



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



IMPROVING CYBERSECURITY READINESS OF
THE EUROPEAN VOCATIONAL EDUCATION
AND TRAINING SECTOR

CYBER.EU.VET

RISULTATO
103

TOOLKIT PER
FORMATORI



CYBER.VET

CORSO DI FORMAZIONE

Introduzione

I partner del progetto CYBER.EU.VET hanno elaborato questo programma di formazione, comprendente 6 moduli pensati per l'utilizzo da parte di insegnanti ed educatori nell'ambito della formazione professionale. Ogni modulo include concetti teorici, esempi pratici ed esercizi da svolgere in gruppo. Il programma formativo è stato pensato per essere utilizzato in diversi Paesi Europei e deve essere adattato ai specifici bisogni formativi di ciascuno di essi. In particolare, ci si aspetta che il formatore adatti alle particolari esigenze gli esempi pratici e i casi di studio forniti dal programma.

I MODULI SVILUPPATI DAI PARTNER SEGUONO LA SEGUENTE STRUTTURA:

MODULO 1 - GLI ATTACCHI INFORMATICI - LECSA (LETONIA)	01
MODULO 2 - IL CYBERBULLISMO - AEII (SPAGNA)	15
MODULO 3 - PREVENIRE IL CYBERBULLISMO - IASIS (GRECIA)	21
MODULO 4 - AUTENTICAZIONI E PASSWORD - MEATH PARTNERSHIP (IRLANDA)	27
MODULO 5 - IL WI-FI E LA SICUREZZA - UNIVERSIDADE LUSÓFONA (PORTOGALLO)	35
MODULO 6 - L'UTILIZZO DEI SOCIAL MEDIA - EOS (ITALIA)	37

ATTACCHI INFORMATICI

Modulo 1

1. Presentazione del modulo

Gruppi target

▪ Educatori del settore professionale della formazione

▪ Studenti

▪ Rappresentanti di istituzioni pubbliche attive nei settori educativi: comuni, autorità regionali e nazionali;

Descrizione del modulo

Considerando il crescente numero e la portata degli attacchi informatici ogni anno, in particolare alla luce degli ultimi eventi economici, politici e sociali (conseguenze delle restrizioni Covid-19, conflitto militare in Ucraina, ecc.), è importante parlare di attacchi informatici reali più frequentemente.

Pertanto, lo scopo della formazione è fornire una comprensione fondamentale degli attacchi informatici e imparare come reagire correttamente a possibili incidenti.

Il contenuto di questo modulo copre i seguenti aspetti (unità):

- Definizioni e questioni rilevanti
- Tipologia di attacchi
- Gli incidenti più frequenti (esempi pratici)

Obiettivi formativi

- Al termine di ogni unità è prevista un'attività pratica.
come proteggersi dagli attacchi informatici e come reagire correttamente agli incidenti.
Fornire una comprensione fondamentale delle questioni relative agli attacchi informatici.
- Comprendere le conseguenze e gli impatti dei potenziali attacchi e minacce informatiche.
- Riconoscere e classificare le forme più comuni di attacchi informatici.
 - Imparare a reagire agli attacchi - come segnalare, se si verifica un incidente.

Durata complessiva

▪ Garantire fonti di informazione e letteratura per ulteriori e più specifici apprendimenti, per seguire effettivi attacchi informatici utilizzando adeguate modalità di protezione.
Max 1,5 ore

ATTACCHI INFORMATICI

Modulo 1

Questo modulo verrà utilizzato dal formatore con l'utilizzo di una presentazione PowerPoint che supporta la spiegazione tramite elementi visivi, esempi pratici ed esercizi (max. 20 minuti + un'attività pratica per ogni unità).

Si consiglia di preparare le presentazioni sui modelli PPT creati per il progetto CYBER.EU.VET. Considerando i rapidi sviluppi e progressi nel campo della sicurezza informatica, si raccomanda di rivedere continuamente le unità e, se necessario, adeguare il contenuto tenendo conto degli sviluppi più recenti nel campo.

Inoltre, si raccomanda ai formatori di adattare questo modulo alle esigenze dell'IFP locale e di includere esempi di incidenti informatici specifici. Questo modulo copre principalmente esempi pratici della Lettonia e alcuni esempi internazionali. Si raccomanda di prestare maggiore attenzione all'Unità 3 per analizzare e discutere esempi pratici di incidenti, insieme a immagini e video.

Unità 1 - Attacchi informatici

Cosa significa? Introduzione all'argomento

Attività didattica #1 - Teoria

Definizione

Attacco informatico (pl. attacchi informatici) = un tentativo di ottenere un accesso illegale e non autorizzato a un computer o sistema informatico allo scopo di danneggiarlo o manipolarlo. Il suo scopo è disabilitare, interrompere, distruggere o controllare i sistemi informatici o alterare, bloccare, eliminare, manipolare o sottrarre i dati contenuti in tali sistemi. Con la comparsa delle restrizioni del Covid-19 e la necessità di passare a un formato di lavoro e apprendimento digitale, il numero di minacce e attacchi informatici è aumentato e la protezione digitale è diventata più importante.

Il termine "attacco informatico" è strettamente correlato a termini quali "minaccia informatica" (possibilità che si verifichi un particolare attacco) e "rischio informatico".

Attacchi informatici più comuni: attacco malware, attacco phishing, attacco man-in-the-middle, attacco password, attacco denial of service e molti altri.

Tipi di comunicazione degli aggressori: contatti personali, telefono, posta elettronica, malware. (Fonte: <https://cert.lv/lv/2022/02/kiberuzbrukuma-riskam-paklauts-ikviens-interneta-lietotajs>; <https://www.investopedia.com/terms/c/cybersecurity.asp>)

ATTACCHI INFORMATICI

Modulo 1

Chi può eseguire attacchi informatici?

Un attacco informatico può essere lanciato da qualsiasi parte del mondo da qualsiasi individuo o gruppo utilizzando una o più diverse strategie di attacco e può essere mirato a individui, aziende pubbliche o private (aziende).

Perché si verificano attacchi informatici e cosa possono causare?

Gli attacchi nell'ambiente virtuale sono generalmente correlati al furto di identità, all'acquisizione di risorse informatiche, al furto e alla falsificazione di informazioni, all'accesso a segreti commerciali, al ricatto o alla diffamazione. Gli attacchi informatici sono progettati principalmente per ottenere guadagni finanziari (ad esempio rubando numeri e codici di carte di credito), interruzioni e vendette (ad esempio per danneggiare la reputazione di un'organizzazione). Ad esempio, crisi come il Covid-19 o il conflitto militare in Ucraina vengono utilizzate per attirare l'attenzione degli utenti tramite e-mail fraudolente e annunci sui social media.

STATISTICHE: Il lavoro a distanza forzato dalla pandemia ha ovviamente aumentato i rischi per la sicurezza informatica e facilitato nuovi tipi di incidenti. La maggior parte di essi è rilevante anche per gli istituti di istruzione e dovrebbe essere presa in considerazione nelle ulteriori attività di istruzione e formazione per educatori e giovani.

Secondo le informazioni analizzate da Deloitte, nell'aprile 2020 in Svizzera si sono verificati 350 attacchi informatici, rispetto a una norma di 100 - 150 attacchi informatici - (phishing, siti Web fraudolenti, attacchi diretti alle aziende ecc.).

L'aumento del lavoro da remoto richiede una maggiore attenzione alla sicurezza informatica, a causa della maggiore esposizione al rischio informatico. Ciò è evidente, ad esempio, dal fatto che il 47% delle persone cade vittima di una truffa di phishing mentre lavora da casa.

In Lettonia, ad esempio, il numero più alto di indirizzi IP univoci minacciati in Lettonia è stato rilevato da febbraio ad aprile 2020, quando è iniziata la pandemia di Covid-19 (oltre 10.000 al mese) secondo il CERT.LV (Information Technology Security Incident Response Institution della Lettonia), che pubblica mensilmente e annualmente i dati e la panoramica degli incidenti più rilevanti denominati "Kiberlaikapstākji" (Cyber Weather).

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

Strumento interattivo: **mappa live delle minacce informatiche (mondo)**

ATTACCHI INFORMATICI

Modulo 1

Attività didattica #1 - Pratica

Discussione con i partecipanti in materia di attacchi informatici (10-15 min):

- 1) Che tipo di attacchi informatici conosci?
- 2) Tu o parenti/amici avete mai subito un attacco informatico/incidente informatico? Come è andata a finire?

Unità 2 - Tipologie di attacchi informatici

Attività didattica #2 - Teoria

Tipologie e metodi più diffusi di attacchi informatici:

Il **malware** è un software dannoso (worm, virus) che viene utilizzato per danneggiare i dispositivi dell'utente (computer, telefoni, ecc.) o la rete. Esempi di malware: spyware e trojan, worm, virus, adware, spam. A seconda del tipo di codice dannoso, il malware può essere utilizzato dagli hacker per rubare o copiare segretamente dati sensibili, eliminare dati, bloccare l'accesso ai file, interrompere le operazioni di sistema o rendere i sistemi inutilizzabili [DigiCERT].

Il malware viene diffuso principalmente per due scopi: ottenere informazioni (spiando il malware inoltrando dati dal dispositivo della vittima) o per realizzare un profitto (crittografando il ransomware che crittografa i dati sul dispositivo dell'utente e successivamente viene richiesto un riscatto all'utente) [Rapporto CERT 2020]

Phishing o truffe sui dati personali: un metodo in cui un hacker invia un'e-mail apparentemente legittima chiedendo agli utenti di divulgare informazioni riservate. I destinatari vengono indotti a scaricare il malware contenuto nell'e-mail aprendo un file allegato o un collegamento incorporato. Di solito si tratta di siti web che sembrano vere e proprie aziende e gli utenti devono inserire i propri dati personali (conto bancario, numeri di carta di credito e password, comprese quelle dei servizi di autenticazione). La truffa dei dati può essere eseguita anche tramite telefonata o tramite messaggi WhatsApp [Investopedia]

Denial of Service (DoS): gli hacker bombardano i server di un'organizzazione con grandi volumi di richieste di dati simultanee fino a quando il target non può rispondere o si blocca, rendendo così i server incapaci di gestire eventuali richieste legittime. Di conseguenza, l'accesso al servizio non è possibile per gli utenti del sistema. Gli attacchi DoS possono durare da poche ore a molti mesi e possono costare alle aziende tempo e denaro mentre le loro risorse e servizi non sono disponibili [Investopedia]

ATTACCHI INFORMATICI

Modulo 1

Man-in-the-Middle: gli aggressori si inseriscono segretamente tra due parti, ad esempio un singolo utente di computer e un istituto finanziario. A seconda dei dettagli dell'attacco effettivo, questo tipo di attacco può essere classificato più specificamente come attacco man-in-the-browser, attacco monster-in-the-middle o attacco machine-in-the-middle. In questo caso, l'aggressore intercetta, cancella o modifica i dati mentre vengono trasmessi in rete da un computer, smartphone o qualsiasi altro dispositivo connesso [Investopedia, TechTarget]

Attività didattica #2 - Pratica

Discussione di gruppo: cosa caratterizza i messaggi di attacco/fraudolenti? (10-15 minuti)

- Ai partecipanti vengono concessi 10 minuti per annotare le caratteristiche
- Discussione sui risultati

Unità 3 - Esempi di minacce e attacchi

Come identificare una minaccia?

Attività didattica #3 - Teoria

Esempi di attacchi (relativi al conflitto russo-ucraino)

- E-mail fraudolente in inglese che chiedono sostegno a una delle parti in conflitto militare: Ucraina o Russia. Il supporto può essere mostrato acquistando voti e votando in questo modo: si tratta di una frode volta a rubare i dati delle carte di pagamento degli utenti (vedi schermata di stampa)

VIDEO – [How scammers are hijacking Ukraine war charity donations - BBC News](#)

ARTICOLO – [4 Types of Russia-Ukraine War Scams Targeting Consumers](#)

Esempi di attacchi frequenti registrati in Lettonia (2020-2021) e altri esempi

Malware

La situazione Covid-19 è stata utilizzata per diffondere tentativi di malware: ad es. e-mail a nome dell'Organizzazione Mondiale della Sanità (OMS), indicando che l'allegato include le ultime informazioni su Covid-19; collegamenti a grafici che mostrano la diffusione di Covid-19, la cui funzionalità era quella di rubare i dati degli utenti; e-mail dannose alle istituzioni sanitarie riguardanti la consegna di dispositivi di protezione Covid-19, ecc.

ATTACCHI INFORMATICI

Modulo 1

La diffusione del malware più pericoloso al mondo Emotet, sia su reti globali che lettoni, ha lo scopo di rubare informazioni sensibili e di solito ha origine da un'e-mail di un contatto già infetto. Emotet funge da apriporta per altri computer, consentendo l'accesso non autorizzato ad altre famiglie di malware. Più di 200 aziende lettoni sono state contagiate.

Phishing o truffe sui dati personali - La maggior parte dei casi riguardava la truffa di e-mail e dati di Office 365, l'acquisizione di dati bancari, sistemi di pagamento internazionali (incluso Smart-ID - strumento di autenticazione elettronica in Lettonia), dati di accesso e frode di dati di accesso ad account su popolari social media (Facebook e Instagram). L'argomento Covid-19 è stato spesso utilizzato per attirare l'attenzione degli utenti in e-mail fraudolente e annunci sui social media.

Durante la pandemia, sono stati osservati intensificati tentativi di frode di dati utilizzando i marchi dei fornitori di servizi di consegna pacchi (Latvijas Pasts, DHL, Omniva, DPD, AliExpress, ecc.) Inoltre, sono stati osservati attacchi innovativi, ad es. un attacco ai diritti di accesso a Office 365 difficile da rilevare con mezzi tecnici poiché non sono state eseguite azioni dannose sul dispositivo della vittima, ma gli attacchi sono stati effettuati all'interno di Office 365.

VIDEO  ng (sottotitoli in Inglese)

Frode - Intensi tentativi di frode, inclusi attacchi di social engineering. La maggior parte delle frodi era finalizzata ad ottenere dati di accesso alle carte di pagamento dei cittadini, risorse finanziarie, nonché dati di accesso alla posta elettronica. Gli aggressori hanno inviato e-mail e messaggi di testo fraudolenti alla popolazione, oltre a effettuare telefonate fraudolente, il più delle volte fingendosi rappresentanti di banche o fornitori di servizi di posta elettronica. Diverse aziende hanno subito interferenze commerciali (BEC), subendo una perdita totale di quasi 200.000 euro. La questione della consegna della merce è stata anche oggetto di tentativi di frode ai danni di venditori che hanno pubblicato informazioni sulla vendita di merci su portali pubblicitari. Fingendo di essere acquirenti interessati e utilizzando la piattaforma di comunicazione WhatsApp, i truffatori hanno espresso il desiderio di acquistare il prodotto, come se utilizzassero i servizi di un corriere, e hanno chiesto ai venditori di inserire i dettagli della carta sui siti Web contraffatti Omniva, DPD e successivamente Latvijas Pasts per rivelare entrambi il codice CVV e il saldo.

Gli aggressori hanno utilizzato indirizzi di siti Web personalizzati (domini) simili agli indirizzi dei siti Web originali per fuorviare il pubblico.

ATTACCHI INFORMATICI

Modulo 1

Gli aggressori hanno anche cercato di ottenere informazioni sulla carta di pagamento inviando e-mail chiedendo loro di richiedere un saldo in Bitcoin registrandosi a un servizio di scambio di criptovaluta fraudolento.

I tentativi più attivi sono stati le campagne estorsive, in cui gli hacker hanno affermato di aver violato il dispositivo di un utente e di aver ottenuto materiale compromettente per il quale è stato fissato un riscatto; lotterie fraudolente per conto di marchi noti, che offrono di vincere gli smartphone più recenti o altri premi di valore.

ALTRI ESEMPI

Pubblicità ingannevoli sui social media - utilizzando i nomi di famosi personaggi lettoni a loro insaputa, gli utenti di Internet sono stati invitati a investire in criptovaluta. I truffatori hanno anche fatto telefonate e cercato di convincere le persone a investire. In alcuni casi, sono stati osservati ripetuti tentativi fraudolenti in cui alle vittime di frodi finanziarie è stato offerto aiuto per recuperare le risorse perdute.

Truffe telefoniche - falsificando i numeri di telefono di diversi istituti di credito e fingendosi rappresentanti di banca, truffatori, sfruttando la scarsa conoscenza del pubblico su ulteriori metodi di autenticazione, defraudando risorse finanziarie a diverse migliaia di utenti, causando perdite complessive per centinaia di migliaia di euro a Istituti di credito lettoni.

Anche gli hacker si stanno adattando alla diffusione del lavoro da remoto: considerando la necessità delle aziende di passare rapidamente a una condizione di lavoro da remoto e l'implementazione della circolazione dei documenti elettronici, gli hacker sfruttano questa situazione per adattare i loro attacchi - ad es. alcuni contabili aziendali hanno ricevuto e-mail a nome del direttore o di un altro dipendente per effettuare un pagamento urgente o modificare il conto paghe.

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

ATTACCHI INFORMATICI

Modulo 1

Interferenza nella corrispondenza commerciale delle aziende - compromettendo le e-mail delle aziende o dei loro partner di collaborazione, gli aggressori scelgono il momento adatto per inviare a una delle parti una fattura con un account modificato.

Messaggi truffa - gli aggressori tentano di intercettare gli account di WhatsApp chiedendo di inviare per errore un codice di sei cifre al numero di telefono del destinatario. Quando verrà ricevuto un messaggio dalle persone nella tua lista di contatti, alcune persone trasferiranno i loro codici, perdendo l'accesso al proprio account WhatsApp. L'uso dell'autenticazione a due fattori sarebbe un mezzo di protezione contro un simile attacco.

ESEMPIO Condividere con l'hacker cifre sensibili ([vedi articolo](#))

ESEMPIO SMS dalla banca con link pericoloso ([example with SMS from SEB bank](#)).

Email truffa - i truffatori fingono di essere un ufficio postale nazionale (Latvijas Pasts) e chiedono alle persone di pagare per la consegna di una spedizione presumibilmente ritardata. Il collegamento fornito nell'e-mail conduce a un sito Web fasullo per dati di carte di pagamento fraudolente ([vedi print screen](#)).

ATTACCHI INFORMATICI

Modulo 1

Falsi negozi online - durante le festività natalizie è stata osservata un'attività particolarmente elevata per mezzo di pubblicità sui social media e a causa delle restrizioni del Covid-19 che hanno costretto le aziende a vendere i loro prodotti online.

ESEMPIO [Scammers lure AliExpress users to fake online stores; How to Recognize a Scam](#)

Truffa romantica - i truffatori approfittano delle persone in cerca di partner romantici, spesso tramite siti Web di incontri, app o social media fingendo di essere potenziali compagni. Giocano su trigger emotivi per farti fornire denaro, regali o dettagli personali.

ESEMPIO [Investigation story on Romance Scammer \[by North Lab\]](#)

Attacchi Denial of Service (DoS e DDoS) - Sono stati registrati attacchi DDoS contro istituzioni pubbliche e municipali (ad es. Biblioteca nazionale, Centro di sistemi informativi culturali, ecc.) Attacchi DDoS prolungati hanno interrotto una scuola. Segnalazioni simili sono pervenute da altre istituzioni educative all'inizio dell'anno scolastico. Anche le istituzioni educative di altre parti d'Europa si trovano ad affrontare tali sfide.

Sia in Europa che in Lettonia, sono diventati di attualità i seguenti incidenti: tentativi di estorsione di denaro rivolti principalmente a istituzioni finanziarie o società del settore privato (gli aggressori hanno eseguito una serie di attacchi di prova, minacciando di sospendere il funzionamento dei siti Web aziendali o di altre risorse mediante attacchi di fino a 2 Tbit/s).

ATTACCHI INFORMATICI

Modulo 1

ALTRI TREND

Dispositivi compromessi e fughe di dati - Le compromissioni delle apparecchiature possono interessare individui, aziende, nonché istituzioni statali e municipali. Ciò può avvenire attraverso e-mail già compromesse o l'infezione di un dispositivo tramite l'apertura di allegati o collegamenti da contatti apparentemente familiari, come colleghi e partner commerciali; può anche accadere attraverso siti Web compromessi, ad es. tramite un plugin obsoleto o un sistema di gestione dei contenuti obsoleto. Come è avvenuto nel 2020-2021, quando diverse istituzioni nazionali hanno perso temporaneamente l'accesso ai propri account sui social network quando gli aggressori hanno preso il controllo di uno dei profili degli amministratori degli account. Sono state presentate segnalazioni di irruzioni nelle riunioni di Zoom e MS Teams, a causa della scarsa conoscenza delle misure di sicurezza disponibili (ad esempio, sala d'attesa, accesso limitato dall'estero, ecc.).

Tentativi di intrusione (qualsiasi attacco che mira a compromettere gli obiettivi di sicurezza di un'organizzazione) - dopo l'aumento dell'attività di lavoro remoto dei bot alla ricerca di dispositivi vulnerabili, configurati in modo inadeguato e/o password deboli per dispositivi connessi a una rete (dispositivi rilasciati frettolosamente dal datore di lavoro, laptop personali che hanno iniziato a essere utilizzati per lavoro, nonché servizi RDP scarsamente protetti con password deboli) è aumentato in modo significativo.

VIDEO  "Intrusion Examples" e "Intrusion Detection"

FONTE CERT.LV and “Kiberlaikapstākļi” (Cyber Weather); Investopedia
- Additional elements

NOTE Considera anche discussioni su altri metodi su informazioni false e fraudolente, come deepfake e altri.

Attività didattica #3 - Pratica

Alla fine dell'unità viene organizzato un test Kahoot in cui i partecipanti devono rilevare se le informazioni fornite sono fraudolente e devono identificare il tipo (metodo) di minaccia informatica.

ATTACCHI INFORMATICI

Modulo 1


Unità 4 - Cosa fare in caso di incidente?

Prevenire e come prepararsi

Attività didattica #4 - Teoria

ALCUNI SUGGERIMENTI E TRUCCHI PER PROTEGGERSI

- Controlla sempre attentamente le tue e-mail e fai attenzione a: allegati o collegamenti incorporati da fonti o mittenti sconosciuti/sospetti; messaggi con un senso di urgenza che ti chiedono di scaricare qualcosa o eseguire qualche altra attività; offre con una promessa di ricompensa che sembra troppo bella per essere vera.

VIDEO  Clicker (Spaidonis) with subtitle in English

- Prestare attenzione all'ortografia dell'indirizzo URL. I siti di phishing utilizzano spesso indirizzi Web che sembrano simili a quelli di un sito ufficiale, ma contengono un semplice errore ortografico, come la sostituzione di "1" con una "l". Un'ortografia errata o strana è un segnale indicativo di una possibile truffa.

- Usa password complesse e diverse tra i tuoi dispositivi, account e-mail e account di social media. Per ulteriori suggerimenti, vedere il modulo CYBER.EU.VET sulle password (Modulo 4).

ATTACCHI INFORMATICI

Modulo 1

- Ove possibile, modifica le impostazioni per utilizzare l'autenticazione a più fattori sui tuoi dispositivi. Ad esempio, password e face ID o impronta digitale sul telefono; Gmail, nel frattempo, ha una di queste impostazioni, per cui quando un utente accede da un nuovo dispositivo, dopo aver inserito nome utente e password, riceve una richiesta di conferma della propria identificazione da un altro dispositivo, solitamente un telefono.

two-step verification in WhatsApp (for Android users).

- Non eseguire transazioni sensibili all'interno del Wi-Fi pubblico non protetto nei bar e in altri luoghi pubblici simili.

- Assicurati che almeno i dati più importanti sul tuo dispositivo abbiano una copia di backup (nel cloud storage o su un dispositivo esterno). Assicurati di poter ripristinare i dati necessari dai backup e scopri quanto tempo ci vuole.

- Aggiornamenti software: è fondamentale seguire gli aggiornamenti software e installarli immediatamente. Anche un solo giorno di ritardo può essere critico.

- Usa una VPN. Le reti private virtuali aggiungono un ulteriore livello di protezione all'utilizzo di Internet da casa. Non si può fare affidamento esclusivamente su di essi per prevenire gli attacchi informatici, ma possono essere un'utile barriera contro gli attacchi informatici.

- Segui regolarmente le notizie nel mondo degli attentati e prova a pensare che gli eventi globali, nazionali e locali, sia politici che economici, ma anche quelli legati alle sofferenze globali (pandemia, conflitti militari) possano essere usati come argomento/"copertura" per potenziali attacchi informatici.

- Ulteriori (in lettone): Raccomandazioni CERT.LV alla luce del peggioramento della situazione geopolitica e dell'aumento delle minacce informatiche in Europa:
<https://cert.lv/lv/2022/02/cert-lv-ieteikumi-saasinoties-geopolitiskajai-situacijai-eiropa-un-pieaugot-kiberdraudiem>

Dove segnalare una minaccia o un incidente informatico

- Il tuo posto di lavoro, istituto scolastico: invia screenshot, immagini o video alla persona interessata presso il tuo istituto (ad es. Dipartimento IT). Avvisa i tuoi colleghi e amici.

Istituzioni a supporto del cyber spazio nazionale (caso della Lettonia)

- CERT.LV (supporto nella risoluzione di incidenti, monitoraggio del cyberspazio, avvisi), istruzioni su come inoltrare e-mail fraudolente (in lettone)

Polizia di Stato

- Lettone Safer Internet Center (violazioni e contenuti illegali su Internet, sicurezza dei bambini su Internet) e altri

ATTACCHI INFORMATICI

Modulo 1

DOVE INFORMARSI

Per seguire le notizie sulla sicurezza informatica e le minacce informatiche, **leggi regolarmente le risorse locali o internazionali:**

<https://portswigger.net/daily-swig/cyber-attacks>

<https://www.euronews.com/tag/cyber-attack>

OUCH! Newsletters - la principale newsletter gratuita di sensibilizzazione sulla sicurezza informatica progettata per tutti.

Link per la Lettonia (alcune informazioni sono disponibili in Inglese):

<https://www.esidross.lv/>

<https://cert.lv/lv/> (contenente "Cyber Weather "(Kiberlaikapstākļi), instruction how to forward fraudulent e-mails (in Lettone)

<https://drossinternets.lv/>

Attività didattica #4 - Pratica

Discussione con i partecipanti: valutazione dell'utilità del modulo (5-10 min di attività)

2. Risultati di apprendimento del modulo

Conoscenze

- Conoscenza di base sui principali problemi degli attacchi informatici.
- Panoramica sugli incidenti reali (alla luce degli eventi globali).
- Fonti di informazioni da seguire per gli avvertimenti e l'attualità delle minacce.

Abilità

Gli studenti saranno in grado di identificare e classificare tipi comuni di minacce informatiche e di spiegarle.

Competenze

- Gli studenti saranno in grado di riconoscere una potenziale minaccia informatica e sapere dove segnalare la minaccia.
- Gli studenti saranno in grado di selezionare strumenti e tecniche di base per proteggersi dagli attacchi informatici.

3. Bibliografia

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.lv> LIKTA (Latvian Information and Communication Technologies Association): <https://likta.lv/digitalas-parmainas-izglitiba/>

Li, Y., Liu, Q (2021), A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments, Science Direct, Vol. 7, p. 8176-8186: <https://www.sciencedirect.com/science/article/pii/S2352484721007289>

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

Prat, M.K. (2021), Cyber-attack – definition:

<https://www.techtarget.com/searchsecurity/definition/cyber-attack>

Simplilearn, Cyber Security Full Course 2022: <https://youtu.be/yr1Psapupsc>

CERT.LV (2022), IT drošības seminārs "Esi drošs" martā (in Latvian):

https://cert.lv/lv/2022/02/it-drosibas-seminars-esi-dross-marta#Sanita_Vitola

Esi Drošs (2022), Kiberuzbrukuma riskam pakļauts ikviens interneta lietotājs (in Latvian):

<https://www.esidross.lv/2022/02/10/kiberuzbrukuma-riskam-paklauts-ikviens-interneta-lietotajs/>

CYBERBULLISMO

Effetti, conseguenze e prevenzione

Modulo 2

1. Presentazione del modulo

Gruppi Target

Educatori del settore professionale della formazione

Studenti

Rappresentanti di istituzioni pubbliche attive nei settori educativi: comuni, autorità regionali e nazionali;

Descrizione del modulo

Al giorno d'oggi, le persone trascorrono molto del loro tempo davanti a uno schermo. I giovani stanno crescendo in un mondo in cui le nuove tecnologie sono necessarie e il principale mezzo di comunicazione che utilizzano è Internet. Stare sui social media, ad esempio, offre molti vantaggi, ma anche molti rischi.. Ci sono molte persone che sono state vittime di bullismo o sono vittime di bullismo. Nella maggior parte dei casi, non erano consapevoli di questo o dei problemi che può causare nelle loro vite. Per questo motivo, vorremmo utilizzare questo modulo, per capire cos'è il cyberbullismo e come possiamo prevenirlo.

Obiettivi formativi

- Comprensione del cyberbullismo
- Sapere come rilevarlo
- Effetti del cyberbullismo
 - Comprendere le principali conseguenze
 - Fornire tecniche per prevenirlo e affrontarlo

Durata complessiva

2 ore

CYBERBULLISMO

Effetti, conseguenze e prevenzione

Modulo 2

Unità 1 - Come rilevare il cyberbullismo

Quali sono gli effetti?

Questa unità sarà consegnata dal formatore come una presentazione PowerPoint il cui scopo è condividere le conoscenze teoriche accompagnate da più elementi visivi - brevi video e casi reali di cyberbullismo che riassumono le informazioni dalle diapositive PowerPoint (max. 30 minuti). Si consiglia di preparare le presentazioni sui modelli PPT personalizzati per il progetto CYBER.EU.VET.

Attività didattica #1

Il formatore presenta agli studenti una presentazione con i seguenti contenuti suggeriti (massimo 30 minuti):

Il cyberbullismo, sebbene spesso associato al cyberstalking, è di per sé un problema molto serio e la cui prevalenza è aumentata negli ultimi anni.

Come rilevare il cyberbullismo?

Il cyberbullismo può essere **difficile da riconoscere** perché avviene a porte chiuse o in un telefono/computer privato.

Ecco alcuni dei segnali più comuni che indicano che qualcuno potrebbe essere vittima di cyberbullismo:

- Si arrabbia insolitamente se non può usare il computer o il telefono o dopo aver usato il computer.

- Cambia rapidamente schermata o chiude i programmi quando passa qualcuno.

- Evita discussioni su ciò che stanno facendo al computer.

- Ritiro da familiari o amici.

- Riluttanza a partecipare ad attività che prima gli piacevano.

- **Inspiegabile calo del rendimento scolastico.**
Gli effetti del cyberbullismo possono essere devastanti per le vittime. Possono provare varie emozioni negative, come tristezza, rabbia, frustrazione e umiliazione. Possono anche rifiutare di andare a scuola, sentirsi isolati e soli, come se non avessero nessuno a cui rivolgersi.

- Segnala sempre più sintomi di malattia.

CYBERBULLISMO

Effetti, conseguenze e prevenzione

Modulo 2

Le vittime possono anche soffrire accademicamente, poiché potrebbero essere troppo imbarazzate per andare a scuola o partecipare alle lezioni. In alcuni casi, le vittime possono anche prendere in considerazione il suicidio.

Il cyberbullismo può anche avere effetti negativi su coloro che ne sono testimoni mentre accade a qualcun altro. Possono sentirsi spaventati, impotenti e tristi. Possono anche avere difficoltà a dormire e mangiare e possono persino sviluppare ansia e depressione.

Effetti e conseguenze del cyberbullismo:

Quando il bullismo avviene online, può sembrare di essere attaccato ovunque, anche a casa tua. Può sembrare che non ci sia scampo. Gli effetti possono durare a lungo e influenzare una persona in molti modi:

- **Psicologicamente:** sentirsi turbati, imbarazzati, stupidi, persino impauriti o arrabbiati
- **Emotivamente:** provare vergogna o perdere interesse per le cose che ami
- **Fisicamente:** sensazione di stanchezza (per la mancanza di sonno) o sintomi come mal di stomaco e mal di testa

La sensazione di essere derisi o molestati dagli altri può impedire alle persone di parlare apertamente o di cercare di affrontare il problema. In casi estremi, il cyberbullismo può persino portare le persone a togliersi la vita.

[VIDEO Watch Hurt | Cyberbully Short Film](#)

Effetti:

- Malattia
- Depressione
- Isolamento

Attività didattica #2

Rabbia

Discussione di gruppo – Domande e risposte; Valutazione e Feedback (max. 10 minuti)
Umiliazione
Ora che conosci i segni più comuni di qualcuno vittima di cyberbullismo,

- Conosci qualcuno in questa situazione?
- Potresti aiutarli?

CYBERBULLISMO

Effetti, conseguenze e prevenzione

Modulo 2

Unità 2 - Come prevenire e contrastare il cyberbullismo

Attività didattica #1

il formatore presenta agli studenti una presentazione con i seguenti contenuti suggeriti (massimo 30 minuti):

Il cyberbullismo è facilitato dal facile accesso a piattaforme e dispositivi multimediali digitali. Spesso, questi vengono utilizzati senza alcuna supervisione. Questo rende il cyberbullismo un problema incredibilmente difficile da affrontare. Prevenire la pratica richiederebbe una grande quantità di tempo e risorse per monitorare efficacemente ogni interazione online. Sebbene spesso non sia possibile per le persone liberarsi completamente degli strumenti digitali, ci sono metodi che genitori, studenti ed educatori possono utilizzare per combattere il fenomeno e ridurre gli effetti dannosi.

Per i genitori, un modo efficace per affrontare il danno derivante dal cyberbullismo è semplicemente parlare del problema con i propri figli.

È anche importante discutere della sicurezza online, della privacy e della gestione delle password. Stabilisci linee guida su come gli studenti devono comportarsi online e istruisci i giovani ad essere aperti con i loro genitori su qualsiasi danno che hanno subito a causa del bullismo online o nel mondo reale.

I giovani possono aiutare a evitare di essere vittime di cyberbullismo prestando attenzione a ciò che pubblicano. Dovrebbero evitare di condividere le loro password e assicurarsi che le loro impostazioni sulla privacy online li proteggano.

Gli studenti svolgono un ruolo importante nella prevenzione del cyberbullismo. Se i giovani che conoscono i fatti di cyberbullismo si accorgono che sta accadendo a qualcun altro, possono avvisare un adulto di fiducia. Dovrebbero anche essere gentili, generosi e solidali con il bambino vittima di bullismo. Insegnanti, educatori e altri adulti fidati devono unirsi a genitori e giovani per combattere il cyberbullismo. Spesso queste persone possono individuare i cambiamenti nel comportamento di un bambino e possono aiutare a risolvere il problema prima che possano farlo i genitori.

La tecnologia e Internet non sono il problema. Sono le persone che lo usano per danneggiare gli altri il vero problema. Per questo, è importante insegnare agli adolescenti come utilizzare i social media in modo sicuro e responsabile e diventare consapevoli di come agire, qualora subissero il cyberbullismo.

CYBERBULLISMO

Effetti, conseguenze e prevenzione

Modulo 2

Cosa fare se sei vittima di cyberbullismo?

- NON RISPONDERE o commentare il messaggio del cyberbullo.
- BLOCCARE le persone coinvolte.
- DISCONNETTERTI dal sito in cui si sta verificando il bullismo.
- Proteggi le tue PASSWORD e controlla i tuoi CONTROLLI SULLA PRIVACY.
- SALVA tutto. Fai uno screenshot o stampa l'incidente come prova.

Cosa dovresti fare se vedi che si sta verificando un cyberbullismo?

- **SEGNALA** il cyberbullismo, quasi tutti i siti di tecnologia hanno un'opzione per segnalare qualcuno per cyberbullismo.
- Dillo al tuo genitore o un adulto di cui ti fidi e chiedi consiglio.

Se la situazione al fornitore di tecnologia, app o social media.
Se un altro è stato coinvolto, contatta le forze dell'ordine.

Se la situazione coinvolge compagni di classe, informa i tuoi insegnanti.

▪ **Intraprendere un'azione legale:** sia la calunnia che la diffamazione sono reati che possono sfociare in un processo. Mostra il tuo sostegno alla persona vittima di bullismo, ad esempio rivolgendole un messaggio gentile.

▪ **Chiedere aiuto:** è molto difficile affrontare il cyberbullismo da soli!

VIDEO  [s Story: Cyberbullied by a Best Friend](#)

Come posso informarmi?

▪ Organizzazioni che possono aiutare: ci sono molte organizzazioni là fuori che condividono informazioni sul cyberbullismo. I siti Web seguenti stanno creando e condividendo contenuti utili che sono veramente utili per chiunque sia preoccupato o subisca il cyberbullismo.

▪ Blog e podcast: tenere il passo con blog e podcast incentrati sull'argomento è un ottimo modo per rimanere aggiornati e ricevere gli ultimi consigli o punti di vista.

▪ App e software: sono disponibili numerosi prodotti che consentono ai genitori di limitare e/o monitorare l'attività online dei propri figli. Spetta a ciascun genitore decidere se questo tipo di monitoraggio è appropriato in base all'età e alle abitudini di Internet del proprio figlio. Alcuni cercano persino un linguaggio che potrebbe essere prepotente. Ci sono anche aziende che collaborano con le scuole per consentire la segnalazione anonima di episodi di bullismo.

CYBERBULLISMO

Effetti, conseguenze e prevenzione

Modulo 2

Attività didattica #2

Discussione di gruppo – Domande e risposte; Valutazione e Feedback (max. 15 minuti)

Esercizio di scrittura:

Descrivi una situazione in cui sai che è in corso un cyberbullismo.

Questo può essere reale o fittizio.

Puoi aiutare? Come? Perché o perché no? Spiega come ti fa sentire.

2. Risultati formativi del modulo

Conoscenze

- Lo studente saprà come rilevare il cyberbullismo e come la vittima lo sente e lo vive.

-

Comprendere i fatti sul cyberbullismo ed essere consapevoli dei metodi per affrontarlo, giovani, adulti ed educatori può aiutare a creare un mondo digitale migliore e più empatico.

Capacità

- Lo studente capirà come riconoscere quando qualcuno è vittima di cyberbullismo.

-

Lo studente sarà in grado di capire quale livello di risposta e supporto è necessario a seconda dello scenario in questione.

Competenze

- Lo studente sarà in grado di riconoscere un episodio di cyberbullismo e affrontarlo immediatamente utilizzando gli strumenti adeguati.

- Lo studente sarà in grado di identificare quale sia il miglior metodo di supporto e quale sia il più adatto al caso in questione.

3. Bibliografia

<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/>

PREVENIRE IL CYBERBULLISMO

Modulo 3

1. Presentazione del modulo

Gruppi Target

Educatori del settore professionale della formazione

Studenti

Rappresentanti di istituzioni pubbliche attive nei settori educativi: comuni, autorità regionali e nazionali;

Descrizione del modulo

Questo è un modulo di follow-up di "Cyberbullismo. Cos'è? Come possiamo rilevarlo?" e fornisce ai gruppi target le competenze per diffondere la consapevolezza del cyberbullismo e per fornire tecniche di prevenzione in modo da non diventare vittime del cyberbullismo.

Obiettivi formativi

- Comprendere l'importanza della prevenzione
- Diffondere la consapevolezza sul cyberbullying
- Aumentare la consapevolezza sulle tecniche di prevenzione del cyberbullying

Durata Complessiva

1,5 ore

PREVENIRE IL CYBERBULLISMO

Modulo 3

Unit 1 - Perché prevenire il Cyberbullismo?

Questa unità sarà fornita dall'educatore come una presentazione di PowerPoint che includerà sia materiale teorico e più caratteristiche visive come brevi film e scenari di cyberbullismo nella vita reale che riassumeranno le informazioni dalle diapositive di PowerPoint (da 20 a 30 minuti rispettivamente su ciascuna unità).

Si consiglia di preparare presentazioni sui modelli PPT personalizzati per il progetto CYBER.EU.VET. La presentazione è seguita da una discussione di gruppo, per tutti per riflettere sull'apprendimento.

Attività didattica #1

Il formatore presenta agli studenti una presentazione con il seguente contenuto suggerito (max. 20 minuti):

Prevenire o Intervenire?

Secondo la ricerca, le persone che sono vittime di cyberbullismo hanno una varietà di risultati negativi, tra cui difficoltà emotive, fisiche, mentali e accademiche. Inoltre, il cyberbullismo è una fonte significativa di stress per i giovani. Le vittime sono ferite psicologicamente, vergognose e talvolta spaventate a causa del cyberbullismo. Non solo si incolpano per le molestie e gli abusi che subiscono, ma si sentono anche tremendamente ansiosi. Infatti, oltre il 35% degli individui presi di mira da cyberbullies esibito sintomi di stress, secondo una ricerca. Questo tipo di bullismo può essere particolarmente dannoso in quanto è spesso molto pubblico. Di solito, molte persone possono vedere ciò che è scritto o pubblicato. È difficile, se non impossibile, cancellare tutte le tracce di qualcosa una volta che è stato pubblicato online. Ciò significa che il bullismo può essere in corso.

Quando le persone sono molestate da altri sui social media, tramite messaggi di testo, chat istantanea e post sul blog su base frequente, possono iniziare a sentirsi senza speranza. Possono sentire che il suicidio è l'unico modo per fermare la loro sofferenza. Poiché i pericoli del cyberbullismo sono così gravi, è fondamentale che gli educatori VET insegnino loro ss[AB1] di questo problema prima che causi danni reali. Ottenere prevenzione riduce i rischi di essere esposti al cyberbullismo

PREVENIRE IL CYBERBULLISMO

Modulo 3

Attività didattica #2

Discussione di Gruppo (max. 10 minuti)

Chiedete ai vostri studenti:

- Perché la prevenzione è così importante nel cyberbullying?
-

Sei mai stato informato sul cyberbullying?

Di solito come vieni informato sui reati di cyberbullying?

Unità 2 - Diffondere Consapevolezza

Attività didattica #1

Il Trainer offre una presentazione agli studenti con i seguenti contenuti suggeriti (max. 30 minuti): è fondamentale discutere con gli studenti su come utilizzare i social media in modo sicuro e responsabile, individuando i criminali del cyberbullismo e imparando cosa fare se sono vittime di bullismo online.

VIDEO  [Bullying - How to Avoid Cyber Abuse](#)

PENSA PRIMA DI POSTARE - Gli studenti dovrebbero prendere l'abitudine di leggere attraverso il loro lavoro prima di pubblicarlo. Possono digitare il post nella sezione note del loro computer o smartphone e poi rivisitarlo poche ore dopo per decidere se pubblicarlo o meno. Perché i cyberbulli potrebbero usare ciò che pubblichi contro di te in qualche modo, sarai meno incline a dire qualsiasi cosa rimpiangerai in seguito o che potrebbe essere usata contro di te. Certo, se qualcuno vuole usare qualcosa contro di te, si sforzerà di ottenere anche le informazioni più insignificanti, ma il controllo prima della condivisione può ridurre la gravità dell'attacco informatico. Pensare prima di pubblicare potrebbe aiutare a mantenere un rapporto sano con i social media.

FAI ATTENZIONE AI DISPOSITIVI PUBBLICI - Gli studenti dovrebbero anche fare attenzione quando si utilizzano dispositivi pubblici come i computer dell'università o della biblioteca siccome ci sono molti modi in qualcuno potrebbe approfittare di questo.

Ci sono molte possibilità per i dispositivi pubblici di essere infettati da programmi dannosi, come i registratori di tasti (keylogger).

PREVENIRE IL CYBERBULLISMO

Modulo 3

Un keylogger, secondo la maggior parte delle fonti, è un'applicazione software che controlla e registra in modo discreto tutte le battiture. Possono essere utilizzati per intercettare le password e altri dati personali immessi tramite la tastiera, ponendo una grave minaccia per gli utenti, come ad esempio la consegna di accesso ai tuoi account di social media per i criminali informatici. La cosa più importante da sapere quando si tratta di keylogger è che spesso non possono essere rilevati dai programmi anti-virus, poiché ci sono molti keylogger legittimi disponibili sul mercato ai fini del controllo parentale, della sicurezza aziendale, ecc.

VIDEO [a Keylogger Be Spying on You?](#)

Oltre ai programmi di monitoraggio specializzati, gli studenti dovrebbero anche essere invitati a disconnettersi dai loro account in quanto potrebbero involontariamente lasciarli aperti e disponibili per coloro che utilizzeranno i computer accanto a lui.

PROTEZIONE ONLINE

È fondamentale utilizzare password forti ovunque quando si tratta di combattere il cyberbullismo e altre attività fraudolente. Una password forte è quella che non può essere facilmente indovinata o compromessa. Una password forte dovrebbe essere lunga, contenere una combinazione di numeri, caratteri speciali e lettere maiuscole/ minuscole e non dovrebbe in nessun caso includere informazioni evidenti come nome, data di nascita, ecc. Salvaguardando i tuoi account, ti assicuri che nessuno possa accedervi.

CYBERBULLYING DOVREBBE ESSERE DENUNCIATO.

Assicurati che i tuoi studenti comprendano l'importanza di segnalare il cyberbullismo. Ciò comporta non solo il rilevamento di cyberbulli, ma anche l'informazione della piattaforma di social media, del fornitore di servizi Internet e di altre parti pertinenti. Per porre fine alle molestie, potrebbero anche aver bisogno di informare le autorità locali.

Dopo aver archiviato tutti i documenti necessari, gli studenti devono intraprendere le azioni necessarie per bloccare l'individuo o l'account responsabile del cyberbullismo. Dovrebbero anche essere consapevoli che, anche dopo aver bloccato l'autore del reato, potrebbero creare account alternativi per avvicinarsi alla vittima. La buona notizia per quanto riguarda il bullismo online che si verifica online è che in genere può essere registrato, conservato e presentato a qualcuno che può aiutare. Le vittime dovrebbero tenere quella prova in caso le cose sfuggissero di mano.

VIDEO: IGNORE OR REPORT A CYBER BULLY



PREVENIRE IL CYBERBULLISMO

Modulo 3

Attività didattica #2

Presenta agli studenti il seguente caso di studio:

[YouProMe Erasmus+ project – www.youpromeproject.eu](http://www.youpromeproject.eu)

Jessica ha 18 anni. Vive con i suoi due genitori, entrambi professionisti e sempre impegnati a lavorare. Jessica è la più grande di tre figli. Non c'è nessuno in famiglia con problemi di salute noti. Studia a scuola ed è una studentessa laboriosa. È appassionata di animali e le piace uscire con i suoi amici. Ha un ragazzo. Jessica ha un telefono cellulare ed è un utente regolare dei social network.

Jessica ha riferito: "Ho inviato il mio ragazzo alcune foto un paio di settimane fa. Pensavo fosse comunque il mio ragazzo, ma poi li ha mostrati al suo amico e il suo amico li ha mandati a tutti. La scuola ha scoperto e ora la polizia ha parlato con lui e il suo amico. Non sono più tornato a scuola da allora, ma tutti mi chiamano sguardina sui social media. Non sopporto quando mi fissano, e so già cosa pensano. Anche le ragazze hanno un'opinione simile su di me. La cosa stupida è che tutti lo fanno, tutti mandano foto, ma sono stato sfortunato ad avere un ragazzo che mi ha tradito. Non mi fiderò mai più di nessuno. Sento che tutto è finito e non c'è modo di tornare indietro."

Di conseguenza, Jessica è stata assente da scuola per un mese e si rifiuta di tornare. Ha abbandonato tutte le sue attività sportive scolastiche. Sua madre ha parlato con l'operatore sportivo e ha detto che è preoccupata per alcune delle cose "oscure" che Jessica ha detto. Jessica è desiderosa di cambiare la sua presenza online e ritrovare la fiducia iniziale. Jessica e la sua famiglia non sono a conoscenza di quale sostegno è disponibile e come sostenere al meglio la sua salute mentale o qualsiasi conoscenza di come un operatore giovanile può mediare in questa situazione. Jessica ha capito il rischio di abusare di internet e riconosce che ha bisogno di sostegno per gestire la sua salute mentale in quanto questo ha influenzato il suo processo decisionale.

Ora potete iniziare una conversazione basata su queste domande (max. 30 minuti):

- Quali rischi sono presenti qui?
- Quali servizi dovresti coinvolgere?
- Che linea d'azione suggerisci a Jessica e sua madre?

PREVENIRE IL CYBERBULLISMO

Modulo 3

2. Risultati formativi del modulo

Conoscenze

- Lo studente comprenderà l'importanza del prevenire il cyberbullying

- Lo studente saprà che tipo di tecniche sono disponibili per evitare di essere vittima di cyberbulli

Capacità

- Lo studente sarà in grado di diffondere la consapevolezza della prevenzione del cyberbullismo

- Lo studente sarà in grado di insegnare importanti tecniche di prevenzione ai loro studenti

Competenze

- Lo studente sarà in grado di implementare eventi di sensibilizzazione efficaci di diffusione contro il cyberbullismo

- A seconda della situazione, lo studente sarà in grado di determinare quale tipo di assistenza è necessaria.

3. Bibliografia

<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/>

AUTENTICAZIONE E PASSWORD

Modulo 4

1. Presentazione del modulo

Gruppi Target

▪ Educatori del settore professionale della formazione

▪ Studenti

▪ Rappresentanti di istituzioni pubbliche attive nei settori educativi: comuni, autorità regionali e nazionali;

Descrizione del modulo

I professionisti VET e i loro studenti affrontano quotidianamente diverse minacce alla sicurezza informatica. Sebbene ci siano vari materiali educativi sulla sicurezza informatica disponibili online, non sono tutti aggiornati fino ad oggi o sono percepiti dagli studenti come troppo semplici o troppo complessi.

Il contenuto educativo di questo modulo fornirà agli studenti competenze e conoscenze per migliorare la loro comprensione dell'autenticazione e delle password, al fine di rafforzare la loro capacità di formazione, ma anche per migliorare le loro competenze in modo da evitare attacchi di sicurezza informatica. Educatori VET meglio attrezzati saranno in grado di supportare ulteriormente i loro studenti nel riconoscere le minacce quotidiane evitandole.

Obiettivi formativi

▪ Migliorare la comprensione dell'autenticazione nella sicurezza informatica

▪

▪ Migliorare la comprensione dei diversi metodi di autenticazione

▪

▪ Migliorare la comprensione delle caratteristiche principali dei metodi di autenticazione più comuni

▪ Comprendere i rischi di non utilizzare password complesse

Durata Complessiva

2 ore
Fornire tecniche per gestire facilmente password complesse

AUTENTICAZIONE E PASSWORD

Modulo 4

Unità 1 - Autenticazione

Questa unità sarà fornita dal trainer come una presentazione di PowerPoint condividendo le conoscenze teoriche accompagnate da più elementi visivi - brevi video che riassumono le informazioni dalle diapositive di PowerPoint (max. 20 minuti).

Si consiglia di preparare le presentazioni sui modelli PPT personalizzati per il progetto CYBER.EU.VET. Considerando i rapidi sviluppi e progressi nel campo della Cybersecurity, si raccomanda di rivedere continuamente le unità e, se necessario, modificare il contenuto considerando i più recenti sviluppi nel campo.

La presentazione è seguita da una discussione di gruppo di 10 minuti al fine di riflettere sul processo di apprendimento e valutare il livello di comprensione degli studenti dell'argomento, creando allo stesso tempo spazio ulteriori domande e feedback.

Attività didattica #1

Il formatore fornisce una presentazione con i seguenti contenuti suggeriti (max. 20 minuti):

Cos'è l'autenticazione? Il processo di autenticazione nel contesto dei sistemi informatici significa la garanzia e la conferma dell'identità di un utente. Prima che un utente tenti di accedere alle informazioni memorizzate in una rete, deve dimostrare la propria identità e il permesso di accedere ai dati. Quando si accede a una rete, un utente deve fornire informazioni di accesso univoche, tra cui un nome utente e una password, una pratica progettata per proteggere una rete da infiltrazioni da parte di hacker. L'autenticazione si è ulteriormente ampliata negli ultimi anni per richiedere più informazioni personali dell'utente, ad esempio la biometria, per garantire la sicurezza dell'account e della rete da parte di coloro che hanno le competenze tecniche per sfruttare le vulnerabilità.

VIDEO:  [IS AUTHENTICATION?](#)

Perché l'Autenticazione è importante? L'autenticazione è un passo cruciale per mantenere i dati degli utenti al sicuro e per prevenire e bloccare qualsiasi accesso non autorizzato ai dati online. Se l'autenticazione non è sicura, il sistema può essere facilmente attaccato e violato e i criminali informatici possono accedere ai dati e alle informazioni archiviate nel sistema.

AUTENTICAZIONE E PASSWORD

Modulo 4

è molto importante evitare che ciò accada e assicurarsi che gli utenti siano a conoscenza di diversi metodi di autenticazione gratuiti o a pagamento per impedire qualsiasi accesso non autorizzato ai propri dati personali o professionali. Per le organizzazioni e le aziende, si consiglia di investire in strumenti di autenticazione di alta qualità al fine di proteggere i loro dati online da eventuali potenziali violazioni.

VIDEO:  [CYBERSECURITY TIP - AUTHENTICATION](#)

Metodi di autenticazione con password comuni

Considerando la natura in continua evoluzione di diversi tipi di minacce informatiche e attacchi, c'è stata una vasta gamma di diversi metodi di autenticazione sviluppati negli ultimi anni.

Alcuni dei metodi di autenticazione più comuni sono:

1. Standard Password Authentication
2. Two-Factor Authentication
3. Token Authentication
4. Biometric Authentication
5. Computer Recognition Authentication
6. CAPTCHAS

1. STANDARD PASSWORD AUTHENTICATION

▪ La forma di autenticazione più semplice e più utilizzata:

▪ Richiede l'inserimento di un nome utente, accompagnato da un codice segreto o una password che consente l'accesso a una rete, un account o un'applicazione.

Per ridurre il rischio di compromettere una password, gli utenti dovrebbero scegliere una password complessa. Un gestore di password o un software sicuro può aiutare a prevenire qualsiasi accesso non autorizzato ai dati memorizzati online.

2. TWO-FACTOR AUTHENTICATION (2FA)

▪ L'autenticazione a due fattori richiede agli utenti di autenticarsi tramite qualcosa "sanno" e qualcosa "hanno". Una password serve come "qualcosa che sanno," e un oggetto fisico specifico come uno smartphone che serve come "qualcosa che hanno."

▪ L'autenticazione a due fattori di solito richiede all'utente di inserire il proprio nome utente, una password e un codice una tantum inviato a un dispositivo fisico (telefono cellulare, lettore di schede, ecc.)

AUTENTICAZIONE E PASSWORD

Modulo 4

3. AUTENTICAZIONE DI TOKEN

- I sistemi di token utilizzano un dispositivo fisico appositamente costruito per fornire l'autenticazione a due fattori, ed è consigliabile se si preferisce non fare affidamento sui telefoni cellulari.

- Questo potrebbe essere un dongle inserito nella porta USB del dispositivo, o forse una smart card con identificazione a radiofrequenza o chip di comunicazione vicino al campo.

- Per mantenere un sistema di token sicuro, è fondamentale assicurarsi che il dispositivo di autenticazione fisica (ad esempio, dongle o smart card) non cada nelle mani sbagliate.

4. AUTENTICAZIONE BIOMETRICA - L'autenticazione biometrica si basa sulle caratteristiche fisiche di un utente per identificarle. L'autenticazione biometrica potrebbe fare uso di impronte digitali, scansioni della retina o dell'iride, o riconoscimento facciale e vocale. Questa è una forma di autenticazione altamente sicura perché non ci sono due individui che abbiano le stesse caratteristiche fisiche. L'autenticazione biometrica è un modo efficace per sapere esattamente chi sta accedendo al sistema.

5. RICONOSCIMENTO DEL COMPUTER - Il riconoscimento del computer è un metodo di autenticazione delle password che verifica la legittimità di un utente controllando che si trovi su un particolare dispositivo. Questi sistemi installano un piccolo plug-in software sul dispositivo dell'utente la prima volta che accede con successo. Questo plug-in contiene un marcatore di dispositivo crittografico. Quando l'utente successivo accede, il marcatore viene controllato per assicurarsi che siano sullo stesso dispositivo trusted.

- Questo sistema è invisibile per l'utente e non richiede ulteriori azioni di autenticazione da loro. Essi semplicemente inseriscono il loro nome utente e la password come al solito, e la verifica avviene automaticamente.

- Per mantenere un elevato livello di sicurezza, i sistemi di autenticazione del riconoscimento informatico devono abilitare l'accesso da nuovi dispositivi utilizzando altre forme di verifica (ovvero l'autenticazione a due fattori con un codice fornito tramite SMS).

6. CAPTCHAS - I CAPTCHA non si concentrano sulla verifica di un particolare utente, in contrasto con gli altri metodi elencati in questo articolo fanno. Invece, i CAPTCHA mirano a determinare se un utente è umano, prevenire tentativi di computer-driven per entrare in conti (es. attacchi di forza bruta). Il sistema CAPTCHA visualizza un'immagine distorta di lettere e numeri, o immagini, e chiede all'utente di digitare ciò che vede. Poiché i computer e i bot faticano a identificare correttamente queste distorsioni, i CAPTCHA migliorano la sicurezza creando un'ulteriore barriera ai sistemi di hacking automatizzati.

AUTENTICAZIONE E PASSWORD

Modulo 4

Attività didattica #2

Discussione di Gruppo – Q&A, Valutazione e Feedback (max. 10 minuti)

Domande consigliate per la Valutazione:

- Cos'è l'autenticazione?
- Perché l'autenticazione è importante?
- Quali sono i metodi di autenticazione più comuni attualmente in uso e quali sono le loro caratteristiche principali?

Unità 2 - Password

Attività didattica #2

1. COSE CHE NON DOVRESTI FARE

Slides con immagini che esemplificano cose che le persone non dovrebbero fare, al fine di coinvolgere il pubblico

CASI STUDIO

- “The Belgian Police have posted it with the WiFi password on. This was shown on national TV” - https://www.reddit.com/r/cybersecurity/comments/cnkhft/the_belgian_police_have_a_post_it_with_the_wifi/
- “A password for the Hawaii emergency agency was hiding in a public photo, written on a Post-it note” - <https://www.businessinsider.com/hawaii-emergency-agency-password-discovered-in-photo-sparks-security-criticism-2018-1>
- “Four embarrassing password leaks on live TV” - <https://www.itgovernance.co.uk/blog/four-embarrassing-password-leaks-on-live-tv>

2. STATISTICHE

Presentazione di alcune statistiche:

- 81% of Data Breaches happen due to poor password security
- Bad employee password habits
- Top 200 most common passwords

AUTENTICAZIONE E PASSWORD

Modulo 4

3. L' IMPORTANZA DI UNA PASSWORD SICURA

The anatomy of an unhackable password

4. REGOLE BASE

Descrivere un set di regole base come:

- Evitare di utilizzare i gestori di password del browser; è un modo semplice per un "malware" per accedere a loro.
- Non condividere la tua password.
- Memorizza le password, non registrarle su carta o digitalmente. Memorizza le password regolarmente (almeno ogni due mesi)
- Se possibile, abilitare l'autenticazione a due fattori
- Ogni password deve essere usata su una sola piattaforma
- Modificare la password originale al momento dell'acquisto di un dispositivo
- Non usare parole comuni. Uno dei tipi di attacco più frequenti è via "dizionario"

Regole per una password più sicura:

- Crea password complesse: almeno 12 caratteri, con caratteri maiuscoli e minuscoli, con

Memorizzarle invece di registrarle:

- Non usare termini facilmente 'rilevabili' che tipicamente includono: nome, città di nascita, o termini conosciuti, nome dell'animale, numero di registrazione dell'auto; numero di cellulare, compleanni del membro della famiglia, ecc.
- Usa un detto, espressioni comuni o qualcosa di facile da memorizzare

Ad esempio, usare le prime due lettere di ogni parola

Attività didattica #2

Passare da maiuscolo, minuscolo e simboli

Esercizio di gruppo

Testa la lunghezza della tua password - <https://www.passwordmonster.com>

Sono già stato craccato? - <https://haveibeenpwned.com/Passwords>

Discussione e Feedback (max. 10 minuti)

AUTENTICAZIONE E PASSWORD

Modulo 4

Domande consigliate per la valutazione:

- Quanti anni la tua password resiste a una normale macchina algoritmo di crack?

▪ Dovrei cambiare la mia password?

Attività didattica #3

Il trainer presenta agli studenti una presentazione con i seguenti contenuti suggeriti (max. 20 minuti):

Cosa sono i gestori di password?

▪ Casseforti digitali

- Consentono di memorizzare credenziali e note di vari servizi
- Le coordinate bancarie possono anche essere salvaguardate

▪ Una sola chiave master

L'autenticazione Biometrica può essere usata

Gestori di password locali

▪ Salva i dati sul dispositivo corrente

- Il file della password è crittografato
- Ogni password deve essere salvata in un file crittografato separato
- Può essere utilizzato solo su un singolo dispositivo

Esempio come KeypassXC

Gestori di password online

▪ I dati vengono memorizzati nel cloud

Attività didattica #4

Consentono l'accesso a credenziali e note di vari servizi su qualsiasi dispositivo

Gruppi hands-on

▪ Create una complessa password

▪ Nessuna installazione richiesta

- Installate un Password Manager per computer o smartphone

▪ Attivate MFA

Una sola chiave master

- I dati vengono crittografati dal dispositivo al server

AUTENTICAZIONE E PASSWORD

Modulo 4

Discussione e Feedback (max. 10 minuti)

Domande Consigliate per la valutazione:

Quanto è stato difficile ?

- Utilizzerai queste buone pratiche?

2. Risultati formativi del modulo

Conoscenze

- Comprendere la definizione di autenticazione, la sua importanza, e alcuni dei metodi di autenticazione più comuni
- Comprendere i rischi di non utilizzare password complesse
- Utilizzare le migliori pratiche nella gestione delle password personali

Capacità

- Identificare e applicare il metodo di autenticazione più adeguato e appropriato
- Identificare e applicare la complessità della password più adeguata e appropriata

Competenze

- Percepire l'importanza dell'autenticazione
- Decidere il metodo di autorizzazione più appropriato per le diverse attività online e applicarle per migliorare la sicurezza online
- Percepire l'importanza di usare password complesse
- Strutturare le tecniche di buone pratiche per gestire la password personale

3. Bibliografia

<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>

UTILIZZO DEL WI-FI

SICURO

Modulo 5

1. Presentazione del modulo

Gruppi Target

▪ Educatori del settore professionale della formazione

▪ Studenti

▪ Rappresentanti di istituzioni pubbliche attive nei settori educativi: comuni, autorità regionali e nazionali;

Descrizione del modulo

Il presente modulo si concentrerà sul fare luce sulle minacce reali che si collegano ai sistemi wifi pubblici, su come funzionano ed infine su come prevenirle.

Obiettivi formativi

▪ Sensibilizzare sui pregiudizi riguardo l'uso delle reti wifi pubbliche

▪ Fornire conoscenza sulle minacce derivanti dall'uso delle reti wifi pubbliche

Durata complessiva

1 ora

Unità 1

il modulo comprende sia parti di apprendimento video che discussioni aperte. Nello specifico, inizialmente verrà mostrato un primo video introduttivo. Questo video mostra, con l'aiuto di un esperto, come sia rischioso connettersi ad internet nelle reti pubbliche. Tuttavia, questo primo video è molto breve e non permettere di cogliere molto del processo sottostante. Questa prima parte si conclude poi con una discussione tra studenti.

UTILIZZO DEL WI-FI SICURO

Modulo 5

Unità 2

In secondo luogo, verrà preso in considerazione un video più specifico. Nonostante il suo modo informale di trattare l'argomento, trasmette una migliore comprensione dell'argomento. Una volta che il **video** è terminato, il facilitatore è chiamato a proporre una discussione tra i partecipanti sui rischi delle reti pubbliche e, se possibile, condividere le proprie esperienze personali.

Attività didattica #1

Uno degli aspetti su cui questo modulo vuole porre l'attenzione è la facilità con cui queste minacce del wifi pubblico vengono proposte. Un'attività di apprendimento continuo è provare ad applicare i suggerimenti appresi dai contenuti video di questo modulo, dal ristorante/bar dove i partecipanti fanno pausa pranzo alla stazione dei treni e aeroporto dove i partecipanti si fermeranno per tornare a casa dopo la mobilità.

2. Bibliografia

https://www.youtube.com/watch?v=4YbXXW3DLQM&ab_channel=Techquicke

https://www.youtube.com/watch?v=1OVTmrXGHyU&ab_channel=CBSBoston

<https://www.kaspersky.com/resource-center/preemptive-safety/public-wifi-risks>

<https://goodspeed.io/blog/7-dangers-of-public-wifi.html>

https://www.youtube.com/watch?v=NkNgW3TwMy8&ab_channel=TheModernRogue

L'UTILIZZO DEI SOCIAL MEDIA

Modulo 6

1. Presentazione del modulo

Gruppi Target

Educatori del settore professionale della formazione

Studenti

Rappresentanti di istituzioni pubbliche attive nei settori educativi: comuni, autorità regionali e nazionali;

Descrizione del modulo

I social network online (OSN) hanno assunto uno spazio senza precedenti nella sfera professionale, educativa e privata della vita quotidiana delle persone, inclusa quella degli educatori VET e dei loro studenti. Mentre i benefici di tale integrazione sono stati più facili da riconoscere e adottare come componente integrante dell'istruzione formale e informale, i molteplici rischi associati ad esso non hanno ricevuto la dovuta attenzione e sono spesso ignorati dagli stessi educatori.

Un approccio semplicistico spesso è usato riguardo la sfaccettata problematica della sicurezza dei social network, così come la complessità di alcuni dei materiali formativi disponibili, non sufficienti per sviluppare le capacità necessarie per prevenire e rispondere alle minacce derivanti dall'uso di queste piattaforme.

Questo modulo cercherà di fornire agli allievi un insieme di conoscenze di base e di rafforzare la loro capacità di formazione, ma anche di migliorare il loro approccio personale alla sicurezza dei social network.

Obiettivi formativi

- Comprendere i rischi informatici e le minacce associate all'uso dei social media networks
- Rafforzare l'impatto dei processi di disinformazione sulla sicurezza delle piattaforme UGC
- Identificare le tipologie differenti di minacce alla sicurezza informatica

Durata complessiva

- Rafforzare la capacità di prevenire e rispondere alle minacce informatiche sui social media
- Fornire tecniche per gestire più facilmente password complesse.

L'UTILIZZO DEI SOCIAL MEDIA

Modulo 6

Unità 1 - Minacce dei social media

Questa Unità sarà facilitata dall'uso di una presentazione Power Point e introdotta dalla lettura di titoli di notizie che offrono storie diffuse di vittime di minacce informatiche attraverso i social media (foto di VIP rubate, persone che hanno perso la vita a causa di notizie false sull'immunizzazione, ecc...)

Le storie e il contenuto saranno adattati per essere pertinenti al contesto e aggiornate alle ultime scoperte.

La presentazione è seguita da 10 minuti di discussione di gruppo per riflettere sull'apprendimento e valutare la capacità dei partecipanti di comprendere l'argomento, ma anche per creare uno spazio per ulteriori domande e feedback.

Attività didattica #1

Il formatore, con una presentazione, espone ai partecipanti i seguenti contenuti suggeriti (max 20 minuti):

Cos'è un Social Network Online? Un Social Network Online (OSN) è una struttura sociale composta da individui o organizzazioni chiamate nodi, connessi da una o più specifiche tipologie di interdipendenza, come un'amicizia, un interesse in comune, e lo scambio di finanziamenti, relazioni di credenze conoscenze o prestigio.

I siti di social networking come Facebook, Twitter, Instagram, ecc... sono non solo usati per comunicare o interagire con altre persone a livello globale ma anche un modo efficace per la promozione aziendale.

A differenza delle piattaforme web tradizionali, i social media sono esclusivamente dedicati a ospitare e distribuire contenuti generati dagli utenti (UGC) secondo criteri (algoritmi) basati sulle azioni e le preferenze espresse dagli utenti stessi e registrate nei dati. In questo senso, tutti gli utenti sono attivi partecipanti nei processi di sostenibilità dei social network.

Che cos'è una minaccia sui Social Media? Una minaccia sui Social Media può essere qualsiasi cosa che compromette la sicurezza di un account. Una minaccia informatica può essere sia intenzionale che non intenzionale, mirata o non mirata, e può provenire da diverse fonti, tra cui nazioni straniere impegnate nello spionaggio e nella guerra informatica, criminali, hackers, scrittori di virus, impiegati contrariati e appaltatori che lavorano all'interno di un'organizzazione.

L'UTILIZZO DEI SOCIAL MEDIA

Modulo 6

Come si presenta una minaccia sui Social Media? Dato che i social network hanno un numero enorme di utenti e memorizzano innumerevoli quantità di dati, sono obiettivi naturali per gli spammers, il phishing e attacchi malevoli. In più, gli attacchi sui social online includono il furto di identità, la diffamazione, lo stalking, la lesione alla dignità personale e il bullismo informatico. Gli hackers creano profili falsi e imitano personalità o marchi, o diffamano un individuo noto all'interno di una rete di amici.

I problemi di privacy richiedono che i profili degli utenti non pubblichino e distribuiscano informazioni sul web. Le informazioni sulle home pages personali potrebbero contenere dati molto sensibili come le date di nascita, indirizzi di casa, numeri di telefono personali, e così via. Queste informazioni possono essere usate dagli hackers che usano tecniche di ingegneria sociale per ottenere benefici di tali informazioni sensibili e rubare denaro.

Come le minacce sui Social Media cambiano tra le piattaforme? Il modo in cui una minaccia sui social media viene effettuata da un aggressore dipende dai suoi obiettivi. Facebook permette agli utenti di mantenere privati le loro foto e commenti, per cui un malintenzionato spesso chiede l'amicizia agli amici dell'utente che ha preso di mira o invia direttamente una richiesta di amicizia all'utente stesso per accedere ai suoi post. LinkedIn è un altro obiettivo comune dei social media conosciuto per il business networking. Se un malintenzionato prende di mira un'azienda, LinkedIn è un eccellente sito di social media site per raccogliere le email aziendali per un attacco di phishing. Dato che molte piattaforme di social media visualizzano pubblicamente i post degli utenti, gli aggressori possono raccogliere silenziosamente dati senza che gli utenti ne vengano a conoscenza. Alcuni aggressori compiranno ulteriori passi per ottenere l'accesso alle informazioni dell'account contattando gli account presi di mira o i suoi amici.

Perché è importante parlare di minacce OSN? Al 30 dicembre 2020 ci sono quasi 4 miliardi di utenti nel panorama di internet. Della popolazione totale su internet, ci sono 2.7 miliardi di clienti dinamici mensili su Facebook, 330 milioni account attivi su Twitter e 320 milioni di utenti attivi su Pinterest. L'uso dei siti di social networking sta crescendo esponenzialmente. Se guardiamo solo a Facebook, sette nuovi profili vengono creati ogni secondo, 510.000 commenti sono postati ogni 60 secondi, 298.000 status sono aggiornati e 136.000 foto sono caricate nello stesso momento. Poiché viene caricata un'enorme quantità di dati, il rischio di una breccia nella sicurezza è alto. Chiunque può postare contenuti dannosi nascosti dentro dati multimediali o con localizzatori di risorse uniformi (URLs). Esistono circa 83 milioni di profili falsi che corrispondono a utenti illegittimi o professionisti che effettuano test o ricerche. Ogni giorno vengono hackerati all'incirca 100.000 siti web.

L'UTILIZZO DEI SOCIAL MEDIA

Modulo 6

Sebbene alcuni siti di social networking come Twitter non permettono di rilevare informazioni personali agli utenti, alcuni aggressori esperti possono dedurre informazioni riservate analizzando i post degli utenti e le informazioni che condividono online. Le informazioni personali che condividiamo online potrebbero bastare ai criminali informatici per ottenere le nostre email e passwords.

Il valore dei dati personali

I social media offrono spesso i loro servizi gratuitamente. Le informazioni personali non sono solo la valuta delle reti di social media, ma anche il principale obiettivo delle minacce informatiche sui social media.

Può essere facile lanciare un attacco perché molte persone sono solite fornire le loro informazioni personali alle piattaforme dei social media. I malintenzionati possono facilmente raccogliere questi dati e usarli a fini di lucro.

La raccolta di informazioni da rubare è solo un tipo di uso dei social media per la ricognizione. Le informazioni postate sui social media potrebbero essere usate per ottenere password o impersonare account aziendali.

Con una lista di obiettivi, un aggressore potrebbe poi esaminare gli account dei social media per le informazioni personali. Le informazioni personali possono aiutare gli aggressori a ottenere la fiducia dell'obiettivo in un attacco di social engineering. Possono, anche, essere usati per indovinare le risposte delle domande di sicurezza per l'acquisizione di un account o usati per avvicinarsi all'utente con privilegi più alti. Il nome di animali domestici, delle squadre sportive preferite e la storia dell'istruzione sono tutti potenziali indizi di password o risposte alle domande usate per verificare l'identità dell'utente per reimpostare una password.

Perché conoscere le minacce OSN?

Le interfacce e i processi facili da usare che queste piattaforme offrono potrebbero alludere a persone prive di conoscenze o capacità necessarie per accedere ai loro servizi e contenuti in maniera sicura.

L'educazione è la chiave per fermare le minacce delle reti di social media.

Il primo passo è educare gli utenti sui pericoli di divulgare troppe informazioni online al pubblico. Anche gli account social media impostati come privati potrebbero essere usati in un attacco, se l'aggressore ottenesse l'accesso ai feed privati. Gli utenti non dovrebbero mai postare informazioni aziendali private sui loro account dei social media o informazioni che potrebbero essere usate per l'acquisizione di un account.

L'UTILIZZO DEI SOCIAL MEDIA

Modulo 6

Il secondo passo è educare gli utenti su come i contenuti digitali sono prodotti e distribuiti, e su come possono guidare le azioni dell'utente verso obiettivi specifici per i quali i contenuti sono stati creati. Tutti i contenuti dei social media sono creati e veicolati dagli utenti in base ai loro differenti obiettivi personali e/o collettivi. Per queste ragioni, alcuni di questi contenuti potrebbero non essere sempre convenienti, veri o etici.

Infine, gli utenti devono essere educati all'uso sicuro e alla manutenzione dei dispositivi attraverso i quali accedono ai servizi delle reti di social media, in quanto sono normalmente vettori di rischi e intrusioni. Alcuni punti educativi a questo proposito sono già stati illustrati in altri moduli formativi e comprendono:

- Evitare di cliccare sugli annunci, specialmente i pop-up che invitano gli utenti a scaricare software per visualizzare i contenuti.
- Non condividere le password.
- Evitare messaggi o post sui social media che sollecitano azioni rapide come tecnica di social engineering.
- Non accettare richieste di amicizia da parte di persone che non si conoscono anche se l'utente ha diversi amici in comune.
- Evitare l'uso dei siti di social media da hotspot wi-fi pubblici (un luogo comune per i malintenzionati per spiare i dati utilizzando attacchi man-in-the-middle [mitm]).
- Cambiare regolarmente codici di accesso e password.

Attività didattica #2

Chiedere agli studenti di cercare il proprio nome su un motore di ricerca gestito dai social media o su Google, e di elencare tutte le informazioni private che possono essere rilevate dai contenuti multipli che si sono trovati (luogo e data di nascita, dettagli e informazioni sui membri della famiglia, indirizzi, numeri di telefono, animali domestici, partner romantici, hobbies e preferenze). Invitarli a pensare i modi in cui queste informazioni potrebbero essere usate contro di loro.

Unità 2 - Tipologie di minacce sugli OSN

Attività didattica #1

Chiedere agli studenti di elencare qualsiasi minaccia alla sicurezza loro pensano si possa incontrare sui social media e chiedergli di spiegare se credono che tale minaccia potrebbe esistere prima dell'esistenza dell'OSN.

VARIE MINACCE SULLE RETI SOCIAL ONLINE E MEDIA

Possiamo dividere le minacce su OSN in tre categorie:

- 1.Minacce convenzionali che includono minacce che gli utenti hanno sperimentato dalla fase iniziale dei social media
- 2.Minacce moderne sono attacchi che usano tecniche avanzate per compromettere gli account degli utenti
- 3.Attacchi mirati sono attacchi che hanno come obiettivo qualche utente in particolare.

MINACCE CONVENZIONALI

Spam - Spam è il termine usato per indicare messaggi elettronici di massa non richiesti. Sebbene la posta elettronica è un modo convenzionale per mandare gli spam, le piattaforme di social networking hanno più successo nel diffondere spam. I dati di comunicazione degli utenti legittimi possono essere facilmente ottenuti da siti web aziendali, blog, e newsgroup . Non è difficile convincere il cliente preso di mira a leggere messaggi spam e fidarsi di essere protetto. La maggior parte dello spam è pubblicità aziendale, può essere usato per raccogliere dati sensibili dagli utenti o potrebbe contenere virus, malware o truffe.

Attacchi malware - Malware è un'applicazione programmata che è esplicitamente evoluta per contaminare o accedere al sistema del computer, di solito senza che l'utente lo sappia. Malware può essere usato dalla struttura dei social network per diffondersi attraverso URLs condivisi o applicazioni sub OSN come giochi elettronici o plugin.

Phishing - Un attacco di phishing è un tipo di attacco di ingegneria sociale in cui l'aggressore può acquisire informazioni sensibili e riservate come username, password e i dettagli della carta di credito di un utente attraverso siti falsi e email che sembrano vere.

L'UTILIZZO DEI SOCIAL MEDIA

Modulo 6

Nel caso di OSN, un aggressore ha bisogno di attirare il cliente su una pagina falsa dove può eseguire un attacco di phishing. Per far accadere questo, l'aggressore usa doversi metodi di ingegneria sociale. Per esempio: può mandare un messaggio ad un utente che dice: "la tua foto personale è stata condivisa su questo sito, per favore controlla!" Facendo click su quel URL, l'utente è reindirizzato ad un sito falso che sembra un sito di social network legittimo.

MINACCE MODERNE

Attacco di cross-site scripting - Il cross-site scripting è un vettore di attacco prevalente tra gli infiltrati. Fondamentalmente, l'attacco esegue un codice JavaScript dannoso sul browser della vittima attraverso differenti tecniche. Il browser può essere dirottato con solo un singolo click di un pulsante che può mandare uno script dannoso al server. Questo script viene si ritorce contro la vittima e viene eseguito sul browser. Link e pulsanti accattivanti nei siti di social media popolari come Twitter e Facebook possono indurre l'utente a seguire gli URL, così come gli avvisi di allerta pop-up di virus e gli annunci promettenti o contenuti multimediali che richiedono la visita di un link o il fare click su un pulsante per essere sbloccati. Alcuni utenti possono essere invitati a copiare e incollare link contenenti JavaScript sulla barra degli indirizzi dei loro browser. Questi attacchi possono anche rubare informazioni o agire come spyware. Così gli attacchi possono anche dirottare i computer a lanciare attacchi a utenti ignari mentre il vero autore dell'attacco è nascosto dietro il dispositivo compromesso.

Attacco di clonazione del profilo - In questo attacco, l'aggressore clona il profilo dell'utente grazie a conoscenze pregresse o a informazioni raccolte online. L'aggressore può usare questo profilo clonato sia nella stessa o in un'altra piattaforma di social network per creare una relazione di fiducia con gli amici dell'utente reale. Una volta che la connessione è stata stabilita l'aggressore inganna gli amici della vittima a credere nella validità del profilo falso e ad accedere con successo alle informazioni riservate che non sono condivise nei loro profili pubblici. Questo attacco può, inoltre, essere usato per commettere altri tipi di crimini informatici, come bullismo informatico, stalking informatico e ricatto.

Hijacking - Per hijacking si intende il dirottamento, ovvero, l'avversario compromette o prende il controllo dell'account dell'utente per effettuare frodi online. I siti senza autenticazioni multifattoriali e gli account con password deboli sono più vulnerabili al hijacking, poiché le password possono essere ottenute attraverso il phishing. Una volta l'account è stato dirottato, il dirottatore può mandare messaggi, condividere link dannosi e cambiare le informazioni dell'account, tutto questo compromette il controllo dell'utente sul proprio account, così come la sua reputazione.

L'UTILIZZO DEI SOCIAL MEDIA

Modulo 6

Attacco di inferenza - L'attacco di inferenza deduce le informazioni riservate di un gestore, che l'utente potrebbe volere non rivelare, attraverso altre statistiche pubblicate dall'utente su alcuni OSN. Utilizza procedure di data-mining su dati visibilmente disponibili come l'elenco degli amici dell'utente e la topologia di rete. Utilizzando questa tecnica, un aggressore può trovare informazioni segrete di un'organizzazione o informazioni geografiche e di istruzione dell'utente.

Attacco Sybil / Botnet - Negli attacchi Sybil, un nodo rivendica identità multiple in una rete. Può essere dannoso per le piattaforme di social network in quanto contengono un enorme numero di utenti che sono accoppiati attraverso una rete peer-to-peer. I Peer sono i framework di computer associati l'uno all'altro attraverso internet e possono condividere documenti direttamente senza la necessità di un server centrale. Questa rete di dispositivi può anche essere chiamata BotNet. Un'entità online può creare diverse identità false e usare queste identità per distribuire informazioni spazzatura, malware, o persino colpire la reputazione e la popolarità di un'organizzazione. Ad esempio, un sondaggio sul web può essere manipolato utilizzando vari protocolli internet (IP) per inviare un numero enorme di voti e l'aggressore può mettere in minoranza un cliente autentico. Un esercito simile può, ad esempio, condividere un singolo messaggio più volte e rendere il suo contenuto virale.

Clickjacking - Il clickjacking è una procedura in cui l'intruso inganna l'utente a fare click su una pagina differente da quella che intendeva cliccare. L'aggressore sfrutta la vulnerabilità dei browser per eseguire questo attacco. Carica un'altra pagina sulla pagina alla quale l'utente vuole accedere, come un livello trasparente. Le due varianti conosciute del clickjacking sono il likejacking e il cursorjacking. Il livello frontale mostra la sostanza con cui il cliente può essere adescato. A questo punto quando il cliente tocca quel contenuto, in realtà tocca come il pulsante "mi piace". Più persone mettono "mi piace" al post, più questo si diffonde. Nel cursor jacking, un aggressore sostituisce il reale cursore con un'immagine personalizzata del cursore. Il cursore reale viene sostituito dalla posizione reale del mouse. In questo modo, l'intruso può indurre con l'inganno il consumatore a fare click su un sito dannoso grazie ad un posizionamento intelligente degli elementi della pagina.

L'UTILIZZO DEI SOCIAL MEDIA

Modulo 6

Attacco di de-anonimizzazione - In molti siti di social networking come Twitter e Facebook, gli utenti possono nascondere o proteggere la loro vera identità prima di rilasciare qualsiasi dato usando un alias o un nome falso. Ma se una terza parte vuole scoprire la vera identità dell'utente, può farlo tracciando i cookies, le tipologie di rete, e l'iscrizione ai gruppi di utenti per rivelare la vera identità. Si tratta di una sorta di metodo di estrazione delle informazioni in cui le informazioni misteriose vengono incrociate con altre fonti di informazioni per riconoscere nuovamente le informazioni sconosciute. Un aggressore può raccogliere informazioni sull'appartenenza al gruppo di un utente rubando la storia dai suoi browser e combinando questa storia con i dati raccolti. Così l'aggressore può de-anonimizzare l'utente che visita il sito web dell'aggressore.

MINACCE MIRATE

Bullismo informatico - Il bullismo informatico è l'uso dei mezzi di comunicazione elettronici come email, chat, conversazioni telefoniche e social network online per bullizzare o molestare una persona. Diversamente dal bullismo tradizionale, il bullismo informatico è un processo continuo poiché viene mantenuto costante attraverso i social media. L'aggressore invia ripetutamente messaggi di intimidazione, commenti sessuali, posta pettegolezzi e qualche volta pubblica immagini o video imbarazzanti per molestare una persona. Può anche pubblicare informazioni personali o private sulla vittima causando imbarazzo o umiliazione. Il bullismo informatico può anche accadere accidentalmente, nonostante sia raro che il ripetersi di tali mail, testi e post online possa essere accidentale.

Cyber grooming - Il cyber grooming consiste nell'instaurare una relazione emotiva con la vittima (solitamente bambini o adolescenti) con l'intenzione di abusarne sessualmente o mentalmente. Il punto principale del cyber grooming è di acquisire la fiducia del giovane con la quale si possono ottenere dal ragazzo informazioni intime e personali. I dati sono spesso di natura voluttuosa, attraverso conversazioni sessuali, immagini e video che danno all'aggressore il vantaggio di minacciare e ricattare la vittima. Gli aggressori spesso approcciano adolescenti o bambini attraverso identità contraffatte in siti per bambini, lasciandoli vulnerabili e non informati del fatto che sono stati avvicinati con il cyber grooming come obiettivo finale. Tuttavia, la vittima può avviare inconsapevolmente il processo di grooming quando riceve offerte remunerative, per esempio, denaro in cambio di dati di contatto o proprie foto personali. L'anonimato e l'accessibilità dei media avanzati permettono agli aggressori di avvicinarsi a diversi giovani simultaneamente, accrescendo esponenzialmente i casi di cyber grooming.

L'UTILIZZO DEI SOCIAL MEDIA

Modulo 6

Stalking informatico - Lo stalking informatico è l'osservazione di un individuo mediante internet, email o qualche altro tipo di corrispondenza elettronica che provoca il timore di violenza e interferisce con la pace mentale di quell'individuo. Comporta la violazione del diritto di privacy di una persona. L'aggressore rintraccia le informazioni personali o riservate delle vittime e le usa per minacciarle con continui e persistenti messaggi durante il giorno. Questa condotta rende la vittima eccezionalmente preoccupata per la propria sicurezza e che si crei in lei una sorta di problema, paura o turbamento. Al giorno d'oggi, la maggior parte degli individui condivide le proprie informazioni personali come il numero di telefono, il luogo di residenza, la zona e gli orari sui propri profili social, cos' come la posizione in cui vive. Un malintenzionato può raccogliere questi dati e usarli per lo stalking informatico.

Attività didattica #2

Chiedere agli studenti di lavorare a coppie e chiedergli di impersonare il rispettivo compagno mentre lo intervistano per 10 minuti. Invitateli a tentare le loro risposte cercando di ricavare le informazioni dal modo in cui sono vestite, dagli accessori che portano, e da qualsiasi altro dettaglio contestuale che potrebbe essere utile per impersonarli.

Attività didattica #3

Chiedere agli studenti di scorrere sui feed dei loro social media per un minuto e di contare tutte le "call-to-actions", link e bottoni che sono invitati a cliccare. Invitateli ad una riflessione di gruppo su come ciascuno di questi link rappresenti potenzialmente delle minacce e su come dovrebbero decidere quando e dove non interagire con il contenuto.

Unità 3 - Consigli per la protezione dei Social Media

Attività didattica #1

Distribuire a ciascuno studente uno o più schede che propongono schermate di pubblicazioni sui social media (inventate) provenienti da diverse piattaforme e invitateli a identificare quali informazioni sensibili loro possono ricavare dai singoli post e quali possibili minacce possono derivare dai quei post.

L'UTILIZZO DEI SOCIAL MEDIA

Modulo 6

COS'È LA PROTEZIONE DEI SOCIAL MEDIA

Le linee guida di protezione dei social media hanno lo scopo di prevenire accessi non autorizzati ai vostri account social, proteggere la vostra identità online da false impersonificazioni o furti di dati o di proteggere la vostra rete da identità o contenuti dannosi dei social media. Poiché le modalità e gli obiettivi delle minacce dei OSN spesso dipendono dal tipo di piattaforma, di conseguenza dovrebbero essere prese in considerazione alcune pratiche specifiche per prevenire le minacce.

PRATICHE GENERALI

Utilizzare una password forte: per mantenere la sicurezza degli account, gli utenti dovrebbero usare password forti. Non dovrebbe essere troppo corta perché una password corta può essere facile da indovinare. Dovrebbe essere lunga abbastanza e deve contenere caratteri alfanumerici con qualche carattere speciale. Gli utenti non dovrebbero usare la stessa password più account, perché se in qualche modo un malintenzionato viene a conoscenza della password, può compromettere tutti gli account di quell'utente.

Limitare la condivisione della posizione: oggi giorno condividere la posizione è

diventata

una tendenza. Molti siti di social network hanno introdotto anche la funzione di geotagging, che effettua automaticamente il tag della posizione geografica di un utente quando questo carica un contenuto multimediale sul social media. L'utente deve passare alla modalità manuale, affinché la posizione non venga taggata automaticamente. Gli utenti devono stare molto attenti a caricare i propri contenuti multimediali, poiché potrebbero contenere metadati sensibili, e si raccomanda che di cambiare il geotagging in modalità manuale in tutti i dispositivi mobili e account.

Essere selettivi con le richieste di amicizia: è stato osservato che molti utenti accettano richieste di amicizia senza analizzare il profilo completo del richiedente. Le persone, in genere, accettano le richieste di amicizia in base agli amici in comune. Se il richiedente ha alcuni amici in comune, allora accettano la richiesta. Qualche volta, i malintenzionati creano i loro profili attrattivi di proposito o possono impersonare un account. Quindi, se la persona che invia la richiesta di amicizia è sconosciuta, bisogna ignorarla. Potrebbe trattarsi di un account falso che tenta di rubare informazioni sensibili.

Attenzione a ciò che si condivide: gli utenti dovrebbero stare attenti ai loro post, perché potrebbero rivelare informazioni personali, e qualche volta anche quelle degli altri. Molte organizzazioni hanno regole e normative ferree per la condivisione di informazioni e contenuti multimediali. Ci sono molti casi di persone che sono state licenziate per aver condiviso informazioni illegalmente.

L'UTILIZZO DEI SOCIAL MEDIA

Modulo 6

Questa situazione può essere evitata se gli impiegati sono ben informati sui protocolli delle organizzazioni per le quali lavorano in merito alle immagini, ai video e ai messaggi che possono postare online. Condividere informazioni illegittimamente può danneggiare la reputazione dell'organizzazione sul mercato, i suoi dati e la sua proprietà intellettuale.

Essere consapevoli dei link e delle applicazioni di parti terze: gli utenti illegittimi possono accedere all'account di qualcuno e ottenere informazioni sensibili condividendo link dannosi. Ai nostri giorni, gli URL abbreviati stanno diventando molto popolari sulle piattaforme di social media. Questi URL abbreviati potrebbero essere offuscati da codici o script dannosi. Questi script cercano di raccogliere informazioni personali e riservate dell'utente, il che potrebbe servire a violare la privacy dell'utente. Inoltre, gli hacker potrebbero trarre vantaggio dalle vulnerabilità presenti in un applicazione di parti terze che è integrata con molti social network popolari. Un esempio di applicazioni di parti terze di questo tipo sono i giochi sui social network online, e che richiedono le informazioni pubbliche dell'utente per poter usufruire dei loro servizi. Queste informazioni possono essere fornite a estranei o interventi di parti terze. Per evitare questo rischio, gli utenti dovrebbero stare attenti quando installano applicazioni di parti terze nei loro profili.

Installare un software di sicurezza internet: Alcune minacce il cui schema è conosciuto possono essere facilmente rilevate attraverso degli antivirus. Minacce come il cyber grooming, il bullismo informatico possono essere rilevate in parte usando un software antivirus.

PRATICHE PER LA PIATTAFORMA DI CONDIVISIONE MULTIMEDIALE

- Non si dovrebbe pubblicare informazioni sensibili nelle proprie foto e didascalie. Esporre troppe informazioni personali in un profilo può essere pericoloso.

- Si dovrebbe evitare di condividere la posizione attuale sui social media. I servizi di geotagging forniti da differenti piattaforme multimediali dovrebbero essere disattivate manualmente.

- Se un applicazione non si usa per un periodo prolungato, è meglio revocarne l'accesso. Ci sono così tante applicazioni di parti terze che usano gli account dei social media per effettuare il login. Per sicurezza e privacy, si dovrebbe permettere l'accesso solo alle applicazioni affidabili.

- Abilitare l'autenticazione in due fasi per tutti i propri account di social media, ove possibile. Questo fornisce un ulteriore livello di sicurezza all'account. In caso in cui il malintenzionato scopra la password dell'utente, avrà comunque bisogno di un secondo fattore di autenticazione. Il secondo fattore consiste in un codice unico, sensibile al tempo, che l'utente riceve via messaggio sul proprio telefono cellulare.

L'UTILIZZO DEI SOCIAL MEDIA

Modulo 6

PRATICHE PER I FORUM DI DISCUSSIONE

- Si dovrebbe prestare attenzione quando si clicca sui link provenienti da diverse fonti. Potrebbe trattarsi di qualche sito sospetto che cerca di ottenere le credenziali dell'utente.
- L'utente dovrebbe sempre tenere d'occhio l'URL del sito. I siti dannosi potrebbero sembrare completamente indistinguibili da quelli reali. Tuttavia, l'URL può contenere piccole incongruenze, come una leggera variazione nel modo in cui è scritto (es. "0" invece che "o", indistinguibile se si legge velocemente) o un nome di un dominio alternativo.
- Stare attenti con le comunicazioni che richiedono al cliente di agire prontamente, offrendo qualcosa che sembra irrealistico o che richiedono informazioni personali.

PRATICHE PER LE PIATTAFORME DI CONNESSIONE SOCIAL

- Gli utenti dovrebbero imparare le impostazioni di privacy e sicurezza delle diverse piattaforme di social media e usarle. Ogni piattaforma fornisce le impostazioni, la configurazione e le sezioni sulla privacy per limitare chi e quali gruppi possono vedere vari aspetti del profilo dell'utente. Le impostazioni sulla privacy fornite dai siti come impostazioni predefinite non dovrebbero essere lasciate inalterate.
- Più dettagli sono forniti, più è facile per il malintenzionato usare queste informazioni per rubare l'identità o per commettere altri crimini informatici. Pertanto, la condivisione di informazioni dovrebbe essere limitata.
- Prima di accettare una richiesta di amicizia, si dovrebbe fare un controllo completo sul profilo del richiedente. Si possono creare gruppi diversi per la condivisione di diverse tipologie di informazioni, come gruppi diversi per i collegi e per la famiglia.

PRATICHE PER RETI PROFESSIONALI

- Le reti professionali sono usate principalmente per creare contatti e accrescere la visibilità nei confronti dei potenziali compagni di reclutamento. Quindi, per usare in maniera sicura le reti professionali, si dovrebbero cercare i dettagli forniti dagli altri utenti prima di aggiungerli alla propria lista di contatti. Genericamente, un malintenzionato non fornisce molti dettagli sulla propria carriera.
- Un utente dovrebbe controllare se ci sono degli errori di ortografia o grammatica nei profili dell'altro, perché se qualcuno si candida per un lavoro, starà molto attento a scrivere bene, senza commettere errori di grammatica o ortografia. Dovrebbe contenere informazioni accurate e presentare bene quella persona.
- Controllare la coerenza nella carriera di una persona può essere una buona abitudine se un utente vuole rimanere al sicuro su una rete professionale. Un profilo che cambia continuamente e drasticamente in un breve periodo di tempo è il modo più utilizzato dall'aggressore per attirare. Nel momento in cui il truffatore ha bisogno di prendere di mira

L'UTILIZZO DEI SOCIAL MEDIA

Modulo 6

- Si dovrebbe, inoltre, fare un controllo incrociato delle informazioni. Se una persona dichiara di essere impiegato di una azienda, l'utente può controllare l'elenco dell'azienda e non dovrebbe esitare a verificare con il dipartimento di risorse umane dell'azienda.

Attività didattica #2

Chiedere agli studenti di spiegare chi pensano abbia accesso all'ultimo post che hanno pubblicato sul loro sito preferito di social network. Infine, aiutarli a controllare le loro impostazioni di privacy e vedere quanto di quello che si è detto corrisponde alla verità. Aprire una discussione di gruppo su ciò che è venuto fuori.

Attività didattica #3

Invitare gli allievi a guardare di nuovo le schede che hanno ricevuto durante l'**attività di apprendimento 1** di questa unità e chiedergli se possono identificare ulteriori rischi nelle pubblicazioni sui social media presentate prima. Chiedergli cosa farebbero per ridurre tali rischi.

2. Risultati formativi del modulo

Comprensione

- Rischi informatici e minacce associate all'uso dei social media network
- Sicurezza delle piattaforme UGC (UGC = Contenuti Generati dall'Utente)

Capacità

- Identificare le differenti tipologie di minacce informatiche.

Competenze

- Prevenire e rispondere alle minacce informatiche sui social media
- Gestire password complesse

L'UTILIZZO DEI SOCIAL MEDIA

Modulo 6

3. Bibliografia

<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

DISCLAIMER

Il progetto è stato finanziato dall'Unione Europea. I punti di vista e le opinioni espresse sono, tuttavia, esclusivamente quelli dell'autore/i e non necessariamente riflettono quelli dell'Unione Europea o dell'Agenzia esecutiva per l'istruzione e la cultura (EACEA). Né l'Unione Europea, né l'EACEA possono essere ritenute responsabili per questo.





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



IMPROVING CYBERSECURITY READINESS OF
THE EUROPEAN VOCATIONAL EDUCATION
AND TRAINING SECTOR

MATERIALE DIDATTICO

IMATERIALE FORMATIVO
PER LA CONSAPEVOLEZZA
SULLA SICUREZZA
INFORMATICA NEL
SETTORE IFP



INTRODUZIONE MATERIALE FORMATIVO

AL

GAME JAMS

INTRODUZIONE

Dall'autunno 2021, in occasione del Mese europeo della sicurezza informatica, alla primavera del 2022, i partner del progetto CYBER.VET.EU hanno organizzato diversi GameJam nei paesi dei partner. I giovani sono stati coinvolti dando loro la possibilità di essere vicini ai temi della cybersecurity e fornendo loro nuovi strumenti.

L'obiettivo principale di questo Intellectual Output era risolvere la necessità di una maggiore consapevolezza sulla sicurezza informatica. Ci siamo rivolti al processo di "gamification" per ottenere una soluzione facile da adottare, veloce da implementare, scalabile nel tempo e inclusiva. Il processo di gamification, definito come "l'applicazione delle meccaniche di gioco a contesti non di gioco con l'obiettivo di indurre coinvolgimento e aumentare i livelli di motivazione", è un modo dimostrato per mantenere gli utenti coinvolti in attività di apprendimento, con grandi risultati anche nel breve periodo di tempo grazie allo sfruttamento dell'intrattenimento che motiva i partecipanti a impegnarsi di più con il materiale e ad esercitarsi. In quanto tale, questo output fungerà da combinazione di linee guida, formazione e pratica, con la caratteristica di essere facilmente aggiornabile quando dovrebbe essere aggiunto nuovo materiale.

RISULTATI DELLE GAME JAMS

Maggiore consapevolezza della sicurezza digitale

- Maggiore consapevolezza della sicurezza digitale tra le comunità dei partecipanti (famiglia, amici, colleghi)

Riduzione del tasso di successo del malware all'interno delle istituzioni

Riduzione degli eventi di fuga di dati

Cresce l'interesse per il settore della cybersecurity come opportunità di lavoro.

AEII / INERCIA DIGITAL [ES]

ATTIVITÀ

Le attività più rilevanti svolte dai partner spagnoli AEII e Inercia Digital sono state:

Hackaton

GameJams

Giornate informative

Conferenza internazionale

Evento divulgativo

RISULTATI

Le sessioni di GameJam in Spagna hanno fornito alcuni risultati utili che possono essere visualizzati qui:

<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

La cybersicurezza nell'educazione

I partner spagnoli AEII e Inercia Digital hanno partecipato online a un Hackathon dal 20 al 22 ottobre 2021, con 47 partecipanti, molti dei quali esperti IT.

<https://www.comprometidosporelfuturo.com/proyectos#> supportato da Boehringer Ingelheim in Spagna.

PROBLEMA DA RISOLVERE

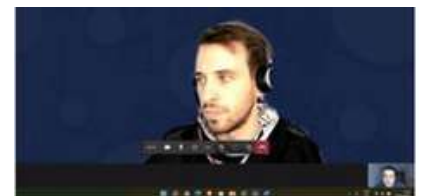
Il cyberbullismo è uno dei principali rischi di Internet per i giovani. È comune trovare post con contenuti offensivi nei confronti di alcune persone e che questi vengano utilizzati per molestare e deridere le vittime.

Il cyberbullismo spesso causa gravi disturbi nelle vittime come disturbo da stress post-traumatico, depressione, pensieri e comportamenti suicidari o ansia.

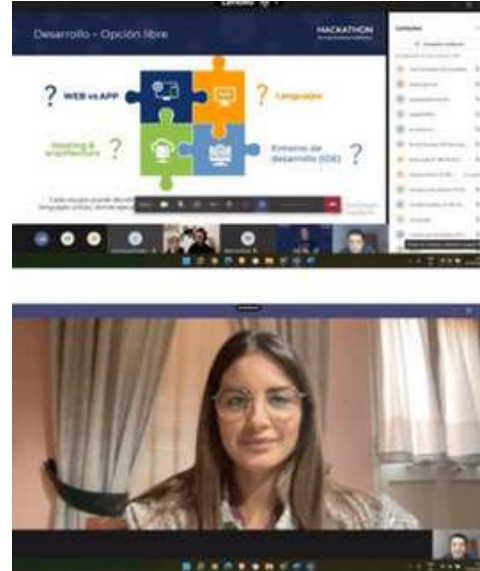
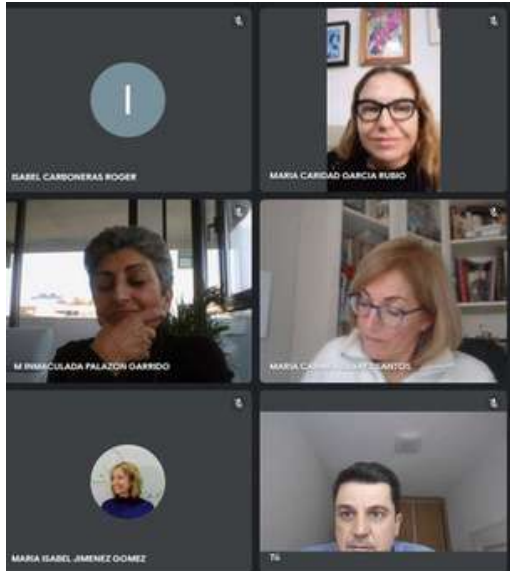
Questa sfida consiste nello studiare e analizzare ciò che i giovani sanno sulla sicurezza, oltre a renderli consapevoli dei rischi che corrono nei loro centri educativi e nella vita quotidiana. Questa sfida cerca, attraverso la gamification, la maggiore consapevolezza di studenti e insegnanti nella vita di tutti i giorni sui temi legati alla sicurezza nell'uso delle nuove tecnologie.

RISULTATI

- Gioco e animazione legati alla sicurezza informatica nell'istruzione
 - Coinvolgimento della pubblica amministrazione, scuole di formazione professionale, esperti IT, insegnanti, studenti e partner di progetto
- Realizzazione di brevi video interattivi



AEII / INERCIA DIGITAL [ES]



In generale, dopo aver condotto numerosi sondaggi, la conoscenza della sicurezza informatica di insegnanti e studenti nei centri di formazione professionale è ancora bassa in Spagna. Per questo motivo, questo progetto e altri simili sono molto rilevanti in Spagna.

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

GAME JAM

NGO Nest Berlin, Extrafondente Open Source - EOS e IASIS hanno realizzato insieme una sessione di GameJam nel febbraio 2022. Il GameJam è iniziato sabato 12 ed è durato complessivamente 6 giorni. Ha visto le squadre nazionali sviluppare e lavorare insieme su una bozza di gioco (di un gioco online o da tavolo).

È stata riunita una giuria indipendente a cui è stato chiesto di valutare la bozza del gioco seguendo linee guida comuni e un modello di valutazione.

La squadra vincitrice ha ricevuto un tutoraggio di 6 mesi e risorse tecniche per sviluppare ulteriormente l'idea del gioco.

RIGUARDO AL GIOCO

È un gioco da tavolo strategico a turni da 2 a 6 giocatori, che richiede dai 30 ai 60 minuti per essere giocato. In questo gioco inganni gli umani per convincerli che sei il miglior gatto e ottieni più prestigio ottenendo il maggior numero possibile di servitori di gatti umani. Tieni gli occhi aperti, gli altri gatti boss cercheranno attivamente di sabotare la tua strada per raggiungere gli umani e prendersi la gloria per se stessi. Non fidarti delle loro facce carine!

Perdi la partita se non hai un numero elevato di umani come servitori o il decimo round è finito e nessuno dei giocatori ha almeno 4 umani al proprio comando.

La difficoltà è che ci sono 6 Boss che cercano di ingannare gli umani per farli diventare i loro servitori e quindi i capi possono controllarli, ma tutti hanno lo stesso obiettivo e alcuni potrebbero persino aiutare gli umani a liberarsi dal controllo del gatto.

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

Mau Mau

Characters



Name	Mau Mau
Backstory	His is the most ancient cat of them all, his ancestral family were mummified alongside Pharaohs in their tombs. He still can talk and walk among Egyptian gods and goddess
Appearance	Will have a god aspect and similar to the original real cat
Special Capacities	Very intelligent, leader and knows how to attract human with his charm
Special Weaknesses	Forget he is not a "God times" anymore and bossy

CYBERVET GAME JAM - THE KITTEN ALGORITHM... ☆ 2 of 3

175% 7 of 20

LECSA (LV)

GAME JAM

Il partner LECSA dalla Lettonia ha organizzato un evento GameJam dal 27 settembre al 1 ottobre 2021. A causa delle restrizioni epidemiologiche e delle diverse località dei partecipanti, è stato organizzato come un evento di tipo ibrido (in loco presso la Saldus Technical School e tramite la piattaforma Zoom). Durante l'evento sono state formate 6 squadre (4-5 persone per squadra) per lavorare allo sviluppo dei prototipi del gioco. Per ottenere alcuni risultati tangibili, il concetto di Game Jam prevedeva lo sviluppo di due tipi di giochi: giochi per computer e giochi da tavolo.

ATTIVITÀ

Agosto - settembre 2021 è stato dedicato alla pianificazione e all'organizzazione dell'evento (ricerca di esperti in sicurezza informatica e sviluppo del gioco, distribuzione delle informazioni ai potenziali partecipanti, pianificazione dell'agenda e definizione dei criteri per il gioco, ecc.)

Evento moltiplicatore – Attualità nei cyberattacchi (27.09.2021): Introduzione del progetto CYBER.EU.VET e conferenza sulle tendenze nei cyberattacchi con Mr. Armins Palms, esperto di sicurezza informatica del CERT.LV (IT Security Incident Response Institution of the Repubblica di Lettonia)

Numero di partecipanti: 26 persone

Luogo: Saldus Technical School (città di Saldus) e piattaforma ZOOM

Annuncio del Game Jame (27.09.2021): definizione e discussione sulle attuali sfide nella sicurezza informatica (valutazione dei bisogni); formazione di team, incontro con i mentori e discussione su ulteriori lavori (workshop sul motore di gioco Unity), brainstorming sull'idea e sul concept del gioco.

Attività di Game Jam in corso (28.09-30.09.2021): i team hanno lavorato allo sviluppo dei prototipi, se necessario è stata assicurata la consultazione con i mentor.

Presentazione dei progressi (30.09.2021): presentazione dei concetti del gioco e dei progressi del lavoro per ricevere suggerimenti dai mentori.

Gran finale (01.10.2021): quattro squadre hanno presentato i loro risultati e i mentori hanno fornito la valutazione. Una squadra, che stava sviluppando un gioco per computer, si è ritirata. Conclusione dell'evento e discussione informale.

Numero di partecipanti: 30

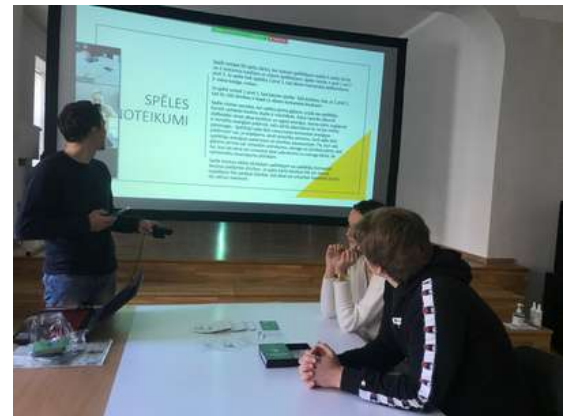
Luogo: Saldus Technical School e piattaforma ZOOM

LECSA (LV)



RISULTATI

1. Prototipo di gioco online - Il virus
2. Gioco da tavolo - Carte sulla sicurezza
3. Gioco da tavolo - Cyberwar
4. Gioco di carte competitivo - Cyber Mind



ESEMPIO Cyber Mind - A competitive card game

Questo è un gioco di carte educativo con elementi quiz. Il compito principale del gioco è insegnare le basi della sicurezza quotidiana su Internet e ciò a cui le persone si espongono facendo cose sciocche su di esso. Copre argomenti come la sicurezza in Internet e la protezione dei dati nel contesto dell'utilizzo dei social network. Nel risultato del gioco le persone (giocatori) dovrebbero essere in grado di riconoscere i tentativi di truffa nella vita reale.

Sviluppato dal team Veiksminieki (dal lettone: persone di successo), studenti della scuola tecnica Saldus durante il Game Jam in Lettonia (ottobre 2021):

Renars Ricards Hartmanis, Estere Ozoliņa, Sindija Diāna Valtere e altri.

Livello: base (per principianti). Gruppo target – alunni, studenti, insegnanti e genitori

Il gioco contiene: 50 carte, 2 cuscini sanitari (per contare la salute dei giocatori), 2 dadi e una carta delle regole.

LECSA (LV)

GAME JAM

IL GIOCO

I tentativi di attacchi informatici nel mondo aumentano ogni giorno, quindi il governo mondiale ha avuto l'idea di organizzare un torneo per identificare le persone che portano rischi informatici e contrattaccare contro di loro.

Gioco educativo che aiuta a conoscere i principali tipi di attacchi informatici, i metodi di prevenzione ed eliminazione proteggendo te stesso o la tua squadra e contrattaccando l'avversario. Lo scopo del gioco è togliere tutte le vite dell'avversario/i.

COME GIOCARE GIOCO/REGOLE

Numero di giocatori: 2 o 4 persone (1 contro 1 o 2 contro 2).

Ogni giocatore o squadra (quando 2 contro 2) ha "100 vite" (Salute=HP) all'inizio del gioco. Il conteggio della salute viene eseguito utilizzando blocchi note neri o altre note disponibili.

Assegna una persona separata che segua e calcoli il consumo di energia e salute dei giocatori, se possibile. Altrimenti i giocatori lo fanno da soli.

Ogni giocatore riceve 5 carte. Se il gioco si gioca 2 contro 2, entrambi i giocatori hanno "una mano comune" nella squadra o 10 carte insieme.

Ci sono tre tipi di carte: **Carte Attacco** (rosse), **Carte Scudo** (gialle) e **Carte Vita o Cura** (verdi).

Il gioco si gioca a turni. Il giocatore/la squadra che ottiene il numero più alto con i dadi inizia il gioco.

Ogni carta costa energia. All'inizio di ogni round, il giocatore tira 2 dadi per definire un'Energia che è indicata nella parte superiore della carta (in blu). Le carte devono essere giocate in modo da non superare la quantità di energia ottenuta.

Il giocatore/squadra che inizia il round può attaccare (con Attack Cards), proteggersi (Shield Cards) o aggiungere vita (Healing Cards), mentre i second mover possono usare solo Attack e Shield card per ridurre al minimo la loro vulnerabilità alla vita.

Tieni presente che il numero massimo di vite per giocatore/squadra durante il gioco può essere di 100 HP (ad esempio, se la somma di vite ed energia dopo il round fa 110 HP in totale, il tuo numero di vite rimane comunque - 100 HP).

Il gioco termina non appena un giocatore/squadra esaurisce tutte le vite (0 vite).

Se il gioco esaurisce le carte, devi rimescolare le carte dalla pila.

LECSA (LV)

Esempi di carte:

In **blu** - Energia

In **rosso** - Carte attacco

In **giallo** - Carte scudo

In **verde** - Carte guarigione

-9 **Paying ransomware ransom**



You can pay ransom to the attacker to get your data or system back.

-11 **Ransomware**



The victims system is held hostage until they agree to pay a ransom to the attacker.

+14

-15

-2 **Updating computer and software**



To keep your computer secure you can update it and its software.

-2 **Verifying source of email**



To reduce unwanted spam or chances of opening harmful email attachments, you can verify sources of email by checking if their emails are legitimate.

+5

+5

Esempio di calcolo della guarigione:

CYBER MIND	
CALCULATION OF LIVES	
PLAYER 1/TEAM 1	PLAYER 2/TEAM 2
00 100 HP	00 100 HP
01	01
02	02
03	03
04	04
05	05
06	06
07	07
08	08
09	09
10	10
-	-

LECSA (LV)

GAME JAM

ESEMPIO Cyberwar - Gioco da tavolo

Sviluppato dal team Exodus (studenti della Saldus Technical School), leader del team Valdemārs Šperbergs.

2-6 giocatori < - > Adatto a persone dai 15 anni in su

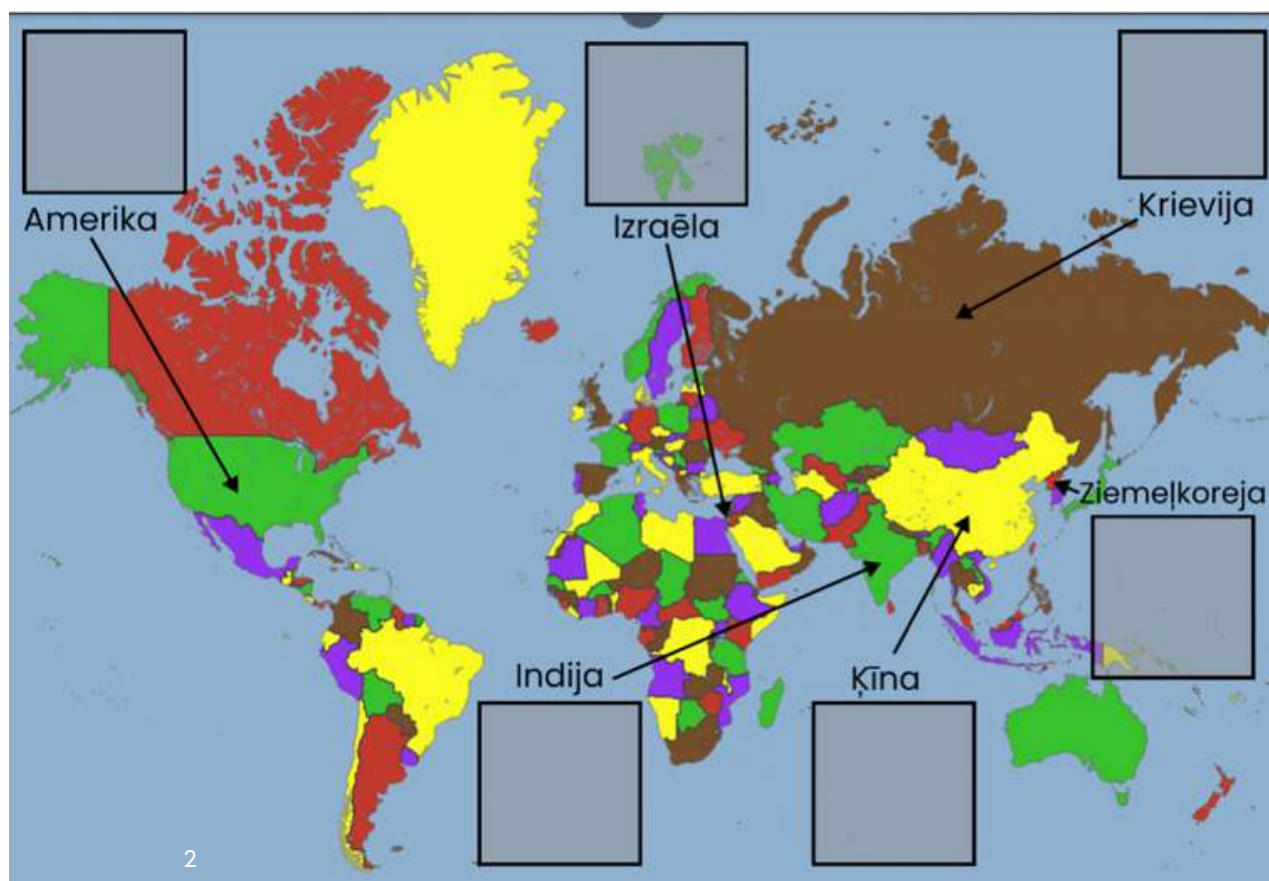
Un gioco da tavolo con una forte enfasi sulla tattica e sulla casualità (caso).

Livello: gioco educativo per coloro che hanno una certa conoscenza della sicurezza informatica.

Il gioco contiene: mappa del mondo, 2 dadi, server, carte con funzione "attacco", "difesa" o "reazione", legenda delle vulnerabilità, una tabella con le possibili mosse per ogni tipo di vulnerabilità.

IL GIOCO

Lo scopo del gioco è proteggere il paese rappresentato dal giocatore e attaccare altri paesi per vincere la guerra informatica. In Cyberwar, ogni giocatore deve scegliere un paese da rappresentare. Ogni giocatore ha un server con 3 vulnerabilità. L'obiettivo del giocatore è hackerare i server di altri paesi sfruttando due vulnerabilità su tre o correggere due vulnerabilità su tre sul proprio server.



LECSA (LV)

COME GIOCARE

I giocatori scelgono il paese da rappresentare e posizionano un oggetto server in un punto designato della mappa. Ogni paese ha i suoi bonus. Ogni giocatore pesca (prende) casualmente 3 vulnerabilità, una per ogni livello di difficoltà, e le posiziona a faccia in giù nelle rispettive posizioni sui propri campi del server. Le vulnerabilità non sono note per i giocatori. Le vulnerabilità hanno 3 livelli di difficoltà. Il livello di difficoltà determina anche quanto grande numero è necessario per sfruttare una vulnerabilità (vedi "Attacchi"), così come determina quante mosse saranno necessarie per correggere la vulnerabilità (vedi "Défense").

Il gioco si svolge nei round, è possibile eseguire le seguenti azioni (mosse): scansione, attacco e difesa. I giocatori determinano la sequenza dei giocatori lanciando due dadi. Inizio Ogni giocatore riceve 4 carte all'inizio di ogni round. Alla fine del round, è possibile – tenere 2 carte o scambiarle con quelle esistenti. Il primo round è un round di scansione in cui non sono consentite carte di attacco o difesa. Nei round successivi, i giocatori possono scegliere di scansionare o attaccare o provare a riparare le proprie vulnerabilità (vedi Défense). Il gioco continua round dopo round fino al raggiungimento di una condizione vincente. Scansione L'attaccante sceglie un paese per scansionare la sua vulnerabilità (ad esempio, "Sto scansionando un russo di 2° livello di vulnerabilità"). Il giocatore esegue la scansione: lancia due dadi, applicando i bonus del paese rappresentato, confronta con il livello di difficoltà di vulnerabilità + bonus del paese della vittima. Se l'attaccante ha ottenuto un numero uguale o superiore al livello di difficoltà di vulnerabilità della vittima, l'attaccante può esaminare la vulnerabilità scansionata. I bonus del paese non vengono aggiunti durante la scansione di te stesso.

Livelli di difficoltà 1° – il giocatore deve ottenere almeno il numero 4 (esclusi i bonus del paese) 2° – il giocatore deve tirare almeno 8 (esclusi i bonus del paese) 3° – il giocatore deve tirare almeno 11 (esclusi i bonus del paese).

LECSA (LV)

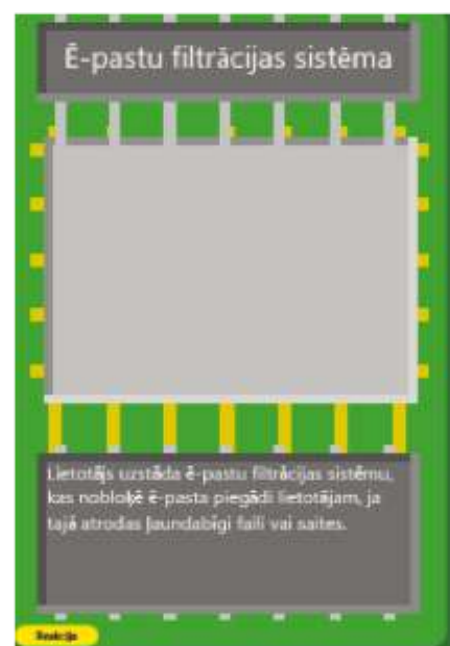
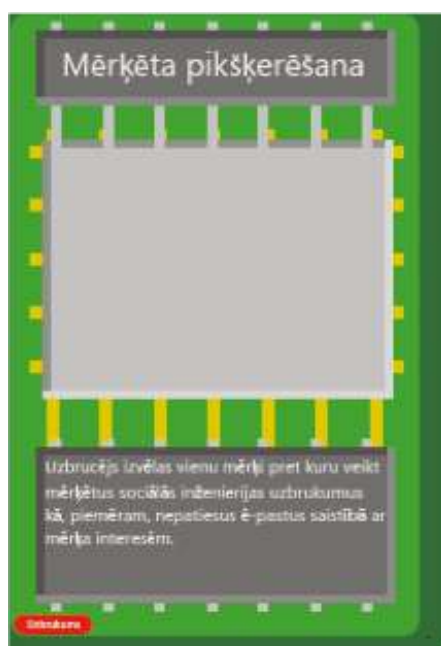
GAME JAM

ATTACCHI

- Il giocatore nomina l'obiettivo dell'attacco (ad esempio, "Attacco una vulnerabilità russa di livello 2") e rivela la carta di attacco a tutti i giocatori, posizionandola accanto alla vulnerabilità.
- Il giocatore tira i dadi per vedere se l'attacco funziona confrontando il tiro con la difficoltà di vulnerabilità + bonus (se il numero ottenuto + i bonus corrispondono o superano la difficoltà, l'attacco ha successo).
- Gli attacchi possono essere respinti utilizzando la Carta Reazione progettata per quell'attacco.
- Ogni attacco ha il proprio tipo di reazione che può essere giocato e il proprio tipo di vulnerabilità per cui funziona.
- Se l'attacco fallisce o viene bloccato da una Carta Reazione, le carte Attacco e Reazione giocate rimangono sul tavolo fino alla fine del round successivo e impediscono agli altri giocatori di attaccare con lo stesso attacco per la stessa vulnerabilità. Dopo la mossa entrambe le carte tornano nel mazzo.

Livelli di difficoltà

- 1° – il giocatore deve ottenere almeno il numero 4 (esclusi i bonus del paese)
- 2° – il giocatore deve tirare almeno 8 (esclusi i bonus del paese)
- 3° – il giocatore deve tirare almeno 11 (esclusi i bonus del paese).



LECSA (LV)

DIFESA

- Difesa: scegliere il metodo giusto contro una particolare vulnerabilità. Reaction Cards blocca (annulla) l'attacco in arrivo (e tutti gli altri attacchi che mirano alla stessa vulnerabilità) per 1 turno.
- Per annullare un attacco in arrivo, il giocatore posiziona una carta di reazione corrispondente al tipo di attacco (vedi tabella con le vulnerabilità) sulla carta di attacco non appena l'attacco viene giocato.
- Per iniziare a riparare un infortunio, un giocatore posiziona una carta Défense accanto all'infortunio da riparare.
- Gli altri giocatori possono attaccare questo infortunio mentre è in Difesa (prima che il turno di Difesa sia terminato).
- Quando il giocatore cerca di riparare un infortunio sul suo server con una carta Défense, non può attaccare, ma può tentare di prevenire gli attacchi con le carte di reazione. Per una riparazione completa è necessario il livello di difficoltà + 1| giro. L'azione di scansione è consentita durante il periodo di riparazione.
- Se il metodo Défense non è corretto, il giocatore salta 3 turni e non può usare Carte Défense durante questo periodo (le reazioni e le azioni di scansione sono consentite).

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

Bonus per i Paesi

USA: +2 in scansione

Russia: +2 per gli attacchi

Cina: +2 per la difesa dagli attacchi

- Corea del Nord: +2 per la difesa contro la scansione

India: +1 in tutti gli attacchi, -1 contro gli attacchi

Israele: +

3 in tutti gli attacchi, -3 contro gli attacchi



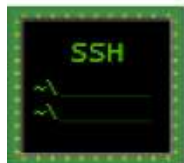
LECSA (LV)

GAME JAM

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



LECSA (LV)



SSH serveris



SSH serveris ar
lietotājvārdu



Administrācijas panelis



Administrācijas panelis
ar lietotājvārdu



Neapmācīts darbinieks



Ievainojams SMB protokols



XSS ievainojums



SQL injekcija



Rūtera panelis ar
noklusējuma lietotājvārdu
un paroli



XSS ievainojums ar filtru



SQL injekcija ar filtru



Nepilnīgi nokonfigurēts
ugunsmūris



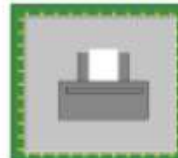
WiFi tīkls ar WEP drošību



Pakalpojuma atteices kļūda



Ievainojama OpenSSL
programma



Ievainojama Print Spooler
programma



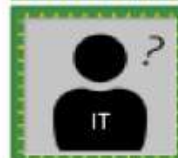
Bufera pārpildes ievainojums



Vājš jaucējvērtības algoritms



Aizņemts priekšnieks



Slinks IT speciālists



LECSA (LV)

GAME JAM



LECSA (LV)



TIPS & EXPERIENCES FROM THE GAMEJAM IN LATVIA

- Durante l'evento di 2 giorni non è possibile sviluppare un vero gioco per computer, ma piuttosto il primo prototipo, che potrebbe essere ulteriormente sviluppato o meno a seconda della motivazione dei partecipanti.
- Premi o altri tipi di benefici possono aiutare a coinvolgere più partecipanti e garantire risultati migliori (più tangibili) alla fine (nel nostro caso - pizza e bevande sono state fornite alla fine dell'evento, ulteriore supporto da parte dei mentori (ad es. la piattaforma)).
- I tutor sullo sviluppo del gioco e sui problemi di sicurezza informatica svolgono un ruolo importante nel Game Jam consultando e aiutando i partecipanti.
- Pianificare in anticipo – poiché si tratta di un evento piuttosto complesso e richiede un'attenta pianificazione.
- Gli organizzatori devono considerare che alcune squadre potrebbero non partecipare alla competizione (a causa dei tempi limitati).

Si prega di consultare i post FB con i risultati dell'evento:
<https://www.facebook.com/cybereuvetproject.eu/posts/138127645211214>
<https://www.facebook.com/saldustehnikums/posts/1780232175520378>



L'evento è stato organizzato da LECSA in collaborazione con Latvijas Universitāte | Ekonomikas un kultūras augstskola / EKA University of Applied Sciences | McĀbols | cert.lv | Coldwild Game s | Saldus tehnikums!

MEATH PARTNERSHIP (IE)

ATTIVITÀ

- Incontro informativo sulla valutazione dei bisogni con gli studenti (formazione di codifica in un istituto locale per l'educazione degli adulti)
- 2 giorni GameJam (sessione informativa online il 1° giorno; 2° giorno dedicato a Game Jam)

Evento - Mattinata di sensibilizzazione sulla sicurezza informatica

1) Incontro informativo sulla valutazione dei bisogni con gli studenti

(formazione sulla codifica in un istituto locale per l'educazione degli adulti)

Data: ottobre 2021

DESCRIZIONE

Al fine di diffondere il progetto e identificare i temi principali per la Game Jam, il team di Meath Partnership ha organizzato una sessione informativa con gli studenti di un corso di formazione locale di Coding. La condivisione delle informazioni sulla Cybersecurity e la discussione sulle minacce più recenti è stata seguita da una sessione di brainstorming di gruppo in cui gli studenti sono stati divisi in due gruppi al fine di discutere le domande che hanno portato all'identificazione degli argomenti più interessanti da approfondire durante il Gamejam. Durante la giornata sono state condivise con i partecipanti anche ulteriori informazioni sul Gamejam e sul progetto CYBER.EU.VET.

ESEMPIO DI DOMANDE PER LA VALUTAZIONE

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)

RISULTATI

Come risultato di questa attività, il team di Meath Partnership ha acquisito una migliore comprensione della conoscenza complessiva degli studenti in relazione alla sicurezza informatica e alle minacce informatiche, nonché informazioni raccolte che sono state ulteriormente incluse nel processo di pianificazione e implementazione del GameJam.



MEATH PARTNERSHIP (IE)

GAME JAM

2) 2-days Gamejam

(online information session on the 1st day; 2nd Day dedicated to Game Jam)

DESCRIZIONE

Il GIORNO 1 è stato dedicato all'accoglienza dei partecipanti e alla presentazione del progetto CYBER.EU.VET e all'apertura del Game Jam, nonché alla condivisione delle informazioni sui 2 temi individuati durante l'incontro di valutazione dei bisogni. Ai partecipanti è stata offerta la possibilità di lavorare individualmente o come parte di un team. Hanno anche avuto l'opportunità di porre qualsiasi domanda o ricevere ulteriori chiarimenti sui procedimenti relative allo sviluppo dei giochi nel giorno 2.

Il GIORNO 2 è stato dedicato allo sviluppo dei giochi e i membri del nostro team e un esperto di supporto IT erano disponibili via Zoom per supportare i partecipanti per tutta la durata del Game Jam da

Dalle 9:00 alle 21:00.

I partecipanti sono stati invitati a caricare i loro giochi sulla piattaforma Itchio sotto un profilo creato appositamente per questo evento: [CYBER.EU.VET : Cybersecurity Game Jam - itch.io](https://itch.io/jam/cybereu-vet)

RISULTATI

Dopo che i partecipanti hanno condiviso le loro bozze di gioco con la squadra, un partecipante ha deciso di andare avanti e caricare il gioco per un'ulteriore valutazione. Il resto dei partecipanti ha deciso di non inviare le proprie bozze poiché erano nelle primissime fasi.



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/cybereu-vet-cybersecurity-gamejam>

Online interactive cybersecurity game:
<https://itch.io/jam/cybereu-vet-cybersecurity-gamejam>



MEATH PARTNERSHIP (IE)

3) Evento - Mattinata di sensibilizzazione sulla sicurezza informatica

Date: November 2021

DESCRIZIONE

L'Evento si è tenuto online Via Zoom per far conoscere il progetto e le sue attività. L'evento è stato ampiamente diffuso tra un'ampia varietà di parti interessate interessate o coinvolte nella sicurezza informatica. L'evento è iniziato con una presentazione e panoramica del progetto e della Game Jam, seguita da una presentazione e discussione sulla Cybersecurity e dalla condivisione di informazioni pratiche su come rimanere online (le attuali minacce informatiche e come eliminare possibili attacchi erano possibili).

RISULTATI

L'evento ha contribuito a sensibilizzare sul progetto e ha anche creato l'opportunità di presentare a un pubblico più ampio i traguardi raggiunti dall'inizio del progetto. È stata anche una grande opportunità per condividere informazioni pratiche e consigli relativi alla sicurezza informatica con i partecipanti all'evento.

COMMON PASSWORD AUTHENTICATION METHODS

TWO-FACTOR AUTHENTICATION (2FA)

- Two-factor authentication requires the users to authenticate via something "they know" and something "they have". A password serves as "something they know," and a specific physical object such as a smartphone serves as "something they have."
- Two-factor authentication usually requires the user to enter their username, a password, and a one-time code that has been sent to a physical device (mobile phone, card reader device etc.).

Co-funded by the Erasmus+ Programme of the European Union. This project has been funded with support from the European Commission. This publication reflects the views only of the author and the Commission cannot be held responsible for any use which may be made of the information contained therein. Project number: 10101 18001 44020 101 000017

CYBER.EU.VET_Common authentication methods.mp4 2 of 2
00:14 / 01:20

WHAT IS AUTHENTICATION?

The process of authentication in the context of computer systems means assurance and confirmation of a user's identity.

Before a user attempts to access information stored on a network, they must prove their identity and permission to access the data.

Co-funded by the Erasmus+ Programme of the European Union. This project has been funded with support from the European Commission. This publication reflects the views only of the author and the Commission cannot be held responsible for any use which may be made of the information contained therein. Project number: 10101 18001 44020 101 000017

CYBER.EU.VET_Authentication.mp4 1 of 2
0:05 / 0:40

COFAC / UNIVERSIDADE LUSÓFONA (PT)

GAME JAM

ATTIVITÀ

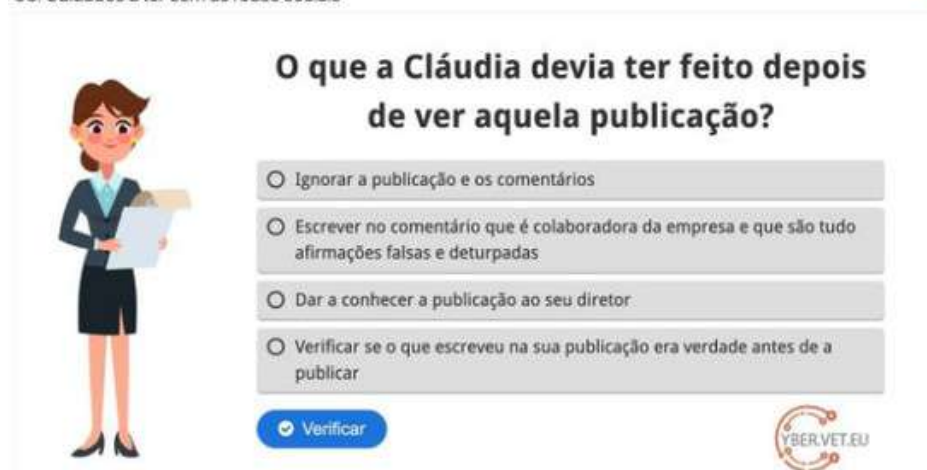
- 1) Cyber & Ethical Hacking post-laurea per futuri professionisti e docenti di mercato
Ott 2021 - Feb 2022 (in collaborazione con una società di consulenza locale denominata Cybersec)
- 2) 2 sessioni GameJam erogate a gennaio 2022 presso le scuole VET:
Escola de Comércio de Lisboa - <https://escolacomerciolisboa.pt>
Escola Profissional Almirante Reis - <https://www.epar.pt>
- 3) Un cybertraining di tre mezza giornate per gli studenti delle scuole superiori nel marzo 2022:
Università Lusofona nell'ambito dell'evento Tecweb - <https://tecweb.ulusofona.pt>

RISULTATI

Rapporto di diffusione delle prove in cui è possibile vedere i diversi test che sono stati effettuati durante un anno solare (da aprile 2021 ad aprile 2022). In questo rapporto possiamo vedere screenshot di pubblicazioni sui social network, poster di diversi eventi, questionari sulla consapevolezza della sicurezza informatica (disponibili in lingua portoghese su https://docs.google.com/forms/d/e/1FAIpQLSeXACV_oepIRpTfbaC1NFKED76kRSYD6cT8cFMKjc7ohGMHZw/viewform).

Durante i Cyberjams, è stato anche creato, sulla base dei sondaggi sulla consapevolezza della sicurezza informatica, una serie di mini-giochi intuitivi/interattivi su semplici situazioni fatte.

06. Cuidados a ter com as redes sociais



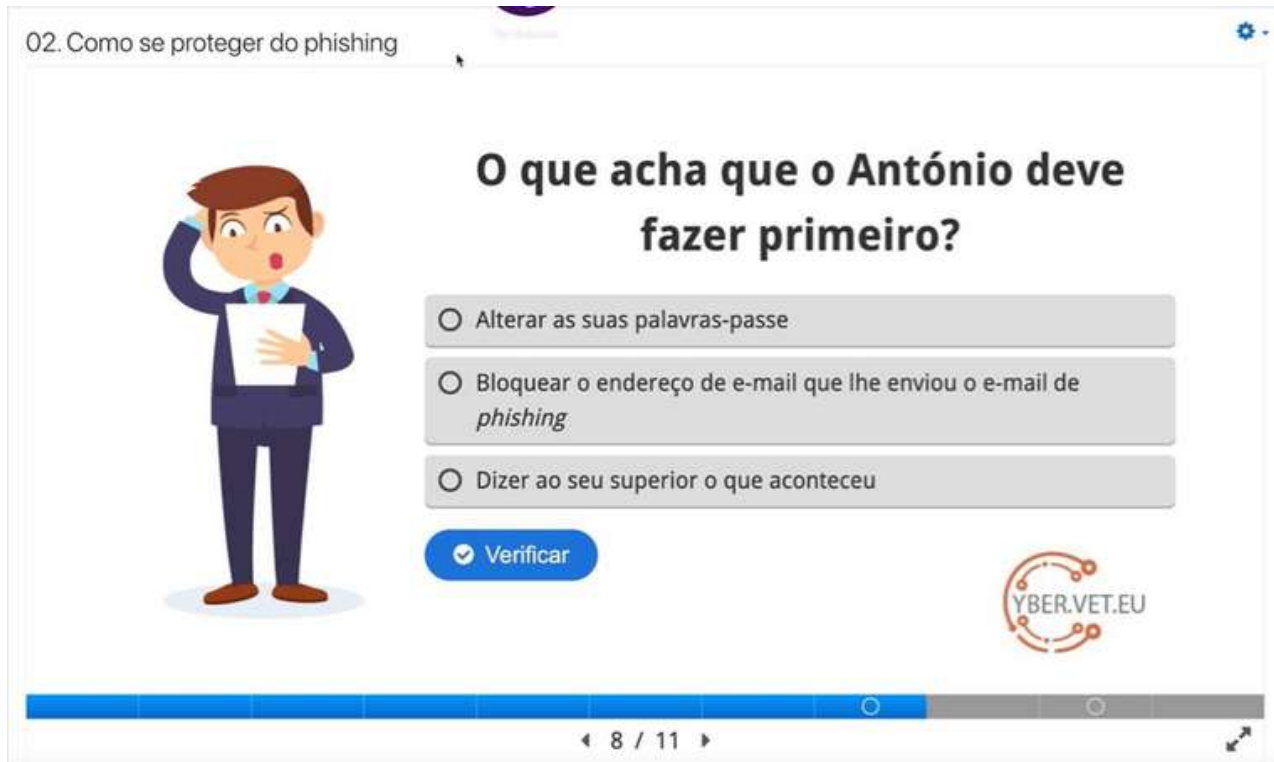
O que a Cláudia devia ter feito depois de ver aquela publicação?

- Ignorar a publicação e os comentários
- Escrever no comentário que é colaboradora da empresa e que são tudo afirmações falsas e deturpadas
- Dar a conhecer a publicação ao seu diretor
- Verificar se o que escreveu na sua publicação era verdade antes de a publicar

Verificar

YBER.VET.EU

COFAC / UDL (PT)



Inoltre, i partner hanno organizzato alcune sessioni per sensibilizzare i partecipanti sull'argomento scelto e hanno anche organizzato un evento moltiplicatore in cui hanno presentato tutti i materiali ei contenuti creati.



TANDEM PLUS NETWORK – MEMBER IASIS [GR]

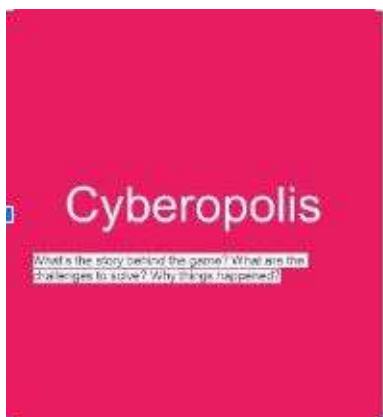
GAME JAM

Strumento di progettazione del gioco (IASIS) - Cyberopolis

Questo gioco è un gioco da tavolo rivolto a persone interessate alla sicurezza informatica, con un massimo di 2-4 giocatori, e i suoi aspetti principali sono la riservatezza dei dati e l'integrità dei dati... mentre i temi che tratta sono malware, phishing, attacchi web-based, attacchi alle applicazioni Web, spam, furto di identità, DDoS e Man in the middle...

Guarda l'immagine di "Cyberopolis" per capire meglio i passi da seguire durante il gioco e quali sono le sfide da risolvere...

Screenshot del gioco durante la sessione di GameJam dove possiamo vedere il successo del gioco e il grande interesse mostrato dai partecipanti.



- You need to conquer cyberopolis and buy its cybersecurity assets
- Become the Cyber Lord
- Be careful of cyber security threats
- Gather all Bitcoins
- Make the other players go bankrupt



TANDEM PLUS NETWORK – MEMBER IASIS [GR]

VIDEO - Prevenire il cyberbullismo

Questo video sviluppato dal partner greco avvicina i visitatori ai diversi modi per prevenire e combattere il cyberbullismo.



DISCLAIMER

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

Design

NGO Nest Berlin e.V.
Berlino, 2022

