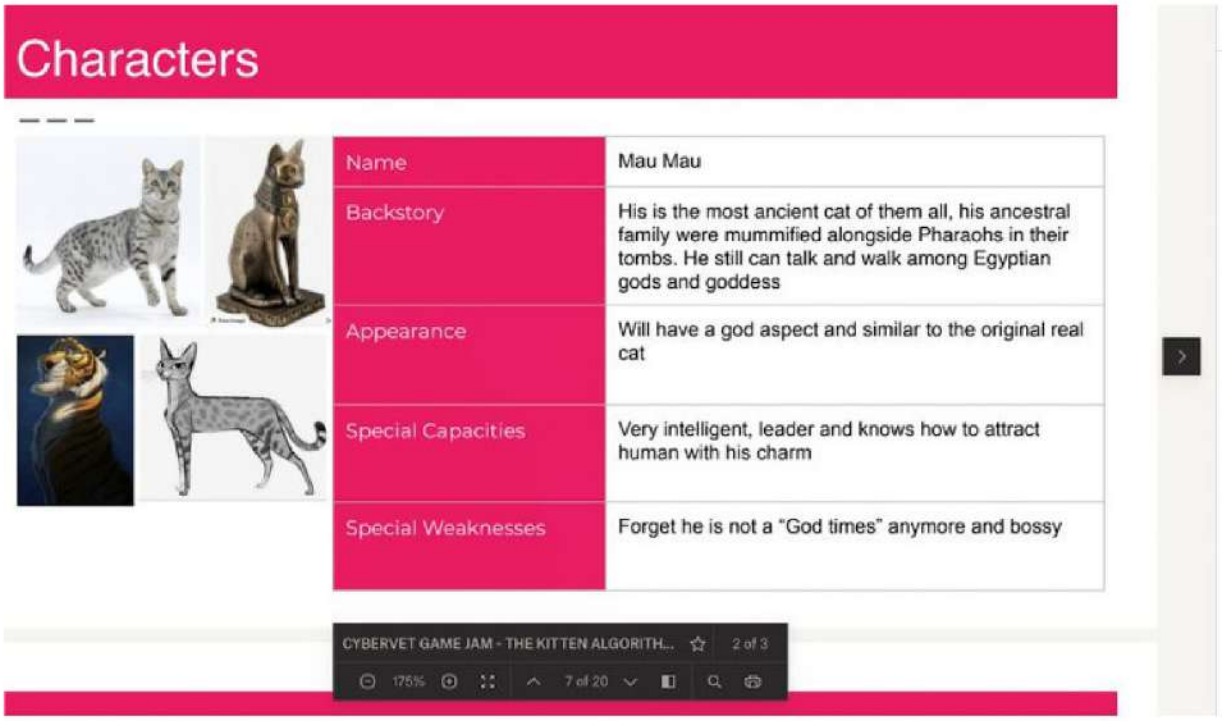
Es un juego de mesa estratégico de 2 a 6 jugadores por turnos, que se juega en unos 30 a 60 minutos. En este juego engañas a los humanos para convencerlos de que eres el mejor gato y consigues más prestigio al conseguir el mayor número de sirvientes de gatos humanos que puedas. Mantén los ojos abiertos, los otros gatos jefes tratarán activamente de sabotear tu camino para llegar a los humanos y llevarse la gloria para ellos. ¡No te fíes de sus bonitas caras!

Pierdes la partida si no tienes un número elevado de humanos como sirvientes o si se acaba la 10ª ronda y ninguno de los jugadores tiene al menos 4 humanos a su cargo.

La dificultad radica en que hay 6 Jefes que intentan engañar a los humanos para que sean sus sirvientes y así los jefes puedan controlarlos, pero todos tienen el mismo objetivo y algunos incluso podrían estar ayudando a los humanos a liberarse del control del gato.

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

Mau Mau



LECSA (LV)

JORNADA DE JUEGOS

El socio LECSA de Letonia organizó un evento GameJam del 27 de septiembre al 1 de octubre de 2021. Debido a las restricciones epidemiológicas y a las diferentes ubicaciones de los participantes, se organizó como un evento de tipo híbrido (in situ en la Escuela Técnica de Saldus y a través de la plataforma Zoom). Durante el evento se formaron 6 equipos (4-5 personas por equipo) para trabajar en el desarrollo de prototipos de juegos. Para conseguir resultados tangibles, el concepto de la Game Jam preveía el desarrollo de dos tipos de juegos: de ordenador y de mesa.

ACTIVIDADES

- Los meses de agosto y septiembre de 2021 se dedicaron a la planificación y organización del evento (búsqueda de expertos en ciberseguridad y desarrollo de juegos, distribución de información a los posibles participantes, planificación de la agenda y definición de criterios para el juego, etc.)
- Evento multiplicador - Actualidad en los ciberataques (27.09.2021): Presentación del proyecto CYBER.EU.VET y conferencia sobre las tendencias en los ciberataques con el Sr. Armins Palms, experto en ciberseguridad de CERT.LV (Institución de Respuesta a Incidentes de Seguridad Informática de la República de Letonia)
  - Número de participantes: 26 personas
  - Lugar: Escuela Técnica de Saldus (ciudad de Saldus) y plataforma ZOOM
- Anuncio del Game Jame (27.09.2021): definición y debate sobre los retos actuales en materia de ciberseguridad (evaluación de necesidades); formación de equipos, reunión con los mentores y debate sobre el trabajo posterior (taller sobre el motor de juego Unity), lluvia de ideas sobre la idea y el concepto del juego.
- Actividades de la Game Jam en curso (28.09-30.09.2021): los equipos trabajaron en el desarrollo de prototipos, se consultó a los mentores, si era necesario.
- Presentación del progreso (30.09.2021): presentación de los conceptos del juego y del progreso del trabajo para recibir las sugerencias de los mentores.
- Gran final (01.10.2021): cuatro equipos presentaron sus resultados y los mentores hicieron una evaluación. Un equipo, que desarrolla un juego de ordenador, ha abandonado. Conclusión del evento y debate informal.
  - Número de participantes:
  - Lugar: Escuela Técnica de Saldus y plataforma ZOOM

LECSA (LV)

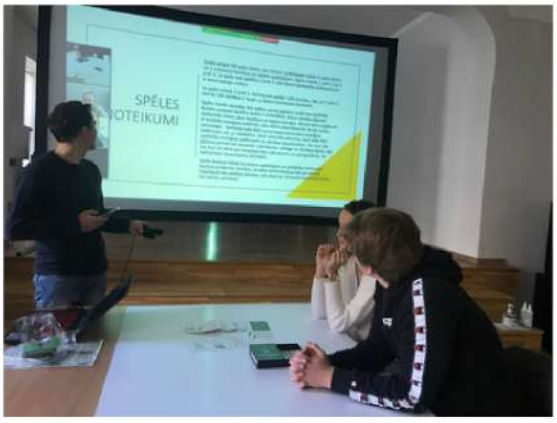
RESULTADOS

1.Prototipo de juego online - El Virus

2. Juego de mesa - Cartas sobre la seguridad

3. Juego de mesa - Ciberguerra

4. Juego de cartas competitivo - Mente cibernética



EJEMPLO - Mente cibernética - Un juego de cartas competitivo

Se trata de un juego de cartas educativo con elementos de concurso. La tarea principal del juego es enseñar
los fundamentos de la seguridad cotidiana en Internet y a qué se expone la gente al hacer tonterías en ella. Abarca temas como la seguridad en Internet y la protección de datos en el contexto del uso de las redes sociales. Como resultado del juego, las personas (los jugadores) deben ser capaces de reconocer los intentos de estafa en la vida real.

Desarrollado por el equipo Veiksminieki (del letón: gente de éxito), estudiantes de la escuela técnica Saldus durante la Game Jam de Letonia (octubre de 2021):
Renars Ricards Hartmanis, Estere Ozoliņa, Sindija Diāna Valtere y otros.
Nivel: básico (para principiantes). Destinatarios: alumnos, estudiantes, profesores y padres.
El juego contiene: 50 cartas, 2 almohadillas de salud (para contar la salud de los jugadores), 2 dados y tarjeta de reglas.

LECSA (LV)

JORNADA DE JUEGOS

SOBRE EL JUEGO

Los intentos de ciberataques en el mundo aumentan cada día, por lo que el gobierno mundial tuvo la idea de organizar un torneo para identificar a las personas de alrededor que están trayendo riesgos cibernéticos, y contraatacar contra ellos.

El juego educativo ayuda a conocer los principales tipos de ciberataques, los métodos de prevención y eliminación protegiéndose a sí mismo o a su equipo y contraatacando al adversario. El objetivo del juego es quitarle toda la vida al/los oponente/s.

CÓMO JUGAR - NORMAS

Número de jugadores: 2 o 4 personas (1 vs 1 o 2 vs 2).

Cada jugador o equipo (cuando es de 2 contra 2) tiene "100 vidas" (Salud=HP) al principio de la partida. El recuento de la salud se realiza mediante el uso de libretas negras u otras notas disponibles.

Asigna a una persona distinta que siga y calcule el consumo de energía y salud de los jugadores, si es posible. De lo contrario, los jugadores lo hacen por sí mismos.

Cada jugador recibe 5 cartas. Si la partida se juega 2 contra 2, ambos jugadores tienen "una mano común" en el equipo o 10 cartas juntas.

Hay tres tipos de cartas: Cartas de ataque (rojas), Cartas de escudo (amarillas) y Cartas de vida (verdes).

El juego se desarrolla en rondas. El jugador/equipo que saque el número más alto con los dados comienza la partida.

Cada carta cuesta energía. Al principio de cada ronda, el jugador tira 2 dados para definir una energía que se indica en la parte superior de la carta (en azul). Hay que jugar las cartas para no sobrepasar la cantidad de energía tirada.

El jugador/equipo que protagoniza la ronda puede atacar (con cartas de ataque), protegerse (cartas de escudo) o sumar vida (cartas de curación), mientras que los segundos sólo pueden usar cartas de ataque y de escudo para minimizar su vulnerabilidad de vida.

Ten en cuenta que el número máximo de vidas por jugador/equipo durante la partida puede ser de 100 HP (por ejemplo, si la suma de vidas y energía después de la ronda hace 110 HP en total, tu número de vidas sigue siendo - 100 HP).

El juego termina cuando un jugador/equipo se queda sin todas las vidas (0 vidas).

Si el juego se queda sin cartas, hay que barajar de nuevo las cartas del montón.

LECSA (LV)

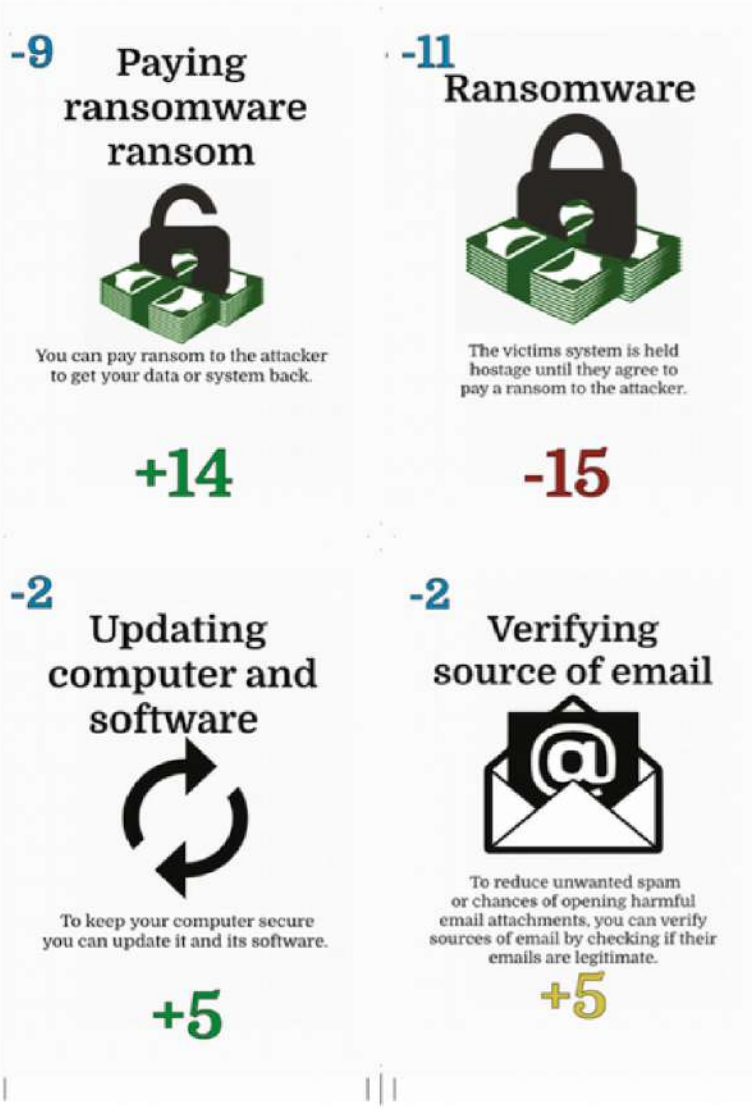
Ejemplo de cartas

En **azul** – energía

En **rojo** - cartas de ataque

En **amarillo** - cartas de escudo

En **verde** - cartas de vida



Ejemplo de cálculo de salud

EJEMPLO Guerra cibernética - juego de mesa

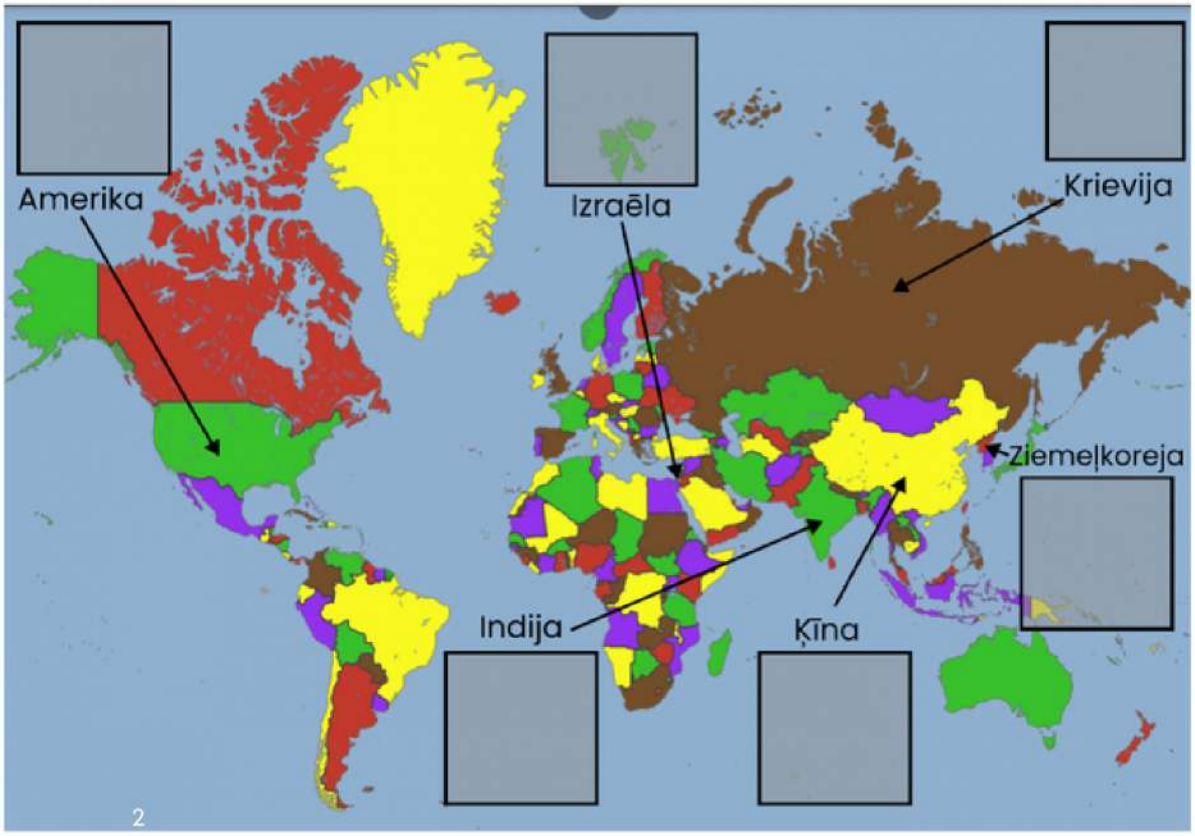
Desarrollado por el equipo Exodus (estudiantes de la Escuela Técnica de Saldus), líder del equipo Valdemārs Šperbergs.

2-6 jugadores < - > Adecuado para personas mayores de 15 años.
Un juego de mesa con un fuerte énfasis en la táctica y la aleatoriedad (azar).

Nivel: juego educativo para aquellos que tienen algunos conocimientos sobre ciberseguridad.
El juego contiene: El juego contiene: Mapa del mundo, 2 dados, servidores, tarjetas con función "ataque", "defensa" o "reacción", leyenda de vulnerabilidades.

SOBRE EL JUEGO

El objetivo del juego es proteger el país representado por el jugador y atacar a otros países para ganar la ciberguerra. En Cyberwar, cada jugador debe elegir un país para representar. Cada jugador tiene un servidor con 3 vulnerabilidades. El objetivo del jugador es hackear los servidores de otros países explotando dos de las tres vulnerabilidades o arreglar dos de las tres vulnerabilidades de su propio servidor.



LECSA (LV)

CÓMO JUGAR

Los jugadores eligen el país que van a representar y colocan un objeto del servidor en el lugar designado del mapa. Cada país tiene sus propias bonificaciones.

Cada jugador sortea (toma) 3 vulnerabilidades -una de cada nivel de dificultad-, y las coloca boca abajo en sus respectivas ubicaciones en sus campos de servidor. Las vulnerabilidades no son conocidas por los jugadores.

Las vulnerabilidades tienen 3 niveles de dificultad. El nivel de dificultad también determina el número necesario para explotar una vulnerabilidad (ver "Ataques"), así como determina cuántos movimientos se necesitarán para solucionar la vulnerabilidad (ver "Defensa").

El juego se desarrolla en rondas, en las que se pueden realizar las siguientes acciones (movimientos): **Exploración, Ataque y Defensa**. Los jugadores determinan la secuencia de jugadores tirando dos dados.

INICIO

- Cada jugador recibe 4 cartas al principio de cada ronda. Al final de la ronda, es posible - quedarse con 2 cartas o cambiarlas por otras existentes.
- La 1ª ronda es una ronda de exploración en la que no se permiten cartas de ataque o defensa. En las rondas siguientes, los jugadores pueden elegir entre Escanear o Atacar o intentar reparar sus vulnerabilidades (ver la defesa). El juego continúa ronda a ronda hasta que se alcanza una condición de victoria.

Exploración

- El atacante elige un país para explorar su vulnerabilidad (por ejemplo, "Estoy escaneando un ruso de 2º nivel de vulnerabilidad").
- El jugador realiza el chequeo - tira dos dados, aplicando las bonificaciones de su país representado, compara con el nivel de dificultad de la vulnerabilidad + las bonificaciones del país de la víctima.
- Si el atacante saca un número igual o mayor que el nivel de dificultad de la vulnerabilidad de la víctima, el atacante puede mirar la vulnerabilidad escaneada.

Las bonificaciones del país no se añaden cuando se explora.

-

Niveles de dificultad

1º - el jugador debe sacar al menos el número 4 (excluyendo las bonificaciones del país)

2º - el jugador debe sacar al menos el número 8 (excluyendo las bonificaciones del país)

3º - el jugado r debe sacar al menos el número 11 (excluyendo las bonificaciones del país).

ATAQUE

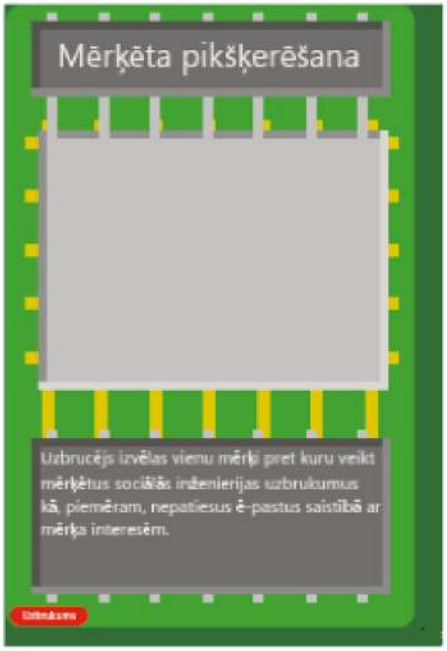
- El jugador nombra el objetivo del ataque (por ejemplo, "Ataco una vulnerabilidad rusa de nivel 2") y revela la carta de ataque a todos los jugadores, colocándola junto a la vulnerabilidad.
- El jugador tira los dados para ver si el ataque funciona comparando la tirada con la dificultad de la vulnerabilidad + los bonos (si el número tirado + los bonos coinciden o superan la dificultad, el ataque tiene éxito).
- Los ataques pueden ser forzados a retroceder utilizando la Carta de Reacción que está diseñada para ese ataque.
- Cada ataque tiene su propio tipo de reacción que se puede jugar y su propio tipo de vulnerabilidad para la que funciona.
- Si el ataque falla o es bloqueado por una Carta de Reacción - las cartas de Ataque y Reacción jugadas permanecen en la mesa hasta el final de la siguiente ronda e impiden el ataque de otros jugadores con el mismo ataque para la misma vulnerabilidad. Después del movimiento, ambas cartas vuelven al montón.

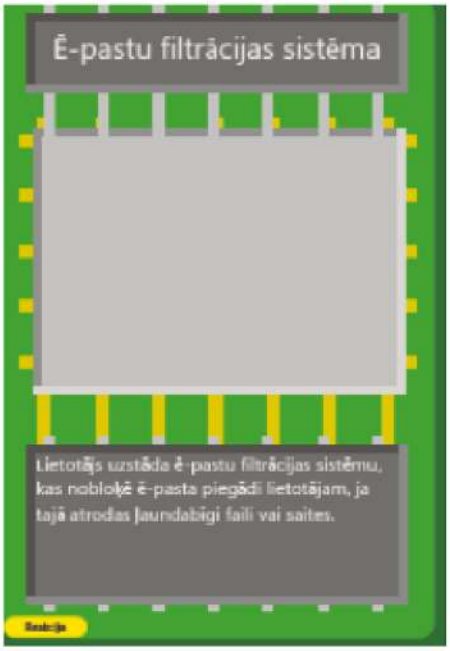
Niveles de dificultad

1º - el jugador debe sacar al menos el número 4 (excluyendo las bonificaciones del país)

2º - el jugador debe sacar al menos el número 8 (excluyendo las bonificaciones del país)

3º - el jugador debe sacar al menos el número 11 (excluyendo las bonificaciones del país).





LECSA (LV)

Defensa

- Defensa: elegir el método adecuado contra una vulnerabilidad concreta. Las Cartas de Reacción detienen (cancelan) el ataque entrante (y todos los demás ataques dirigidos a la misma vulnerabilidad) durante 1 turno.
- Para cancelar un ataque entrante, el jugador coloca una Carta de Reacción que coincida con el tipo de ataque (Ver tabla con las vulnerabilidades) sobre la carta de ataque tan pronto como se juegue el ataque.
- Para empezar a reparar una herida, el jugador coloca una Carta de Defensa al lado de la herida a reparar.
- Otros jugadores pueden atacar esta herida mientras está en Défense (antes de que termine el turno de Défense).
- Cuando el jugador intenta reparar una herida en su servidor con una Carta de Défense, ésta no puede atacar, pero puede intentar evitar los ataques con Cartas de Reacción. Para la reparación completa, se requiere un turno de |nivel de dificultad + 1|. La acción de exploración está permitida durante el periodo de reparación.
- Si el método de Defensa no es correcto, el jugador se salta 3 turnos y no puede usar Cartas de Defensa durante este periodo (las reacciones y las acciones de exploración están permitidas).

Bonificaciones de los países

Estados Unidos: +2 en exploración

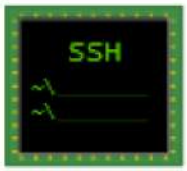
- Rusia: +2 en ataques
- China: +2 en defensa contra ataques
- Corea del Norte: +2 por defensa contra el escaneo
- India: +1 en todos los ataques, -1 contra ataques
- Israel: +3 en todos los ataques, -3 contra ataques

Vulnerabilidad por niveles

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)



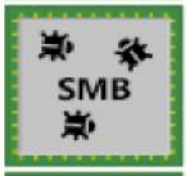
SSH serveris

SSH serveris ar lietotājvārdu

Administrācijas panelis

Administrācijas panelis ar lietotājvārdu

Neapmācīts darbinieks

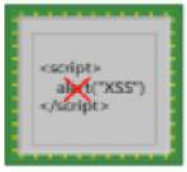


Ievainojams SMB protokols

XSS ievainojums

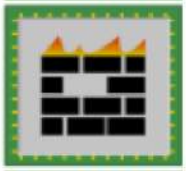
SQL injekcija

Rūtera panelis ar noklusējuma lietotājvārdu un paroli



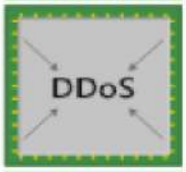
XSS ievainojums ar filtru

SQL injekcija ar filtru



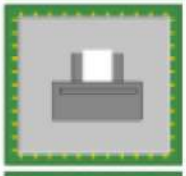
Nepilnīgi nokonfigurēts ugunsmūris

WiFi tīkls ar WEP drošību

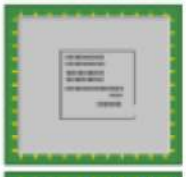


Pakalpojuma atteices kļūda

Ievainojama OpenSSL programma



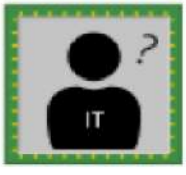
Ievainojama Print Spooler programma



Bufera pārpildes ievainojums

Vājš jaucējvērtības algoritms

Aizņemts priekšnieks



Slinks IT speciālists

LECSA (LV)

JORNADAS DE JUEGO

LECSA (LV)

CONSEJOS Y EXPERIENCIAS DE LA JORNADA DE JUEGOS EN LETONIA

- Durante los dos días del evento no es posible desarrollar un juego de ordenador real, sino el primer prototipo, que puede o no seguir desarrollándose dependiendo de la motivación de los participantes.
- Los premios u otros tipos de beneficios pueden ayudar a involucrar a más participantes y asegurar mejores resultados (más tangibles) al final (en nuestro caso - se proporcionó pizza y bebidas al final del evento, más apoyo de los mentores, (por ejemplo, la colocación de juegos en la plataforma)).
- Los mentores en materia de desarrollo de juegos y ciberseguridad desempeñan un papel importante en la Game Jam, ya que asesoran y ayudan a los participantes.
- Planificar con antelación: al tratarse de un evento bastante complejo, requiere una cuidadosa planificación.
- Los organizadores deben tener en cuenta que algunos equipos pueden quedar fuera de la competición (debido a la limitación de tiempo).

Consulta los posts de FB con los resultados del evento:
https://www.facebook.com/cybereuvetproject.eu/posts/138127645211214
https://www.facebook.com/saldustehnikums/posts/1780232175520378

¡El evento fue organizado por LECSA en cooperación con la Latvijas Universitāte | Ekonomikas un kultūras augstskola / EKA University of Applied Sciences | McĀbols | cert.lv | Coldwild Games | Saldus tehnikums!

MEATH PARTNERSHIP (IE)

ACTIVIDADES

- Reunión informativa de evaluación de necesidades con los estudiantes (formación en codificación en un centro local de educación de adultos)
- Jornada de juegos de 2 días (sesión informativa en línea el primer día; segundo día dedicado a la jornada de juegos)

Evento multiplicador - Mañana de concienciación sobre ciberseguridad

DESCRIPCIÓN & RESULTADOS

1) Reunión informativa de evaluación de necesidades con los estudiantes (formación en codificación en un centro local de educación de adultos) Fecha: Octubre 2021

DESCRIPCIÓN

Para difundir el proyecto e identificar los temas principales de la jornada de juegos, el equipo de Meath Partnership organizó una sesión informativa con los alumnos de una clase local de formación en codificación. El intercambio de información sobre ciberseguridad y el debate sobre las amenazas más recientes fueron seguidos por una sesión de lluvia de ideas en la que los estudiantes se dividieron en dos grupos para debatir cuestiones que permitieran identificar los temas más interesantes que se explorarían durante el Gamejam. También se compartió con los participantes más información sobre la jornada de juegos y el proyecto CYBER.EU.VET.

EJEMPLO DE EVALUACIÓN DE NECESIDADES


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)

RESULTADOS

Como resultado de esta actividad, el equipo de Meath Partnership obtuvo una mejor comprensión de los conocimientos generales de los estudiantes en relación con la ciberseguridad y las ciberamenazas, además de recoger información que se incluyó posteriormente en el proceso de planificación y ejecución de la jornada de juegos.

LA EVALUACIÓN EN ACCIÓN

MEATH PARTNERSHIP (IE)

JORNADAS DE JUEGOS

2) Jornada de juegos de 2 días
(sesión informativa en línea el primer día; segundo día dedicado a la jornada de juegos)

DESCRIPCIÓN

El día 1 se dedicó a dar la bienvenida a los participantes y a presentar el proyecto CYBER.EU.VET y a inaugurar la Game Jam, así como a compartir información sobre los 2 temas identificados durante la reunión de evaluación de necesidades. Se ofreció a los participantes la posibilidad de trabajar individualmente o en equipo. También tuvieron la oportunidad de hacer cualquier pregunta o recibir más aclaraciones sobre los procedimientos
relacionados con el desarrollo de los juegos en el día 2.

El día 2 se dedicó al desarrollo de los juegos y los miembros de nuestro equipo y un experto en apoyo informático estuvieron disponibles a través de Zoom para apoyar a los participantes durante toda la duración de la Game Jam desde las 9 de la mañana hasta las 9 de la noche.
9 de la mañana hasta las 9 de la noche.
Se invitó a los participantes a subir sus juegos a la plataforma Itchio bajo un perfil creado para este evento: CYBER.EU.VET : Cybersecurity Game Jam - itch.io

RESULTADOS

Después de que los participantes compartieran sus borradores de juegos con el equipo, uno de ellos decidió seguir adelante y subir el juego para su posterior evaluación. El resto de los participantes decidieron no presentar sus borradores, ya que estaban en una fase muy temprana.

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

Juego de ciberseguridad interactivo en línea:
https://itch.io/jam/cybereuvet-cybersecurity-gamejam

MEATH PARTNERSHIP (IE)

3) Evento multiplicador - Mañana de concienciación sobre ciberseguridad
Fecha: Noviembre 2021

DESCRIPCIÓN

El Evento Multiplicador se celebró en línea a través de Zoom con el fin de dar a conocer el proyecto y sus actividades. El evento fue ampliamente difundido entre una amplia variedad de partes interesadas o involucradas en la Ciberseguridad. El evento comenzó con una presentación y una visión general del proyecto y de la Game Jam, seguido de una presentación y un debate sobre la Ciberseguridad y el intercambio de información práctica sobre cómo mantenerse en línea (las amenazas cibernéticas actuales y cómo eliminar posibles ataques fueron posibles).

RESULTADOS

El Evento Multiplicador contribuyó a dar a conocer el proyecto y también creó la oportunidad de presentar los hitos logrados desde el inicio del proyecto a un público más amplio. También fue una gran oportunidad para compartir información práctica y consejos relacionados con la ciberseguridad con los participantes que asistieron al evento.

COFAC / UNIVERSIDADE LUSÓFONA (PT)

JORNADA DE JUEGOS

ACTIVIDADES

1) Postgrado en Ciber-Hacking Ético para futuros profesionales y profesores del mercado Oct 2021 - Feb 2022 (en colaboración con una consultora local llamada Cybersec)

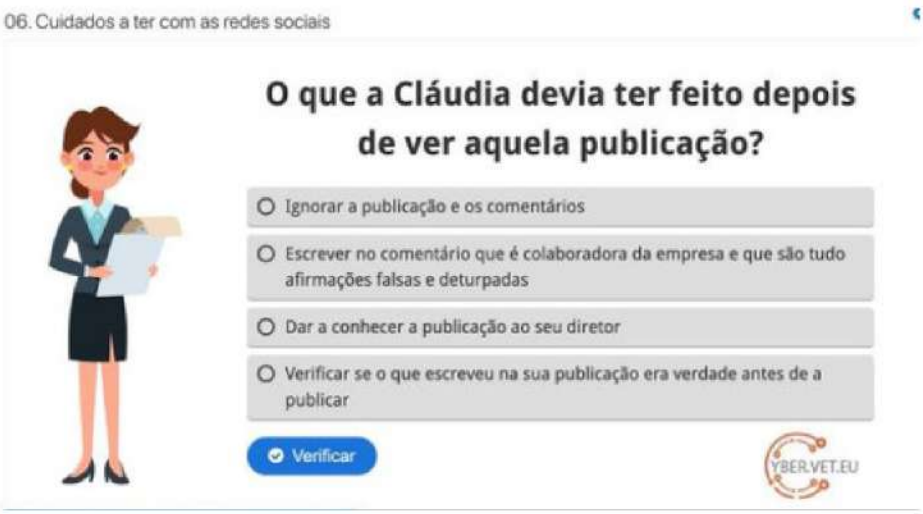
2) 2 sesiones de GameJam impartidas en enero de 2022 en centros de FP:
Escola de Comércio de Lisboa - https://escolacomerciolisboa.pt
Escola Profissional Almirante Reis - https://www.epar.pt

3**)** Una ciberformación de tres días y medio para estudiantes de secundaria en marzo de 2022 en Universidad Lusofona como parte del evento Tecweb - https://tecweb.ulusofona.pt

RESULTADOS

Informe de difusión de pruebas donde se pueden ver las diferentes pruebas que se han realizado durante un año natural (abril 2021 a abril 2022). En este informe podemos ver capturas de pantalla de publicaciones en redes sociales, carteles de diferentes eventos, cuestionarios de concienciación sobre ciberseguridad (disponibles en idioma portugués en https://docs.google.com/forms/d/e/1FAIpQLSeXACV_oeplRpTfbaC1NFKED76kRSYD6cT8cFMKjc7ohGMHZw/viewform).

Durante los Cyberjams, también se creó, a partir de las encuestas de concienciación sobre ciberseguridad, un conjunto de minijuegos amigables/interactivos sobre situaciones sencillas realizadas.



TANDEM PLUS NETWORK – MEMBER IASIS [GR]

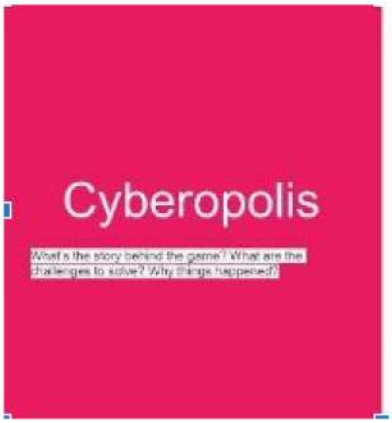
JORNADA DE JUEGOS

Herramienta de diseño de juegos (IASIS) - Ciberopolis

Este juego es un juego de mesa dirigido a personas interesadas en la ciberseguridad, con un máximo de 2 a 4 jugadores, y sus aspectos principales son la confidencialidad y la integridad de los datos... mientras que los temas que trata son el malware, el phishing, los ataques basados en la web, los ataques a aplicaciones web, el spam, el robo de identidad, el DDoS y el Man in the middle...

Consulta la imagen de ''Ciberopolis'' para entender mejor los pasos a seguir durante el juego y qué retos hay que resolver...

Capturas de pantalla del juego durante la sesión de GameJam donde podemos ver el éxito del juego y el gran interés mostrado por los participantes.



TANDEM PLUS NETWORK – MEMBER IASIS [GR]

VIDEO - Prevenir el ciberacoso

Este vídeo elaborado por el socio griego acerca a los visitantes a diferentes formas de prevenir y combatir el ciberacoso.

YBER.EU.VET

Funded by
the European Union

AVISO LEGAL

Diseño
NGO Nest Berlin e.V.
Berlin, 2022

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