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

MELHORAR A PREPARAÇÃO PARA A CIBERSEGURANÇA DO SETOR EUROPEU DO ENSINO E FORMAÇÃO PROFISSIONAL

CYBER.EU.VET

RESULTADO INTELECTUAL IO 3

TOOLKIT DE FORMAÇÃO DE FORMADORES

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

Introdução

Os parceiros do projeto CYBER.EU.VET elaboraram este toolkit para formação de formadores composto por 6 módulos + materiais para serem utilizados por professores e formadores no setor do EFP. Cada módulo abrange uma parte teórica, exemplos práticos e tarefas para trabalho em grupo. O formato de formação é aberto para ser utilizado em diferentes países europeus e deverá ser adaptado às necessidades e condições locais sempre que apropriado. Os ajustes podem estar relacionados principalmente com os exemplos práticos e estudos de caso fornecidos pelo formato de formação.

OS MÓDULOS DE FORMAÇÃO FORAM DESENVOLVIDOS PELOS PARCEIROS DA SEGUINTE FORMA:

CIBERATAQUES

Módulo 1

1. Visão geral do módulo

Grupo-alvo

- Educadores e formadores EFP
- Alunos
- Representantes ou organizações ou iniciativas relevantes (ONG, autoridades nacionais e regionais, instituições de ensino)

Descrição do módulo

Considerando o crescente número e a escala de ciberataques todos os anos, especificamente à luz dos últimos eventos económicos, políticos e sociais (consequências das restrições da Covid-19 e do conflito militar na Ucrânia, etc.), é importante discutir os ciberataques reais mais frequentemente.

Portanto, o objetivo da palestra é fornecer uma compreensão fundamental dos ciberataques e aprender a reagir a possíveis incidentes.

O conteúdo deste módulo abrange os seguintes aspetos (unidades):

- Definição e questões relevantes
- Tipologia
- Os incidentes mais reais (exemplos práticos)
- Como se proteger contra ciberataques e como reagir a incidentes

No fim de cada unidade está prevista uma atividade prática.

Objetivos de aprendizagem

- Fornecer uma compreensão fundamental de questões relacionadas com ciberataques.
- Compreender as consequências e impactos dos ciberataques e ameaças potenciais.
- Reconhecer e classificar as formas mais comuns de ciberataques.
- Saber como reagir aos ataques – onde reportar, caso ocorra algum incidente.
- Assegurar fontes de informação e literatura para uma aprendizagem mais aprofundada com vista a acompanhar ciberataques reais e para formas de proteção.

Duração total

Máx 1,5 h

CIBERATAQUES

Módulo 1

Este módulo será ministrado pelo formador sob a forma de uma apresentação PowerPoint partilhando conhecimentos teóricos acompanhados por mais elementos visuais, exemplos práticos e exercícios (máx. 20 minutos + uma atividade prática por cada unidade).

Recomenda-se que as apresentações sejam elaboradas nos modelos de PPT personalizados para o projeto CYBER.EU.VET. Considerando os rápidos desenvolvimentos e evolução no campo da cibersegurança, recomenda-se rever continuamente as unidades e, se necessário, ajustar os conteúdos tendo em conta os desenvolvimentos mais recentes no terreno.
Além disso, recomenda-se que os formadores adaptem este módulo às necessidades do seu EFP local e incluam exemplos de incidentes atuais na região. Este módulo abrange principalmente exemplos práticos da Letónia, assim como alguns exemplos internacionais. Recomenda-se um maior foco na Unidade 3 para analisar e discutir exemplos práticos de incidentes, juntamente com fotos e vídeos.

Unidade 1 - Ciberataques

O que significam? Introdução ao tópico

Definição e significado

Ciberataque (pl. ciberataques) = uma tentativa de obter acesso ilegal e não autorizado a um computador ou sistema informático com o objetivo de causar danos no mesmo. O objetivo é desativar, interromper, destruir ou controlar sistemas informáticos ou alterar, bloquear, excluir, manipular ou roubar dados contidos nestes sistemas.
Com o aparecimento das restrições da Covid-19 e a necessidade de passar para um formato digital de trabalho e aprendizagem, o número de ciberameaças e ciberataques aumentou e a proteção digital tornou-se mais importante.
O termo "ciberataque" está estreitamente relacionado com termos como "ciberameaça" (possibilidade de ocorrer um determinado ataque) e "ciber-risco".
Os ciberataques mais comuns: ataque de malware, ataque de phishing, ataque man-in-the-middle, ataque de palavra passe, ataque de denial of service e muitos mais.
Tipos de comunicação dos atacantes: contactos pessoais, telefone, correio eletrónico, malware.

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

CIBERATAQUES

Módulo 1

Quem pode realizar ciberataques?

Um ciberataque pode ser lançado a partir de qualquer ponto do mundo por qualquer indivíduo ou grupo utilizando uma ou mais estratégias de ataque diferentes e pode ser direcionado para indivíduos, empresas públicas ou privadas.

Por que acontecem os ciberataques e o que podem provocar?

Os ataques no ambiente virtual estão geralmente relacionados com o roubo de identidade, aquisição de recursos informáticos, roubo e falsificação de informações, acesso a segredos comerciais, chantagem ou difamação. Os ciberataques são concebidos principalmente para obter ganhos financeiros (por exemplo, roubo de números e códigos de cartão de crédito), interrupção e vingança (por exemplo, para prejudicar a reputação de uma organização)

Por exemplo, crises como a Covid-19 ou o conflito militar na Ucrânia são utilizadas para atrair a atenção dos utilizadores em e-mails fraudulentos e anúncios nas redes sociais.

E**STATÍSTICAS**

O trabalho remoto forçado pela pandemia aumentou obviamente os riscos de cibersegurança e facilitou novos tipos de incidentes. A maioria destes também é relevante para instituições de ensino e deve ser tido em conta em atividades educativas e de formação para educadores e jovens.

De acordo com informações analisadas pela Deloitte, ocorreram 350 ciberataques em abril de 2020 na Suíça, em comparação com uma média de 100 a 150 ciberataques (phishing, sites fraudulentos, ataques diretos a empresas, etc.).

O aumento do trabalho remoto exige um maior foco na cibersegurança devido à maior exposição ao ciber-risco. Isto fica claro, por exemplo, pelo facto de 47% das pessoas serem vítimas de um gople de phishing quando trabalham em casa.

Na Letónia, por exemplo, o maior número de endereços IP únicos ameaçados na Letónia foi detetado entre fevereiro e abril de 2020, quando a pandemia de Covid-19 começou (mais de 10.000 por mês), de acordo com o CERT.LV (a Instituição de Resposta a Incidentes de Segurança de Tecnologias da Informação da Letónia) que publica mensal e anualmente dados e a visão geral dos incidentes mais relevantes denominados “Kiberlaikapstākļi” (Cyber Weather).

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

Atividade de aprendizagem #1 - Atividade prática

Discussão com os participantes sobre as respetivas experiências em ciberataques (10-15 min):

1) Que tipo de ciberataques conhece?

2) Já sofreu ou algum dos seus familiares/amigos já sofreram um ciberataque/ciberincidente? Como acabou?

Unidade 2 - Tipos de ciberataques

Atividade de aprendizagem #2 - Teoria

Os métodos (tipos) mais comuns de ciberataques:

Malware é um software malicioso (worms, vírus) que é utilizado para danificar os dispositivos (computadores, telefones, etc.) ou a rede do utilizador. Exemplos de malware: Spyware e Trojans, Worms, Vírus, Adware, Spam. Dependendo do tipo de código malicioso, o malware pode ser utilizado por hackers para roubar ou copiar secretamente dados confidenciais, eliminar dados, bloquear o acesso a ficheiros, interromper as operações do sistema ou tornar os sistemas inoperáveis [DigiCERT].
O malware é disseminado principalmente com duas finalidades - obter informações (espiar dados de encaminhamento de malware do dispositivo da vítima) ou obter lucros (encriptar ransomware que encripta dados no dispositivo do utilizador e, posteriormente, pede-se um resgate ao utilizador) [Relatório CERT 2020]

Phishing ou Golpes com Dados Pessoais – um método no qual um hacker envia um e-mail aparentemente legítimo pedindo aos utilizadores que divulguem informações confidenciais. Os destinatários são induzidos a descarregarem o malware contido no e-mail abrindo um ficheiro anexado ou um link incorporado. Geralmente, são sites que se parecem com empresas reais e os utilizadores têm de inserir as suas informações pessoais (conta bancária, números de cartão de crédito e palavras-passe, inclusive os dos serviços de autenticação). O golpe de dados pode ser realizado também por ligação telefónica ou através de mensagens do WhatsApp [Investopédia]

Denial of Service (DoS) – os hackers bombardeiam os servidores de uma organização com grandes volumes de pedidos de dados simultâneos até que o alvo não consegue responder ou "crasha", tornando os servidores incapazes de tratar pedidos legítimos. Como resultado, o acesso ao serviço não é possível para os utilizadores do sistema. Os ataques DoS podem durar entre algumas horas a muitos meses e podem custar às empresas tempo e dinheiro enquanto os seus recursos e serviços estiverem indisponíveis [Investopédia]

Man-in-the-Middle – os atacantes inserem-se secretamente entre duas partes, por exemplo, um utilizador de computador particular e uma instituição financeira. Dependendo dos detalhes do ataque real, este tipo de ataque pode ser classificado mais especificamente como ataque man-in-the-browser, ataque monster-in-the-middle ou ataque machine-in-the-middle. Neste caso, o atacante interceta, elimina ou modifica os dados à medida que são transmitidos numa rede por um computador, smartphone ou qualquer outro dispositivo conectado [Investopédia, TechTarget]

Atividade de aprendizagem #2 - Atividade prática

de

Discussão em grupo - que tipo de recursos indicam sobre mensagens ataque/fraudulentas? (10 -15 min)

Os participantes têm 10 minutos para escreverem as características.

Discussão sobre os resultados.

Unidade 3 - Exemplo de ameaças e ataques

Como identificar ameaças?

Atividade de aprendizagem #3 - Teoria

Exemplos de ciberataques (à luz da guerra na Ucrânia)

E-mails fraudulentos em inglês a pedir apoio para uma das partes do conflito militar entre Ucrânia ou Rússia. O apoio pode ser demonstrado comprando votos e votando desta forma é uma fraude que visa roubar os dados do cartão de pagamento dos utilizadores(ver o print screen)

VÍDEO – Como os golpistas estão a sequestrar as doações de solidariedade para a guerra da Ucrânia - BBC News

ARTIGO – 4 tipos de golpes da guerra Rússia-Ucrânia direcionados aos consumidores

Exemplos baseados nos principais incidentes na Letónia (2020-2021) e outros exemplos internacionais (seguidos por exemplos visuais)

Malware

A situação da Covid-19 foi utilizada para disseminar tentativas de malware: por exemplo, e-mails em nome da Organização Mundial da Saúde (OMS) que indicavam que o ficheiro incluía as informações mais recentes sobre a Covid-19; links para gráficos que mostravam a propagação da Covid-19, cuja funcionalidade era roubar dados do utilizador, e-mails maliciosos para instituições de saúde sobre entrega de equipamentos de proteção Covid -

CIBERATAQUES

Módulo 1

A disseminação do Emotet, o malware mais perigoso do mundo, tanto em redes globais como letãs, visa roubar informações confidenciais e, geralmente, tem origem num e-mail de um contacto já infetado. O Emotet funciona como um abre portas para outros computadores, permitindo o acesso não autorizado a outras famílias de malware. Mais de 200 empresas letãs foram infetadas.

Phishing ou Golpes com Dados Pessoais

A maioria dos casos visava a fraude de e-mail e dados do Office 365, aquisição de banco,sistema de pagamento internacional (incluindo Smart-ID - ferramenta de autenticação eletrónica na Letónia), dados de acesso e fraude de dados de acesso a contas em redessociais populares (Facebook e Instagram). O tema Covid-19 era frequentemente utilizado para atrair a atenção dos utilizadores em e-mails fraudulentos e anúncios nas redes sociais.

Durante a pandemia, foram observadas tentativas intensificadas de fraude de dados com recurso às marcas de fornecedores de serviços de entrega de encomendas (Latvijas Pasts, DHL, Omniva, DPD, AliExpress, etc.). Também foram observados ataques inovadores, por exemplo, um ataque aos direitos de acesso do Office 365 que era difícil de detetar por meios técnicos, pois não era realizada qualquer ação maliciosa no dispositivo da vítima, mas os ataques eram feitos no Office 365.

VIDEO Phishing (com legendas em inglês)

Fraude

Tentativas de fraude intensivas, incluindo ataques de engenharia social. A maioria das fraudes visava obter dados de acesso a cartões de pagamento, recursos financeiros, assim como dados de acesso a e-mail dos cidadãos. Os atacantes enviaram e-mails e mensagens de texto fraudulentas à população e como fizeram ligações telefónicas fraudulentas, na maioria das vezes, fazendo-se passar por representantes de bancos ou fornecedores de serviços de e-mail. Várias empresas sofreram interferências comerciais (BEC), registando um prejuízo total de quase 200.000 euros.

A questão da entrega de bens também esteve presente nas tentativas de fraude contra vendedores que publicavam informações sobre a venda de bens em portais de publicidade. Fingindo serem compradores interessados e utilizando a plataforma de comunicação WhatsApp, os defraudadores expressavam o desejo de comprar o produto, como se estivessem a utilizar os serviços de uma empresa de entregas, e pediam aos vendedores que inserissem as informações do cartão nos sites falsificados Omniva, DPD e posteriorme nte Latvijas Pasts com vista a revelar o código CVV e o saldo.

Os atacantes utilizaram endereços de sites personalizados (domínios) semelhantes aos

Os atacantes também tentaram obter informações do cartão de pagamento enviando e-mails a pedir-lhes que solicitassem um saldo de Bitcoin, inscrevendo-se num serviço fraudulento de câmbio de criptomoedas.
As tentativas mais ativas foram campanhas de extorsão, nas quais as hackers alegaram ter hackeado o dispositivo de um utilizador e obtido material comprometedor para o qual foi definido um resgate; lotarias fraudulentas em nome de marcas conhecidas, oferecendo-se para ganhar os mais novos smartphones ou outros prémios valiosos.

OUTROS EXEMPLOS

Anúncios enganadores nas redes sociais – utilizando os nomes de letões famosos sem o seu conhecimento, os internautas foram convidados a investir em criptomoeda. Os golpistas também faziam chamadas telefónicas e tentavam persuadir as pessoas a investirem. Em alguns casos, foram observadas repetidas tentativas fraudulentas nas que as vítimas de fraude financeira receberam ajuda para recuperar os seus recursos perdidos.

Fraudes telefónicas – falsificando os números de telefone de diferentes instituições de crédito e fazendo-se passar por representantes bancários, os golpistas, usando o pouco conhecimento do público sobre métodos adicionais de autenticação, defraudaram recursos financeiros de vários milhares de utilizadores, causando perdas totais no valor de centenas de milhares de euros a instituições de crédito letãs.

Os hackers também estão a adaptar-se à disseminação do trabalho remoto: considerando a necessidade de as empresas passarem rapidamente para a situação de trabalho remoto e a implementação da circulação de documentos eletrónicos, os hackers aproveitam esta situação para adaptarem os seus ataques
- por exemplo, vários contabilistas de empresas receberam e-mails em nome do diretor ou de outro funcionário para fazerem um pagamento urgente ou alterarem a conta da folha de pagamentos.

Letónia e Lituânia detêm 108 pessoas por um esquema multimilionário num call center

Interferência na correspondência comercial das empresas – comprometendo os emails das empresas ou dos seus parceiros, os atacantes escolhem um momento adequado para enviar a uma das partes uma fatura com uma conta alterada.

Mensagens fraudulentas – os atacantes tentam intercetar as contas de WhatsApp solicitando, por engano, que se envie um código de seis dígitos para o número de telefone do destinatário. Como se recebe uma mensagem das pessoas que fazem parte da sua lista de contactos, algumas pessoas transferem os seus códigos, perdendo o acesso à respetiva conta do WhatsApp. O recurso a autenticação de dois fatores seria um meio de proteção contra um ataque desses.

.

EXEMPLO Quando o utilizador partilha o código de dígitos com o hacker (ver print screen e artigo)

EXEMPLO SMS do banco local com um link fraudulento (exemplo com SMS do banco SEB).

Emails fraudulentos – os defraudadores fingem ser uma agência postal nacional (Latvijas Pasts) e pedem que as pessoas paguem pela entrega de uma remessa supostamente atrasada. O link fornecido no e-mail leva a um site falso para dados de cartão de pagamento fraudulentos (ver o print screen).

Lojas online falsas – observou-se uma atividade especificamente alta durante a época de férias através de anúncios nas redes sociais e devido às restrições da Covid-19 que forçaram as empresas a venderem os seus produtos online.

EXEMPLOS Os golpistas atraem os utilizadores do AliExpress para lojas online falsas (imagem e caso de golpe); Como reconhecer um golpe

Golpes românticos - os golpistas aproveitam-se de pessoas que procuram parceiros românticos, geralmente através de sites, aplicações ou redes sociais de encontros, fingindo serem possíveis companheiros. Recorrem a gatilhos emocionais para fazerem com que as pessoas forneçam dinheiro, presentes ou informações pessoais.

EXEMPLO História de investigação sobre Golpes Românticos [por North Lab]

Ataques de denial-of-service (DoS e DDoS)

Registaram-se ataques DDoS contra instituições públicas e municipais (por exemplo, Biblioteca Nacional, Centro de Sistemas de Informação Cultural, etc.) Ataques DDoS prolongados perturbaram uma escola. Receberam-se relatórios semelhantes de outras instituições de ensino no início do ano letivo. As instituições de ensino noutras zonas da Europa também estão a enfrentar estes desafios.

Tanto na Europa como na Letónia, os seguintes incidentes tornaram-se atuais - tentativas de extorsão de dinheiro visando principalmente instituições financeiras ou empresas do setor privado (os atacantes realizaram uma série de ataques experimentais, ameaçando suspender a operação de sites de empresas ou outros recursos através de ataques de até 2 Tb/s).

OUTRAS TENDÊNCIAS

Dispositivos comprometidos e fugas de dados

Os comprometimentos de equipamentos podem afetar indivíduos, empresas e instituições estatais e municipais. Isto pode acontecer através de um e-mail já comprometido ou da infeção de um dispositivo através da abertura de anexos ou links de contactos aparentemente familiares, como colegas e parceiros comerciais; também pode acontecer através de sites comprometidos, por ex. através de um plug-in desatualizado ou de um sistema de gestão de conteúdos desatualizado.

Como aconteceu em 2020-2021, quando várias instituições nacionais perderam temporariamente o acesso às suas contas nas redes sociais quando atacantes assumiram o controlo de um dos perfis dos administradores da conta. Apresentaram-se relatórios sobre invasões de reuniões Zoom e MS Teams, como resultado do pouco conhecimento das medidas de segurança disponíveis (ou seja, sala de espera, acesso limitado do estrangeiro, etc.).

Tentativas de intrusão (qualquer ataque que vise comprometer os objetivos de segurança de uma organização) - após o aumento da atividade de trabalho remoto de bots em busca de dispositivos vulneráveis, configurados inadequadamente e/ou palavras-passe fracas para dispositivos ligados a uma rede (dispositivos emitidos à pressa pelo empregador, portáteis pessoais que começaram a ser utilizados para trabalhar, assim como serviços RDP mal protegidos com palavras-passe fracas) aumentaram significativamente.

VÍDEO Exemplos de intrusão

Mais sobre a deteção da intrusão

FONTE CERT.LV e “Kiberlaikapstākļi” (Cyber Weather); Investopédia

- Elementos adicionais

NOTA Equacionar igualmente discussões sobre outros métodos de informações falsas e fraudulentas, como deepfake e outros.

Atividade de aprendizagem #3 - Atividade prática

No fim da unidade, organiza-se um teste Kahoot no qual os participantes têm de detetar se as informações fornecidas são fraudulentas e têm de identificar o tipo (método) de ciberameaç a.

Unidade 4 - O que fazer em caso de incidente?

Prevenção e como se preparar.

Atividade de aprendizagem #4 - Teoria

ALGUMAS DICAS E TRUQUES PARA PROTEÇÃO

Verifique sempre os seus e-mails cuidadosamente e fique atento a: anexos ou links incorporados de fontes ou remetentes desconhecidos/suspeitos; mensagens urgentes que solicitam que descarregue algo ou execute alguma outra tarefa; ofertas com uma promessa de recompensa que parece boa demais para ser verdade.

VÍDEO Clicker (Spaidonis) com legendas em inglês

Preste atenção à ortografia do endereço URL. Os sites de phishing geralmente utilizam endereços da Web semelhantes a um site oficial, mas contêm um erro ortográfico simples, como substituir um "1" por um "l". Ortografia incorreta ou estranha é um sinal indicativo de possível golpe.
Utilize uma palavra-passe forte e diferente para os seus dispositivos, contas de e-mail e contas de redes sociais. Para mais dicas, consulte o módulo CYBER.EU.VET sobre palavras-passe (Módulo 4).

CIBERATAQUES

- Sempre que possível, ajuste as suas definições para utilizar a autenticação multifatores nos seus dispositivos. Por exemplo, palavra-passe e identificação facial ou impressão digital no seu telefone; O Gmail, por sua vez, possui uma destas definições na qual quando um utilizador faz login num novo dispositivo, após inserir o seu nome de utilizador e palava-passe, ele recebe um pedido para confirmar a sua identificação noutro dispositivo, geralmente, um telefone.
- Verificação em duas etapas no WhatsApp (para utilizadores de Android).
- Não realize transações confidenciais numa rede Wi-Fi pública não segura em cafés e noutros locais públicos idênticos.
- Certifique-se de que, pelo menos, os dados mais importantes no seu dispositivo têm uma cópia de backup (em armazenamento na nuvem ou num dispositivo externo).
- Certifique-se de que consegue restaurar os dados necessários dos backups e descubra quanto tempo demora.
- Atualizações de software – é crucial seguir as atualizações de software e instalá-las imediatamente. Mesmo um atraso de um único dia pode ser crucial.
- Utilize um VPN. As redes privadas virtuais adicionam uma camada adicional de proteção à utilização da Internet em casa. Não se pode confiar unicamente nelas para prevenir os ciberataques, mas podem ser uma barreira útil contra os ciberataques.
- Acompanhe regularmente as notícias no mundo dos ataques e tente pensar que os eventos globais, nacionais e locais, tanto políticos como económicos e também aqueles relacionados com o sofrimento global (pandemias, conflitos militares) podem ser utilizados como tema/"capa" para possíveis ciberataques.
- Adicional (em letão): CERT.LV Recomendações do CERT.LV face ao agravamento da situação geopolítica e aumento das ciberameaças na Europa: https://cert.lv/lv/2022/02/cert-lv-ieteikumi-saasinoties-geopolitiskajai-situacijai-eiropa-un-pieaugot-kiberdraudiem

Onde reportar uma ciberameaça ou incidentes

- O seu local de trabalho, instituição de ensino - envie screenshots, fotos ou vídeos para a pessoa relevante na sua instituição (por exemplo, departamento de TI). Avise os seus colegas e amigos.
- Instituições que apoiam o ciberespaço nacional (caso da Letónia)
- CERT.LV (apoio na resolução de incidentes, monitorização do ciberespaço, avisos),
- Instrução sobre como encaminhar e-mails fraudulentos (em letão)
- Polícia
- Centro de Internet Mais Segura da Letónia (violações e conteúdos ilegais na Internet)

FONTES DE INFORMAÇÃO E CASOS REAIS

Para acompanhar as notícias sobre cibersegurança e ciberameaças, **leia regularmente recursos locais ou internacionais:**
https://portswigger.net/daily-swig/cyber-attacks
https://www.euronews.com/tag/cyber-attack
OUCH! Newsletters - a principal newsletter gratuita sobre segurança concebida para todos.

Links para a Letónia (existe alguma informação disponível em inglês):
https://www.esidross.lv/
https://cert.lv/lv/ (incluindo, "Cyber Weather "(Kiberlaikapstākļi), instrução sobre como encaminhar emails fraudulentos (em letão)
https://drossinternets.lv/

Atividade de aprendizagem #4 - Atividade prática

Discussão com os participantes: avaliação da utilidade do curso (atividade de 5-10 min)

2. Resultados de aprendizagem para o módulo

Conhecimentos

- Os alunos terão uma compreensão básica sobre as principais questões de ciberataques.
- Os alunos terão uma visão geral dos incidentes reais (à luz dos eventos globais).
- Os alunos saberão quais as fontes de informação a seguir para avisos e atualidades sobre ameaças.

Competências

Os alunos serão capazes de identificar e classificar tipos comuns de ciberameaças e explicá-las.

Aptidões

- Os alunos serão capazes de reconhecer uma possível ciberameaça e saber onde reportar a ameaça.
- Os alunos serão capazes de selecionar ferramentas e técnicas básicas para se protegerem contra ciberataques.

3. Bibliografia

CERT.LV (Instituição de Resposta a Incidentes de Segurança de Tecnologias da Informação): https://cert.lv/lv

Exemplos de phishing Covid-19: 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

Instituições de Resposta a Incidentes de Segurança de Tecnologias da Informação, (2021), CERT.LV Relatório Anual 2020: https://cert.lv/uploads/parskati/CERTLV-annual-report-2020_ENG.pdf

Relatório informativo, Estratégia de cibersegurança da Letónia 2019-2022 (apenas em letão): https://www.mod.gov.lv/sites/mod/files/document/kiberstrategija.pdf

Centro de Internet mais Segura da Letónia (Projeto-plataforma "Drossinternets.lv"): https://drossinternets.lvLIKTA (Latvian Information and Communication Technologies Association): https://likta.lv/digitalas-parmainas-izglitiba/

Li, Y., Liu, Q (2021), A comprehensive review study of cyber-attacks and cyber security;

Emerging
trends and recent developments, Science Direct, Vol. 7, p. 8176-8186: https://www.sciencedirect.com/science/article/pii/S2352484721007289

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

Prat, M.K. (2021), Cyber-attack – definition: https://www.techtarget.com/searchsecurity/definition/cyber-attack

Simplilearn, Curso Completo de Cibersegurança 2022: https://youtu.be/yr1Psapupsc

CERT.LV (2022), IT drošības seminārs "Esi drošs" martā (in Latvian): https://cert.lv/lv/2022/02/it-drosibas-seminars-esi-dross-marta#Sanita_Vitola

Esi Drošs (2022), Kiberuzbrukuma riskam pakļauts ikviens interneta lietotājs (in Latvian): https://www.esidross.lv/2022/02/10/kiberuzbrukuma-riskam-paklauts-ikviens-interneta-lietotajs/

1. Visão geral do módulo

Grupo-alvo

- Educadores EFP
- Alunos
- Representantes de instituições públicas que atuam nos setores educativos: municípios, autoridades regionais e nacionais

Descrição do módulo

Hoje em dia, as pessoas passam muito tempo em frente a um ecrã. Os jovens estão a crescer num mundo onde as novas tecnologias são necessárias e o principal meio de comunicação que utilizam é a Internet. Estar nas redes sociais, por exemplo, oferece muitas vantagens, mas também muitos riscos. Existem muitas pessoas que foram intimidadas ou estão a ser intimidadas. Na maioria dos casos, não estavam conscientes disto ou dos problemas que isto pode causar nas suas vidas. Por este motivo, gostaríamos de utilizar este módulo para compreender o que é o cyberbullying e como o podemos prevenir.

Objetivos de aprendizagem

Compreender o que é o ciberbullying
Saber como o detetar
Efeitos do Ciberbullying
Compreender as principais consequências
Fornecer técnicas para prevenir e lidar com o ciberbullying

Duração total

2 horas

Unidade 1 - Como detetar o ciberbullying

Quais são os efeitos?

Esta Unidade será ministrada pelo formador sob a forma de uma apresentação PowerPoint cujo objetivo é a partilha de conhecimentos teóricos acompanhados de elementos mais visuais - pequenos vídeos e casos reais de ciberbullying que resumem a informação dos slides PowerPoint (máx. 30 minutos).
Recomenda-se que as apresentações sejam elaboradas nos modelos de PPT personalizados para o projeto CYBER.EU.VET.

Atividade de aprendizagem 1

O formador faz uma apresentação aos alunos com os seguintes conteúdos sugeridos (máx. 30 minutos):
O ciberbullying, embora frequentemente associado ao cyberstalking, é um problema muito sério por si só e cuja prevalência tem vindo a aumentar nos últimos anos.
Como detetar o ciberbullying?
O ciberbullying pode ser **difícil de reconhecer** porque acontece à porta fechada ou num telefone/computador particular.
Aqui estão alguns dos sinais mais comuns de que alguém pode ser vítima de ciberbullying:

- Fica anormalmente chateado se não consegue utilizar o computador ou telefone ou
- depois de utilizar o computador.
- Muda rapidamente os ecrãs ou fecha programas quando alguém passa.
- Evita discussões sobre o que está a fazer no computador.
- Afastamento da família ou de amigos.
- Relutância em participar em atividades de que anteriormente gostava
- Declínio inexplicável no desempenho académico.
- Recusa-se a ir à escola.
- Relata cada vez mais sintomas de doença.
- Mostra sinais de depressão ou tristeza.

Os efeitos do ciberbullying podem ser devastadores para as vítimas. Podem sentir várias emoções negativas, como tristeza, raiva, frustração e humilhação. Podem também sentir-se isolados e sozinhos, como se não tivessem a quem recorrer.

As vítimas também podem sofrer academicamente, pois podem ter vergonha de ir à escola ou participar nas aulas. Em alguns casos, as vítimas podem até pensar em suicídio.
O cyberbullying também pode ter efeitos adversos naqueles que testemunham quando acontece com outra pessoa. Podem sentir-se assustados, desamparados e tristes. Podem também ter problemas para dormir e comer e podem até desenvolver ansiedade e depressão.

Efeitos e consequências do ciberbullying:

Quando o bullying acontece online, pode parecer que está a ser atacado em todos os lugares, até mesmo dentro da sua própria casa. Pode parecer que não há escapatória. Os efeitos podem durar muito tempo e afetar uma pessoa de várias formas:

Mentalmente: sentir-se chateado, envergonhado, estúpido, até com medo ou com raiva
Emocionalmente: sentir vergonha ou perder o interesse pelas coisas que adora
Fisicamente: sentir-se cansado (por perda de sono) ou sentir sintomas como dores de estômago e dores de cabeça

A sensação de ser ridicularizado ou assediado por outras pessoas pode impedir as pessoas de falarem ou tentarem lidar com o problema. Em casos extremos, o cyberbullying pode até levar as pessoas a tirarem a própria vida.

VÍDEO Words Hurt | Cyberbully Short Film

Efeitos:

- Doença
- Depressão
- Isolamento
- Raiva
- Humilhação

Atividade de aprendizagem 2

Discussão em grupo – Perguntas e respostas; Avaliação e Feedback (máx. 10 minutos)
Agora que conhece os sinais mais comuns de alguém que está a sofrer ciberbullying:

- Conhece alguém nesta situação?
- Conseguiria ajudar?

Unidade 2 - How to Prevent/Stop Cyberbullying

Atividade de aprendizagem 1

O formador faz uma apresentação aos alunos com os seguintes conteúdos sugeridos (máx. 30 minutos):

O ciberbullying é facilitado pelo acesso fácil a plataformas e dispositivos de media digitais. Muitas vezes, estes são utilizados sem qualquer supervisão. Isto faz com que o ciberbullying seja um problema incrivelmente difícil de resolver. Prevenir a prática exigiria imenso tempo e muitos recursos para monitorizar eficazmente cada interação online. Embora muitas vezes não seja viável para as pessoas livrarem-se completamente das ferramentas digitais, existem métodos que pais, alunos e educadores podem utilizar para combater o fenómeno e reduzir os seus efeitos nocivos.

Para os pais, uma forma eficaz de lidar com os danos resultantes do ciberbullying é simplesmente conversar sobre o assunto com os seus filhos.

Também é importante discutir a segurança online, a privacidade e a gestão das palavras-passe. Definir diretrizes sobre como os alunos devem comportar-se on-line e instruir os jovens para falarem com os seus pais sobre qualquer malefício que tenham sofrido com o bullying on-line ou no mundo real.

Os jovens podem ajudar a evitar serem vítimas de ciberbullying tendo cuidado com o que publicam. Devem evitar partilhar as suas palavras-passe e garantir que as suas definições de privacidade online as mantêm seguras.

Os alunos desempenham um papel importante na prevenção do ciberbullying. Se os jovens que conhecem os factos do ciberbullying perceberem que isso está a acontecer com outra pessoa, podem avisar um adulto de confiança. Também devem ser gentis, generosos e solidários com a criança que está a sofrer bullying. Professores, educadores e outros adultos de confiança devem unir-se aos pais e jovens no combate ao cyberbullying. Muitas vezes, estas pessoas conseguem detetar alterações no comportamento de uma criança e podem ajudar a resolver o problema antes de os pais o fazerem.

A tecnologia e a internet não são o problema. São as pessoas que o usam para prejudicar os outros que são o verdadeiro problema. Para tal, é importante ensinar os adolescentes a utilizarem as redes sociais com segurança e responsabilidade e a ter consciência de como agir, caso sofram ciberbullying.

O que deves fazer se estiveres a ser vítima de ciberbullying?

- NÃO RESPONDAS ou comentes a mensagem do ciberbully.
- BLOQUEIA as pessoas envolvidas.
- Faz LOG OFF do site onde está a acontecer o bullying.
- Protege as tuas PALAVRAS-PASSE e verifica os teus CONTROLOS DE PRIVACIDADE.
- GUARDA tudo. Faz um screenshot ou imprime o incidente como prova.
- DENUNCIA o ciberbullying: quase todos os sites de tecnologia têm a opção de denunciar alguém por ciberbullying.
- Conta a um ADULTO de confiança o que está a acontecer ou entra em contacto com as autoridades.

O que deves fazer se vires o ciberbullying a acontecer?

Conta aos teus pais ou a um adulto de confiança e pede conselhos.
Denuncia a situação ao fornecedor da tecnologia, aplicação ou rede social.
Se a situação envolver colegas, informa os teus professores.
Mostra o teu apoio à pessoa que está a ser intimidada, por exemplo, enviando-lhe uma mensagem simpática.

Tomar medidas legais: Tanto a calúnia como a difamação são crimes que podem resultar num julgamento.

Pede ajuda: É muito difícil lidar com o cyberbullying sozinho.

VÍDEO Emma's Story: Cyberbullied by a Best Friend

Como posso aprender?

- Organizações que podem ajudar: Existem muitas organizações por aí a partilhar informações sobre ciberbullying. Os sites a seguir estão a criar e a partilhar conteúdos úteis que são realmente úteis para qualquer pessoa ansiosa ou que esteja a sofrer ciberbullying.
- Blogues e podcasts: manter-se atualizado com blogues e podcasts que se centram no tópico é uma ótima forma de se manter atualizado e obter os conselhos ou perspetivas mais recentes.
- Livros.
- Apps e software: Existem inúmeros produtos por aí que permitem aos pais restringirem e/ou monitorizarem a atividade online dos seus filhos. Cabe a cada pai decidir se este tipo de monitorização é adequado com base na idade e hábitos de internet dos seus filhos. Alguns até procuram linguagem que possa ser intimidadora. Existem também empresas que fazem parcerias com escolas para permitir denúncias anónimas de incidentes de bullying.

Atividade de aprendizagem 2

Discussão em Grupo – Perguntas e Respostas; Avaliação e feedback (máx. 15 minutos)

Exercício de escrita:
Descreva uma situação em que sabe que está a acontecer ciberbullying.
Pode ser real ou fictícia.
Consegue ajudar? Como? Porquê ou por que não? Explique como se sente com isto.

2. Resultados de aprendizagem para o módulo

Conhecimentos

O aluno saberá como detetar o ciberbullying e como a vítima se sente e vive isso.
Ao compreenderem os factos do ciberbullying e conhecerem os métodos para o abordar, os jovens, adultos e educadores podem ajudar a criar um mundo digital melhor e mais empático.

Competências

O aluno compreenderá como reconhecer quando alguém está a sofrer ciberbullying.
O aluno será capaz de compreender qual o nível de resposta e apoio que é necessário, dependendo do cenário em questão.

Aptidões

- O aluno será capaz de reconhecer um episódio de cyberbullying e abordá-lo imediatamente utilizando as ferramentas adequadas.
O aluno será capaz de identificar qual é o melhor método de apoio e qual é o mais adequado ao caso em questão.

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/

Atividade de aprendizagem 2

Discussão em Grupo – Perguntas e Respostas; Avaliação e feedback (máx. 15 minutos)

Exercício de escrita:
Descreva uma situação em que sabe que está a acontecer cyberbullying.
Pode ser real ou fictícia.
Consegue ajudar? Como? Porquê ou por que não? Explique como se sente com isto.

2. Resultados de aprendizagem para o módulo

Conhecimentos

O aluno saberá como detetar o ciberbullying e como a vítima se sente e vive isso.
Ao compreenderem os factos do ciberbullying e conhecerem os métodos para o abordar, os jovens, adultos e educadores podem ajudar a criar um mundo digital melhor e mais empático.

Competências

O aluno compreenderá como reconhecer quando alguém está a sofrer ciberbullying.
O aluno será capaz de compreender qual o nível de resposta e apoio que é necessário, dependendo do cenário em questão.

Aptidões

O aluno será capaz de reconhecer um episódio de cyberbullying e abordá-lo imediatamente utilizando as ferramentas adequadas.
O aluno será capaz de identificar qual é o melhor método de apoio e qual é o mais adequado ao caso em questão.

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/

Atividade de aprendizagem 2

Discussão em Grupo – Perguntas e Respostas; Avaliação e feedback (máx. 15 minutos)

Exercício de escrita:
Descreva uma situação em que sabe que está a acontecer ciberbullying. Pode ser real ou fictícia.
Pode ser real ou fictícia.
Consegue ajudar? Como? Porquê ou por que não? Explique como se sente com isto.

2. Resultados de aprendizagem para o módulo

Conhecimentos

O aluno saberá como detetar o cyberbullying e como a vítima se sente e vive isso.
Ao compreenderem os factos do cyberbullying e conhecerem os métodos para o abordar, os jovens, adultos e educadores podem ajudar a criar um mundo digital melhor e mais empático.

Competências

O aluno compreenderá como reconhecer quando alguém está a sofrer ciberbullying.
O aluno será capaz de compreender qual o nível de resposta e apoio que é necessário, dependendo do cenário em questão.

Aptidões

O aluno será capaz de reconhecer um episódio de ciberbullying e abordá-lo imediatamente utilizando as ferramentas adequadas.
O aluno será capaz de identificar qual é o melhor método de apoio e qual é o mais adequado ao caso em questão.

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/

1. Visão geral do módulo

Grupo-alvo

- Educadores EFP
- Alunos
- Representantes de instituições públicas que atuam nos setores educativos: municípios, autoridades regionais e nacionais

Descrição do módulo

Este é um módulo de seguimento do "Ciberbullying. O que é isso? Como podemos detetá-lo?" e dotar os grupos-alvo de competências para a consciência do ciberbullying e para a disponibilização de técnicas de prevenção para não se tornarem vítimas de ciberbullying.

Objetivos de aprendizagem

Compreender a importância da prevenção
Disseminar a consciencialização sobre o ciberbullying
Sensibilizar para as técnicas de prevenção do ciberbullying

Duração total

1,5 h

Unidade 1 - Porquê prevenir o ciberbullying?

Esta Unidade será ministrada pelo educador como uma apresentação em PowerPoint que incluirá tanto material teórico como recursos mais visuais, tais como curtas-metragens e cenários reais de cyberbullying que irão resumir as informações dos slides de PowerPoint (20 a 30 minutos, respetivamente, em cada Unidade).
Recomendamos a elaboração de apresentações nos modelos de PPT personalizados para o projeto CYBER.EU.VET. A apresentação é seguida por uma discussão em grupo para que todos reflitam sobre a aprendizagem.

Atividade de aprendizagem 1

O formador faz uma apresentação aos alunos com os seguintes conteúdos sugeridos (máx. 20 minutos):

Prevenir ou intervir?

De acordo com a pesquisa, as pessoas que sofrem ciberbullying têm uma série de resultados negativos, incluindo dificuldades emocionais, físicas, mentais e académicas. Além disso, o ciberbullying é uma fonte significativa de stress para os jovens. As vítimas estão psicologicamente feridas, envergonhadas e, por vezes, com medo em resultado do ciberbullying. As vítimas não apenas se culpam pelo assédio e abuso de que são vítimas, mas também se sentem tremendamente ansiosas. Na verdade, mais de 35% das pessoas visadas por cyberbullies apresentaram sintomas de stress, de acordo com uma pesquisa. Este tipo de bullying pode ser particularmente prejudicial, pois, geralmente é muito público. Normalmente, muitas pessoas conseguem ver o que é escrito ou publicado. É difícil, se não impossível, apagar todos os vestígios de algo depois de publicado online. Isto significa que o bullying pode ser contínuo.

Quando as pessoas são assediadas com frequência por outras pessoas nas redes sociais através de mensagens de texto, mensagens instantâneas e publicações em blogues, podem começar a sentir-se sem esperança. Podem sentir que o suicídio é a única forma de parar o seu sofrimento. Como os perigos do ciberbullying são tão sérios, é fundamental que os educadores do EFP ensinem os seus ss[AB1] sobre este problema antes que o mesmo provoque danos reais. A prevenção reduz os riscos de exposição ao ciberbullying.

Atividade de aprendizagem 2

Discussão em grupo (máx. 10 minutos)

Pergunte aos seus alunos:
Por que a prevenção é tão importante no ciberbullying?
Já foi informado sobre o ciberbullying?
Como costuma informar-se sobre crimes de ciberbullying?

Unidade 2 - Sensibilização

Atividade de aprendizagem 1

O formador faz uma apresentação aos alunos com os seguintes conteúdos sugeridos (máx. 30 minutos):
É crucial discutir com os alunos a forma de utilizar as redes sociais com segurança e responsabilidade, detetando os criminosos de ciberbullying e aprendendo o que fazer forem intimidados online.
VÍDEO Cyberbullying - How to Avoid Cyber Abuse
PENSAR ANTES DE PUBLICAR
Os alunos devem criar o hábito de ler o seu trabalho antes de o publicar. Podem escrever a publicação na secção de notas do seu computador ou smartphone e voltar a lê-la algumas horas depois para decidir se publicam ou não. Como os cyberbullies podem usar o que publica contra si de alguma forma, terá menos tendência a dizer qualquer coisa de que se arrependerá mais tarde ou que possa ser utilizada contra si. É evidente que se alguém quiser utilizar algo contra si, irão esforçar-se para obter até mesmo as informações mais insignificantes, mas verificar antes de partilhar pode reduzir a gravidade do ciberataque.
Pensar antes de publicar pode ajudá-lo a manter um relacionamento saudável com as redes sociais.

CUIDADO COM OS DISPOSITIVOS PÚBLICOS
Os alunos também devem ter cuidado ao usar dispositivos públicos, como computadores de universidades ou bibliotecas, pois existem muitas formas de alguém tirar proveito disso. Existem muitas possibilidades de os dispositivos públicos serem infetados por programas maliciosos, como keystroke loggers (keyloggers).

Um keylogger, de acordo com a maioria das fontes, é uma aplicação de software que monitoriza e regista discretamente todas as teclas que são pressionadas. Estes keyloggers podem ser utilizados para intercetar palavras-passe e outras informações pessoais inseridas através do teclado, representando uma grande ameaça para os utilizadores, tal como entregar o acesso às suas contas de redes sociais a cibercriminosos. O mais importante a saber quando se trata de keyloggers é que muitas vezes eles não podem ser detetados por programas antivírus, pois existem muitos keyloggers legítimos disponíveis no mercado para fins de controlo dos pais, segurança de empresas, etc.

VÍDEO Could a Keylogger Be Spying on You?

Além de programas especializados de monitorização, também se deve recordar aos alunos que devem sair das suas contas, pois podem involuntariamente deixá-las abertas e disponíveis para aqueles que utilizarão os computadores ao seu lado.

PROTEÇÃO ONLINE

É fundamental utilizar palavras-passe fortes em todos os lugares quando se trata de combater o ciberbullying e outras atividades fraudulentas. Uma palavra-passe forte é uma palavra-passe que não pode ser facilmente adivinhada ou comprometida. Uma palavra-passe forte deve ser longa, conter uma combinação de números, caracteres especiais e letras maiúsculas/minúsculas e, em nenhuma circunstância, incluir informações óbvias como nome, data de nascimento, etc.

Ao proteger as suas contas, garante que ninguém tem acesso às mesmas.

O CIBERBULLYING DEVE SER DENUNCIADO.

Certifique-se de que os seus alunos compreendem a importância de denunciar o ciberbullying. Isto implica não apenas detetar os ciberbullies, mas também informar a plataforma de rede social, o fornecedor do serviço de Internet e quaisquer outras partes relevantes. Para acabar com o assédio, podem até ter de informar as autoridades locais. Depois de preencher toda a documentação necessária, o aluno deve tomar as providências necessárias para bloquear o indivíduo ou a conta responsável pelo ciberbullying. Eles também devem estar conscientes de que, mesmo após bloquear o infrator, podem criar contas alternativas para abordar a vítima. A boa notícia sobre o bullying on-line é que, em regra, pode ser registado, preservado e apresentado a alguém que possa ajudar. As vítimas devem guardar essa prova caso as coisas saiam fora de controlo.

VÍDEO: IGNORE OR REPORT A CYBER BULLY

Atividade de aprendizagem 2

Apresente o estudo de caso abaixo aos alunos

Projeto Erasmus+ YouProMe – www.youpromeproject.eu

Jessica tem 18 anos. Vive com a mãe e com o pai, ambos profissionais e sempre ocupados a trabalhar. Jéssica é a mais velha de três filhos. Ninguém na família tem problemas de saúde. Ela anda na escola e é uma aluna trabalhadora. É apaixonada por animais e gosta de sair com os amigos. Tem um namorado. Jéssica tem telemóvel e é utilizadora assídua das redes sociais.

Jessica relatou: "Há algumas semanas, enviei algumas fotos ao meu namorado. Eu pensava que ele era meu namorado, mas então ele mostrou-as ao amigo e o amigo mandou-as para toda a gente. A escola descobriu e agora a polícia falou com ele e com o amigo. Não voltei à escola desde então, mas agora todos me chamam vadia nas redes sociais. Não suporto quando olham para mim e eu já sei o que estão a pensar. Até as raparigas têm uma opinião semelhante sobre mim. O estúpido é que toda a gente mundo faz isso, todos enviam fotos, mas eu só tive azar de ter um namorado que me traiu. Nunca mais vou confiar em ninguém. Sinto que tudo acabou e agora não há como voltar atrás.

Como consequência, há um mês que Jessica falta à escola e recusa-se a voltar. Abandonou todas as atividades desportivas da escola. A mãe conversou com o assistente social do desporto e jovens e disse que está preocupada com algumas das coisas "sombrias" que Jessica tem dito. Jessica está desejosa de mudar a sua presença online e recuperar a confiança inicial. Jessica e a sua família não sabem que apoio está disponível e como melhor apoiar a sua saúde mental nem têm qualquer conhecimento de como o assistente social pode mediar esta situação. Jéssica percebeu o risco da utilização indevida da internet e reconhece que necessita de apoio para cuidar da sua saúde mental, pois isso influenciou a sua tomada de decisão.

Agora pode iniciar uma conversa com base nestas perguntas (máx. 30 minutos):

Que riscos estão presentes aqui?

Quais serviços devem envolver?

Que curso de ação sugerem para a Jessica e a sua mãe?

2. Resultados de aprendizagem para o módulo

Conhecimentos

O aluno compreenderá a importância de prevenir o ciberbullying
O aluno saberá que tipo de técnicas estão disponíveis para evitar ser vítima de ciberbullies

Competências

O aluno será capaz de divulgar a prevenção do ciberbullying
O aluno será capaz de ensinar técnicas de prevenção importantes aos seus alunos

Aptidões

O aluno será capaz de implementar eventos eficientes de consciencialização contra o ciberbullying
Dependendo da situação, o aluno será capaz de determinar que tipo de assistência é necessária.

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/

AUTENTICAÇÃO E PALAVRA-PASSE

Módulo 4

1. Visão geral do módulo

Grupo-alvo

- Educadores EFP
- Alunos
- Representantes de instituições públicas que atuam nos setores educativos: municípios, autoridades regionais e nacionais

Descrição do módulo

Os profissionais do EFP e os seus alunos enfrentam diariamente diferentes ameaças à cibersegurança. Embora existam vários materiais educativos sobre cibersegurança disponíveis online, nem todos estão atualizados ou então são vistos pelos alunos como demasiado básicos ou demasiado complexos.

Os conteúdos educativos deste módulo dotará os alunos de competências e conhecimentos para melhorarem a sua compreensão de Autenticação e Palavras-passe com vista a fortalecer a sua capacidade de formação, mas também melhorar as suas competências para evitar ciberataques. Educadores do EFP mais bem equipados poderão apoiar ainda mais os seus alunos no reconhecimento das ameaças diárias que os evitam.

Objetivos de aprendizagem

Melhorar a compreensão da autenticação em cibersegurança

Melhorar a compreensão dos diferentes métodos de autenticação

Melhorar a compreensão das principais características dos métodos de autenticação mais comuns

Compreender os riscos de não utilizar palavras-passe complexas

Disponibilizar técnicas para gerir palavras-passe complexas

Duração total

2 horas

AUTENTICAÇÃO E PALAVRA-PASSE

Móulo 4

Unidade 1 - Autenticação

Esta Unidade será ministrada pelo formador sob a forma de uma apresentação PowerPoint cujo objetivo é a partilha de conhecimentos teóricos acompanhados de elementos mais visuais - pequenos vídeos que resumem a informação dos slides PowerPoint (máx. 20 minutos).

Recomenda-se que as apresentações sejam elaboradas nos modelos de PPT personalizados para o projeto CYBER.EU.VET. Considerando os rápidos desenvolvimentos e evolução no campo da cibersegurança, recomenda-se rever continuamente as unidades e, se necessário, ajustar os conteúdos tendo em conta os desenvolvimentos mais recentes no terreno.

A apresentação é seguida por uma discussão em grupo de 10 minutos com vista a refletir sobre o processo de aprendizagem e avaliar o nível de compreensão dos alunos sobre o tema ao mesmo tempo que se cria espaço para mais perguntas e feedback.

Atividade de aprendizagem 1

O formador faz uma apresentação com os seguintes conteúdos sugeridos (máx. 20 minutos):

O que é a autenticação?

O processo de autenticação no contexto de sistemas informáticos significa garantia e confirmação da identidade de um utilizador. Antes de um utilizador tentar aceder a informações armazenadas numa rede, o mesmo deve provar a sua identidade e permissão para aceder aos dados. Ao fazer login numa rede, o utilizador deve fornecer informações únicas de login, incluindo um nome de utilizador e palavra-passe, uma prática concebida para proteger uma rede contra a infiltração de hackers. A autenticação expandiu-se ainda mais nos últimos anos para exigir mais informações pessoais do utilizador, por exemplo, biometria, para garantir a segurança da conta e da rede daqueles com competências técnicas para aproveitar as vulnerabilidades.

VÍDEO: WHAT IS AUTHENTICATION?

Por que a Autenticação é importante?

A autenticação é uma etapa crucial para manter os dados dos utilizadores seguros e para prevenir e bloquear qualquer acesso não autorizado aos dados online. Se a autenticação não for segura, o sistema pode ser facilmente atacado e hackeado e os cibercriminosos podem obter acesso aos dados e informações armazenados no sistema.

IÉ muito importante evitar que isto aconteça e certificar-se de que os utilizadores estão conscientes dos diferentes métodos de autenticação gratuitos ou pagos para impedir qualquer acesso não autorizado aos seus dados pessoais ou profissionais. Para organizações e empresas, recomendamos investir em ferramentas de autenticação de alta qualidade para proteger os seus dados online contra possíveis violações.

VÍDEO: WEEKLY CYBERSECURITY TIP - AUTHENTICATION

Métodos comuns de autenticação de palavra-passe

Tendo em conta a natureza em constante mudança dos diferentes tipos de ciberameaças e ciberataques, ao longo dos últimos anos, desenvolveu-se uma gama alargada de diferentes métodos de autenticação.

Alguns dos métodos de autenticação mais comuns são:

1. Autenticação de palavra-passe padrão
2. Autenticação de dois fatores
3. Autenticação por token
4. Autenticação biométrica
5. Autenticação de Reconhecimento de Computador
6. CAPTCHAS

1. AUTENTICAÇÃO DE PALAVRA-PASSE PADRÃO

A forma de autenticação mais básica e utilizada com maior frequência:

Exige a introdução do nome de utilizador, acompanhado de um código secreto ou palavra-passe que permite o acesso a uma rede, conta ou aplicação.

Para reduzir o risco de uma palavra-passe ser comprometida, os utilizadores devem escolher uma palavra-passe forte. Um software ou gerenciador de senhas seguro pode ajudar a impedir qualquer acesso não autorizado aos dados armazenados online.

2. AUTENTICAÇÃO DE DOIS FATORES (2FA)

A autenticação de dois fatores exige que os utilizadores se autentiquem através de algo que “eles sabem” e algo que “eles têm”. Uma palavra-passe serve como “algo que eles sabem” e um objeto físico específico, como um smartphone, serve como “algo que eles têm.”

Em regra, a autenticação de dois fatores exige que o utilizador insira o seu nome de utilizador, uma palavra-passe e um código único que foi enviado para um dispositivo físico (telemóvel, leitor de cartões, etc.).

AUTENTICAÇÃO E PALAVRA-PASSE

3. AUTENTICAÇÃO POR TOKEN

Os sistemas de token utilizam um dispositivo físico específico para fornecer autenticação de dois fatores e são recomendados se preferir não depender de telemóveis.

Pode ser um dongle inserido na porta USB do seu dispositivo ou talvez um cartão inteligente com identificação por radiofrequência ou chip de comunicação de campo próximo.

Para manter um sistema de token seguro, é crucial assegurar que o dispositivo de autenticação física (ou seja, dongle ou cartão inteligente) não cai em mãos erradas.

4. AUTENTICAÇÃO BIOMÉTRICA

A autenticação biométrica depende das características físicas de um utilizador para o identificar. A autenticação biométrica pode recorrer a impressões digitais, digitalização da retina ou da íris ou reconhecimento facial e de voz. Esta é uma forma de autenticação altamente segura porque não há dois indivíduos com as mesmas características físicas. A autenticação biométrica é uma forma eficaz de saber com precisão quem está a fazer login no sistema.

5. AUTENTICAÇÃO POR RECONHECIMENTO DE COMPUTADOR

O reconhecimento de computador é um método de autenticação de palavra-passe que verifica a legitimidade de um utilizador verificando se o mesmo se encontra num determinado dispositivo. Estes sistemas instalam um pequeno plug-in de software no dispositivo do utilizador na primeira vez que o mesmo faz login com sucesso. Este plug-in contém um marcador de dispositivo criptográfico. Na próxima vez que o utilizador fizer login, o marcador será verificado para garantir que se encontra no mesmo dispositivo fiável. Este sistema é invisível para o utilizador e não requer nenhuma ação de autenticação adicional pela sua parte. Basta inserirem o seu nome de utilizador e palavra-passe como de costume e a verificação acontece automaticamente. Para manter um nível elevado de segurança, os sistemas de autenticação por reconhecimento de computador devem permitir logins de novos dispositivos com recurso a outras formas de verificação (ou seja, autenticação de dois fatores com um código enviado por SMS).

6. CAPTCHAS

Os CAPTCHAs não se centram na verificação de um utilizador específico ao contrário dos outros métodos indicados neste artigo. Em vez disso, os CAPTCHAs visam determinar se um utilizador é humano, evitando tentativas de invasão de contas por computadores (por exemplo, ataques de força bruta). O sistema CAPTCHA apresenta uma imagem distorcida de letras e números ou imagens epede ao utilizador para digitar o que vê. Como os computadores e bots lutam para identificar estas distorções corretamente, os CAPTCHAs aumentam a segurança criando uma barreira adicional para sistemas de hackers automatizados.

Atividade de aprendizagem 2

Discussão em Grupo – Perguntas e Respostas, Avaliação e feedback (máx. 10 minutos)
Perguntas recomendadas para avaliação:
O que é a autenticação?
Por que a autenticação é importante?Quais são os métodos de autenticação mais comuns atualmente em uso e quais são as
suas principais características?

Unidade 2 - Palavra-passe

Atividade de aprendizagem 1

1. COISAS QUE NÃO DEVE FAZER

Slides com imagens que exemplifiquem coisas que as pessoas não devem fazer para atrair o público

ESTUDOS DE CASO

"A polícia belga publicou com a palavra-passe da rede Wi-Fi ativada. Isto passou na TV nacional" - https://www.reddit.com/r/cybersecurity/comments/cnkhft/the_belgian_police_have_a_post_it_with_the_wifi/

"Uma palavra-passe para a agência de emergências do Havai estava escondida numa foto pública, escrita num post-it" - https://www.businessinsider.com/hawaii-emergency-agency-password-discovered-in-photo-sparks-security-criticism-2018-1

"Quatro fugas embaraçosas de palavras-passe na TV em direto" - https://www.itgovernance.co.uk/blog/four-embarrassing-password-leaks-on-live-tv

2. ESTATÍSTICAS

Apresentação de algumas estatísticas:
81% das violações de dados acontecem devido à falta de segurança da palavra-passe
Maus hábitos dos funcionários em termos de palavras-passe
As 200 palavras-passe mais comuns

3. A IMPORTÂNCIA DE UMA PALAVRA-PASSE SEGURA

A anatomia de uma palavra-passe inatacável

4. REGRAS BÁSICAS

Descrever um conjunto de regras básicas como:

Evite utilizar os gerenciadores de palavras-passe do navegador; é uma maneira fácil de um "malware" obter acesso aos mesmos.

Não partilhe a sua palavra-passe.

Memorize as palavras-passe, não as registe em papel ou digitalmente Altere as palavras-passe regularmente (pelo menos, a cada dois meses)

Se possível, ative a autenticação de dois fatores

Cada palavra-passe deve ser utilizada em apenas uma plataforma

Altere a palavra-passe original quando compra um dispositivo

Não utilize palavras comuns. Um dos tipos de ataque mais frequentes é via "dicionário"

Regras para uma palavra-passe mais segura:

Crie palavras-passe complexas: pelo menos, 12 caracteres, com caracteres maiúsculos e minúsculos, com números e caracteres especiai

Não utilize termos facilmente “detetáveis” que normalmente incluem: nome, cidade de nascimento ou termos conhecidos, nome do animal de estimação, número da matrícula do carro; número do telemóvel, aniversários de familiares, etc.

Memorizar em vez de gravar:

Crie uma "chave" pessoal, que faz parte de todas as palavras-passe

Utilize um ditado, expressões comuns ou algo fácil de memorizar

Por exemplo, utilize as duas primeiras letras de cada palavra

Alterne entre maiúsculas, minúsculas e símbolos

Adicione algo que associe ao site/ferramenta

Atividade de aprendizagem 2

Exercício de grupo

Teste o comprimento da sua palavra-passe - https://www.passwordmonster.com

Já me "crakaram" palavras-passe? - https://haveibeenpwned.com/Passwords

Discussão e Feedback (máx. 10 minutos)

Perguntas recomendadas para avaliação:
Quantos anos a sua palavra-passe resiste a uma máquina de algoritmo de crack normal?
Devo alterar a minha palavra-passe?

Atividade de aprendizagem 3

O formador faz uma apresentação aos alunos com os seguintes conteúdos sugeridos (máx. 20 minutos):

O que são gestores de palavras-passe?
Cofres digitais
Permite armazenar credenciais e notas de vários serviços

Os dados bancários também podem ser protegidos

Uma única chave mestra

Pode utilizar-se autenticação biométrica

Gestores de palavras-passe locais
Guarde os dados no dispositivo atual
O ficheiro da palavra-passe é encriptado

Cada palavra-passe deve ser guardada num ficheiro encriptado separado
Só pode ser utilizada num único dispositivo
Exemplo como o KeypassXC
Gestores de palavras-passe online
Os dados são armazenados na nuvem
Permitir acesso a credenciais e notas de vários serviços em qualquer dispositivo

Não é necessária qualquer instalação

Uma única chave mestra

Os dados são encriptados do dispositivo para o servidor

Exemplo de gestores de palavras-passe online inclue Bitwarden, Latspass, Keeper, 1Password

Atividade de aprendizagem 4

Prática em grupo

Criar uma palavra-passe forte
Instalar um gestor de palavras-passe no computador portátil ou smartphone
Ativar MFA

Discussão e Feedback (máx. 10 minutos)
Perguntas recomendadas para avaliação:
Foi difícil?
Vão usar estas melhores práticas?

2. Resultados de aprendizagem para o módulo

Conhecimentos

Compreender a definição de autenticação, a sua importância e alguns dos métodos de autenticação mais comuns
Compreender os riscos de não utilizar palavras-passe complexas
Utilizar as melhores práticas na gestão de palavras-passe pessoais

Competências

Identificar e aplicar o método de autenticação mais adequado e apropriado
Identificar e aplicar a complexidade de palavra-passe mais adequada e apropriada

Competências

Perceber a importância da autenticação
Decidir sobre o método de autorização mais adequado para diferentes atividades online e aplicá-los para aumentar a segurança online
Perceber a importância de utilizar palavras-passe complexas
Estruturar técnicas de melhores práticas para gerir palavras-passe pessoais

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

ÓDULO DE FORMAÇÃO SEGURANÇA DA REDE WI-FI

Módulo 5

1. Visão geral do módulo

Grupo-alvo

- Educadores EFP
- Alunos
- Representantes de instituições públicas que atuam nos setores educativos: municípios, autoridades regionais e nacionais

Esquema do módulo

O presente módulo focará o esclarecimento das ameaças reais relacionadas com sistemas wi-fi públicos, como funcionam e, eventualmente, como evitá-las.

Objetivos de aprendizagem

Sensibilizar para equívocos relativamente à utilização de redes wi-fi públicasDisponibilizar conhecimentos sobre as ameaças envolvidas na utilização de redes wi-fi públicas

Duração total

1 hora

Unidade 1

O módulo compreende partes de aprendizagem em vídeo e discussões abertas. Especificamente, inicialmente será exibido um primeiro vídeo introdutório. Este vídeo demonstra, com a ajuda de um especialista, como as redes públicas são um local arriscado para se ligar à internet. No entanto, este primeiro vídeo é muito curto e não permite captar muito do processo subjacente. Esta primeira parte termina com uma discussão entre os alunos.

Unidade 2

Em segundo lugar, um vídeo mais específico será tido em conta. Apesar da sua maneira informal de abordar o assunto, o vídeo definitivamente proporciona uma melhor compreensão do assunto. Terminado o vídeo, o facilitador é convidado a propor uma discussão entre os participantes sobre os riscos das redes públicas e, se possível, partilharem as suas experiências pessoais.

Atividade de aprendizagem 1

Um dos aspetos relativamente aos quais este módulo pretende chamar a atenção é a facilidade com que estas ameaças de redes wi-fi públicas são apresentadas. Uma atividade de aprendizagem contínua é tentar aplicar as sugestões aprendidas através dos conteúdos de vídeo deste módulo, desde o restaurante/bar onde os participantes irão almoçar até à estação de comboios e aeroporto onde os participantes irão parar no regressar a casa após a mobilidade.

2. Bibliografia

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

A UTILIZAÇÃO DAS REDES SOCIAIS

Módulo 6

1. Visão geral do módulo

Grupo-alvo

- Educadores EFP
- Alunos
- Representantes de instituições públicas que atuam nos setores educativos: municípios, autoridades regionais e nacionais

Visão geral do módulo

As Redes Sociais Online (ONS) assumiram um espaço sem precedentes no quotidiano profissional, educativo e privado das pessoas, inclusive dos educadores do EFP e dos seus alunos. Embora os benefícios de tal integração tenham sido mais fáceis de reconhecer e adotar como um componente integral da educação formal e informal, os vários riscos associados à mesma não receberam a devida atenção e são frequentemente ignorados pelos próprios educadores.

Uma abordagem simplista frequentemente utilizada no que diz respeito à problemática multifacetada da segurança das redes sociais, assim como a complexidade de alguns dos materiais de formação disponíveis, não são suficientes para criar a capacidade necessária para prevenir e responder às ameaças colocadas pela utilização destas plataformas.

Este módulo tentará fornecer aos alunos um conjunto básico de conhecimentos e reforçar a sua capacidade de formação e também melhorar a sua própria abordagem pessoal à segurança das redes sociais.

Objetivos de aprendizagem

Compreender os ciber-riscos e ciberameaças associados à utilização de redes sociais
Reforçar o impacto dos processos de desinformação na segurança das plataformas UGC
Identificar os diferentes tipos de ameças à cibersegurança
Reforçar a capacidade de prevenir e responder a ciberameaças nas redes sociais
Disponibilizar técnicas para gerir palavras-passe facilmente complexas

Duração total

2 horas

A UTILIZAÇÃO DAS REDES SOCIAIS

Módulo 6

Unidade 1 - Ameaças nas Redes Sociais

Esta Unidade será facilitada com o recurso a uma apresentação em PowerPoint e introduzida pela leitura de títulos de notícias que oferecem histórias generalizadas de vítimas de ciberameaças através das redes sociais (fotos de VIP roubados, pessoas que perderam a vida por causa de notícias falsas sobre imunização, etc. ...)
As histórias e os conteúdos serão ajustados para serem relevantes para o contexto e atualizados com as descobertas mais recentes.
A apresentação é seguida por uma discussão em grupo de 10 minutos com vista a refletir sobre o processo de aprendizagem e avaliar a capacidade dos alunos de compreenderem o tema e também para criar espaço para mais perguntas e feedback.

Atividade de aprendizagem 1

O formador faz uma apresentação aos alunos com os seguintes conteúdos sugeridos (máx. 20 minutos):

O que é uma Rede Social Online?

Uma Rede Social Online (OSN) é uma estrutura social composta por indivíduos ou organizações chamados nós, ligados por um ou mais tipos específicos de interdependência, como amizade, interesse comum e troca de finanças, relações de crenças, conhecimento ou prestígio. Os sites de redes sociais como Facebook, Twitter, Instagram, etc. não são utilizados apenas para comunicar ou interagir com outras pessoas globalmente, mas também uma forma eficaz de promover negócios. Ao contrário das plataformas web e multimédia tradicionais, as Redes Sociais destinam-se exclusivamente a alojar e distribuir conteúdos gerados pelo utilizador (UGC) segundo critérios (algoritmos) baseados nas ações e preferências expressas pelos próprios utilizadores e registadas em dados. Neste sentido, todos os utilizadores são participantes ativos nos processos de sustentabilidade das redes sociais.

O que é uma Ameaça de Redes Sociais?

Uma ameaça de redes sociais pode ser qualquer coisa que comprometa a segurança de uma conta. Uma ciberameaça pode ser intencional ou não, direcionada ou não, e pode vir de várias fontes, incluindo nações estrangeiras envolvidas em espionagem e guerra de informação, criminosos, hackers, criadores de vírus, funcionários insatisfeitos e contratados que trabalham numa organização.

Como é uma ameaça de redes sociais

Como as redes sociais têm um grande número de utilizadores e armazenam enormes quantidades de dados, são alvos naturais de spammers, phishing e ataques maliciosos. Além disso, os ataques sociais online incluem roubo de identidade, difamação, perseguição, ofensa à dignidade pessoal e cyberbullying. Os hackers criam perfis falsos e imitam personalidades ou marcas ou difamam uma pessoa conhecida dentro de uma rede de amigos.

As preocupações com a privacidade exigem que os perfis de utilizador nunca publiquem e distribuam informações pela web. As informações nas páginas iniciais pessoais podem conter dados muito confidenciais, como datas de nascimento, moradas residenciais, números de telemóvel pessoais e assim por diante. Estas informações podem ser utilizadas por hackers que recorrem a técnicas de engenharia social para obter os benefícios dessas informações confidenciais e roubar dinheiro.

Como as Ameaças nas Redes Sociais mudam entre plataformas

A forma como uma ameaça de redes sociais é executada por um atacante depende dos seus objetivos. O Facebook permite que os utilizadores mantenham as suas imagens e comentários privados, portanto, um atacante, geralmente, faz amizade com os amigos de um utilizador-alvo ou envia diretamente um pedido de amizade a um utilizador-alvo para aceder às suas publicações. O LinkedIn é outro alvo comum em termos de redes sociais conhecido por redes de negócios. Se um atacante tiver como alvo uma empresa, o LinkedIn é um excelente site de rede social para recolher e-mails comerciais para um ataque de phishing. Como muitas plataformas de redes sociais exibem publicamente publicações de utilizadores, os atacantes podem recolher dados silenciosamente sem o conhecimento do utilizador. Alguns atacantes tomarão medidas adicionais para obter acesso às informações do utilizador entrando em contacto com os utilizadores-alvo ou os seus amigos.

Por que é importante falar sobre ameaças OSN?

Em 30 de dezembro de 2020, havia quase 4 mil milhões de utilizadores da Internet. Da população total na internet, existem 2,7 mil milhões de clientes dinâmicos mensais no Facebook, 330 milhões de utilizadores ativos no Twitter e 320 milhões de utilizadores ativos no Pinterest.

A utilização de sites de redes sociais está a crescer exponencialmente. Se olharmos apenas para o Facebook, sete novos perfis são criados a cada segundo, 510.000 comentários são publicados a cada 60 segundos, 298.000 status são atualizados e 136.000 fotos são carregadas no mesmo período de tempo. Como se carrega uma grande quantidade de dados, existe um risco elevado de violação de segurança. Qualquer pessoa pode publicar conteúdos maliciosos ocultos em dados multimédia ou com localizadores uniformes de recursos (URL) abreviados. Existem cerca de 83 milhões de perfis falsos correspondentes a utilizadores ilegítimos ou profissionais que fazem testes e pesquisas. Cerca de 100.000 sites são invadidos diariamente.

A UTILIZAÇÃO DAS REDES SOCIAIS

Embora alguns sites de redes sociais como o Twitter não permitam a divulgação de informações privadas aos utilizadores, alguns atacantes experientes podem inferir informações confidenciais analisando as publicações dos utilizadores e as informações que os mesmos partilham online. As informações pessoais que partilhamos on-line podem fornecer aos cibercriminosos o suficiente para obter o nosso e-mail e palavras-passe.

O valor dos dados pessoais

As redes sociais geralmente oferecem os seus serviços gratuitamente. As informações pessoais não são apenas a moeda corrente das redes sociais, mas também o principal objetivo das ciberameaças nas redes sociais.

Pode ser fácil lançar um ataque porque muitas pessoas, geralmente, fornecem as suas informações pessoais a plataformas de redes sociais. Os invasores podem recolher facilmente estes dados e utilizá-los para obter ganhos.

Recolher informações para roubar é apenas um tipo de redes sociais para reconhecimento. As informações publicas nas redes sociais podem ser utilizadas para obter palavras-passe ou fazer-se passar por utilizadores empresariais.

Com uma lista de alvos, um atacante pode analisar as contas das redes sociais em busca de informações pessoais. As informações pessoais podem ajudar o atacante a ganhar a confiança do alvo num ataque de engenharia social. Também podem ser utilizadas para adivinhar respostas a perguntas de segurança para uma apropriação fraudulenta de conta ou para se aproximar de um utilizador com mais privilégios. Os nomes de animais de estimação, equipas desportivas preferidas e histórico educativo são possíveis pistas para a palavra-passe ou respostas a perguntas utilizadas para verificar a identidade do utilizador para redefinir uma palavra-passe.

Porquê aprender sobre ameaças OSN?

As interfaces e os processos simples que estas plataformas oferecem podem aludir a pessoas sem o conhecimento ou as competências necessárias para aceder com segurança aos seus serviços e conteúdos.

A educação é a chave para impedir as ameaças das redes sociais online.

O primeiro passo é educar os utilizadores sobre os perigos de divulgar muita informação online ao público. Mesmo as contas de redes sociais definidas como privadas podem ser utilizadas num ataque, caso o invasor obtenha acesso a feeds privados. Os utilizadores nunca devem publicar informações empresariais privadas nas suas contas de redes sociais ou informações que possam ser utilizadas numa apropriação fraudulenta de conta.

O segundo passo é educar os utilizadores sobre como os conteúdos digitais são produzidos e distribuídos e como podem direcionar as ações dos utilizadores para os objetivos específicos para os quais o conteúdo foi criado. Todos os conteúdos de redes sociais são criados e veiculados pelos utilizadores de acordo com os seus diferentes objetivos pessoais e/ou coletivos. Por esses motivos, alguns destes conteúdos podem nem sempre ser convenientes, verdadeiros ou éticos.

Finalmente, os utilizadores devem ser educados para a utilização e manutenção seguras dos dispositivos através dos quais acedem aos serviços de redes sociais online, pois normalmente são vetores de riscos e intrusão. Alguns pontos educativos a este respeito já estão ilustrados noutros módulos de formação e incluem:

- Evite clicar em anúncios, especialmente pop-ups que dão instruções ao utilizador para descarregar o software para visualizar o conteúdo.
- Não partilhe palavras-passe.
- Evite mensagens ou publicações de redes sociais que incitam ações rápidas como uma técnica de engenharia social
- Não aceite pedidos com um aspeto amigável de pessoas desconhecidas, mesmo que o utilizador tenha vários amigos em comum
- Evite a utilização de sites de redes sociais em pontos de acesso de redes wi-fi públicas (um local comum para atacantes bisbilhotarem dados recorrendo a ataques man-in-the-middle [mitm])
- Altere regularmente os códigos de acesso e as palavras-passe.

Atividade de aprendizagem 2

Peça aos alunos que pesquisem os seus próprios nomes num motor de busca operado por uma rede social ou no Google e listem todas as informações privadas que podem ser detetadas pelos vários conteúdos encontrados (local e data de nascimento, pormenores e informações sobre membros da família, moradas, números de telefone, animais de estimação, parceiros românticos, hobbies e preferências). Convide-os a pensarem em formas como essas informações podem ser utilizadas contra eles.

Unidade 2 - Tipo de ameaças OSN

Atividade de aprendizagem 1

Peça aos alunos que listem qualquer ameaça à segurança que consideram que podem encontrar nas mídias sociais e peça-lhes que expliquem se acreditam que essa ameaça poderia existir antes de a OSN existir.

VÁRIAS AMEAÇAS NAS REDES SOCIAIS E MEDIA ONLINE

Podemos dividir as ameaças OSN em três categorias:

1. Ameaças convencionais incluem ameaças que os têm vivido desde os primórdios das rede sociais.
2. Ameaças modernas são ataques que recorrem a técnicas avançadas para comprometer contas de utilizadores.
3. Ataques direcionados são ataques direcionados a um utilizador específico.

AMEAÇAS CONVENCIONAIS

Spam

Spam é o termo utilizado para mensagens eletrónicas em massa não solicitadas. Embora o e-mail seja a forma convencional de espalhar spam, a plataforma de rede social é mais bem- sucedida na disseminação de spam. As informações de contacto de utilizadores legítimos podem ser facilmente obtidas nos sites, blogues e grupos de notícias de empresas. Não é difícil convencer o cliente-alvo a ler as mensagens de spam e confiar que são protegidas. A maior parte do spam é publicidade comercial, também pode ser utilizado para recolher informações confidenciais dos utilizadores ou pode conter vírus, malware ou golpes.

Ataque de malware

O malware é uma aplicação programada desenvolvida explicitamente para contaminar ou aceder a um sistema informático, geralmente, sem o conhecimento do utilizador. O malware pode utilizar a estrutura de redes sociais para se propagar através de URL partilhados ou subaplicações OSN, como e-games ou plug-ins.

Phishing

Um ataque de phishing é um tipo de ataque de engenharia social no qual o agressor pode adquirir informações sensíveis e confidenciais, como nome de utilizador, palavra-passe e informações do cartão de crédito de um utilizador através de sites falsos e e-mails que parecem reais.

No caso das OSN, um agressor tem de atrair o cliente para uma página falsa onde pode realizar um ataque de phishing. Para conseguir isto, o agressor recorre a diferentes métodos de engenharia social. Por exemplo, pode enviar uma mensagem a utilizador dizendo: "as suas fotos pessoais estão partilhadas neste site, verifique!". Ao clicar nesse URL, o utilizador é redirecionado para um site falso que se parece com um site de rede social legítimo.

AMEAÇAS MODERNAS

Ataque de script entre sites

Script entre sites é um vetor de ataque muito comum entre os infiltrados. Fundamentalmente, o ataque executa um JavaScript malicioso no navegador da vítima através de diferentes técnicas. O navegador pode ser sequestrado com apenas um clique de um botão que pode enviar um script malicioso para o servidor. Este script é enviado novamente para a vítima e executado no navegador. Links e botões atraentes em sites populares de redes sociais como o Twitter e o Facebook podem induzir o utilizador a seguir URL, assim como alertas pop-up de vírus e anúncios promissores ou conteúdos multimédia que exigem visitar um link ou clicar num botão para serem desbloqueados. Alguns utilizadores podem ser convidados a copiar e colar links contendo JavaScript na barra de endereço do navegador. Estes ataques podem roubar informações ou agir como spyware. Estes ataques podem igualmente sequestrar computadores para lançar ataques contra utilizadores incautos, enquanto o verdadeiro perpetrador do ataque está escondido atrás da máquina comprometida.

Ataque de clonagem de perfil

Neste ataque, o assaltante clona o perfil dos utilizadores graças a um conhecimento prévio ou a informações recolhidas online. O atacante pode usar este perfil clonado na mesma ou noutra plataforma de rede social para criar uma relação de confiança com os amigos do utilizador real. Quando se estabelece a ligação, o atacante engana os amigos da vítima para que acreditem na validade do perfil falso e acedam com sucesso a informações confidenciais que não são partilhadas nos seus perfis públicos. Este ataque também pode ser utilizado para cometer outros tipos de cibercrimes, como cyberbullying, cyberstalking e chantagem.

Hijacking

No hijacking, o adversário compromete ou assume o controlo da conta de um utilizador para realizar fraudes online. Os sites sem autenticação multifator e contas com palavras-passe fracas são mais vulneráveis ao hijacking, pois as palavras-passe podem ser obtidas através de phishing. Quando uma conta é alvo de hijacking, o hijacker pode enviar mensagens.

Ataque de inferência

O ataque de inferência infere informações confidenciais de um controlador que o utilizador pode não querer divulgar, através de outras estatísticas que são colocadas pelo utilizador numa OSN. Recorre a procedimentos de mineração de dados em dados visivelmente disponíveis, como a lista de amigos do utilizador e a topologia da rede. Recorrendo a esta técnica, um atacante pode encontrar informações secretas de uma organização ou informações geográficas e educativas de um utilizador.

Ataque Sybil / Botnet

No ataque Sybil, um nó reivindica múltiplas identidades numa rede. Pode ser prejudicial para as plataformas de redes sociais, pois contém um grande número de utilizadoresligados através de uma rede peer to peer. Peers são as estruturas de computador que estão associadas entre si através da Internet e podem partilhar registos diretamente sem a necessidade de um servidor central. Esta rede de máquinas também pode ser chamada BotNet. Uma entidade online pode criar várias identidades falsas e utilizar essas identidades para distribuir informações inúteis, malware ou até mesmo afetar a reputação e a popularidade de uma organização. Por exemplo, uma pesquisa na web pode ser manipulade om recurso a várias entregas de protocolo da Internet (IP) para enviar um grande número de votos e o agressor pode superarum cliente real em votos. Um exército semelhante pode, por exemplo, partilhar uma única mensagem várias vezes e tornar o seu conteúdo viral.

Clickjacking

Clickjacking é um procedimento no qual o invasor engana um utilizador para que clique numa página diferente daquela em que ele pretendia clicar. O atacante explora a vulnerabilidade dos navegadores para realizar este ataque. Ele carrega outra página sobre a página a que o utilizador deseja aceder, como uma camada transparente. As duas variações conhecidas de clickjacking são likejacking e cursorjacking. A camada frontal mostra a substância com a qual o cliente pode ser enganado. No momento em que o cliente toca nesse conteúdo, ele realmente toca no botão gosto. Quanto mais pessoas gostarem dapublicação, mais ela se espalha. No cursorjacking, um atacante substitui o cursor real por uma imagem de cursor personalizada. O cursor real é deslocado da sua posição real do rato. Desta forma, o intruso pode induzir o consumidor a clicar no site malicioso com um posicionamento inteligente dos elementos da página.

Ataque de desanonimização

Em muitos sites de redes sociais como o Twitter e o Facebook, os utilizadores podem ocultar ou proteger a sua identidade real antes de libertar qualquer informação utilizando um pseudónimo ou um nome falso. Mas se um terceiro quiser descobrir a identidade real do utilizador, isso pode ser feito rastreando cookies, topologias de rede e registo de grupo de utilizadores para descobrir a identidade genuína do cliente. É uma espécie de método de mineração de informações no qual informações misteriosas são cruzadas com outras fontes de informações para reconhecer novamente as informações desconhecidas. Um atacante pode recolher informações sobre a associação de grupo de um utilizador roubando o histórico do seu navegador e combinando este histórico com os dados recolhidos. Assim, o atacante pode remover o anonimato do utilizador que visita o site desse atacante.

AMEAÇAS DIRECIONADAS

Ciberbullying

O ciberbullying é a utilização de meios eletrónicos, tais como e-mails, chats, conversas telefónicas e redes sociais online para intimidar ou assediar uma pessoa. Ao contrário do bullying tradicional, o ciberbullying é um processo contínuo, pois é mantido continuamente através das redes sociais. O atacante envia repetidamente mensagens intimidadoras, comentários sexuais, publica boatos e, por vezes, publica fotos ou vídeos embaraçosos para assediar uma pessoa. Também pode publicar informações pessoais ou privadas sobre a vítima, causando constrangimento ou humilhação. O ciberbullying também pode acontecer acidentalmente, embora padrões repetidos de tais e-mails, textos e publicações online raramente sejam acidentais.

Cyber grooming

O cyber grooming é o estabelecimento de uma relação íntima e emocional com a vítima (geralmente crianças e adolescentes) com a intenção de forçar o abuso sexual ou mental. O objetivo principal do cyber grooming é conquistar a confiança do jovem e através disso podem obter-se informações íntimas e individuais da criança. Os dados, geralmente, são de natureza voluptuosa através de conversas, fotos e vídeos sexuais, o que dá ao atacante a vantagem de ameaçar e chantagear a criança. Os agressores frequentemente abordam adolescentes ou crianças através de identidade falsificada em sites adequados para crianças, deixando-as vulneráveis e desinformadas sobre o facto de que foram atraídas para mais perto com o objetivo final de cyber grooming. No entanto, a vítima também pode, sem saber, iniciar o processo de grooming quando recebe ofertas gratificantes, por exemplo, dinheiro em troca de informações de contacto ou fotografias pessoais suas. O anonimato e a acessibilidade dos média avançados permitem que os groomers se aproximem de vários jovens simultaneamente, aumentando exponencialmente os casos de cyber grooming.

Cyberstalking

O cyberstalking é a observação de um indivíduo através da internet, e-mail ou algum outro tipo de correspondência eletrónica que resulta em medo de violência e interfere com a paz mental desse indivíduo. Envolve a invasão do direito de uma pessoa à privacidade. O atacante rastreia as informações pessoais ou confidenciais das vítimas e utiliza-as para as ameaçar através de mensagens contínuas e persistentes ao longo do dia. Esta conduta faz com que a vítima fique excecionalmente preocupada com a sua própria segurança e desencadeia nela uma espécie de problema, medo ou perturbação. A maioria das pessoas hoje em dia partilha as suas informações pessoais, como o número de telefone, o local de residência, a área e o horário no seu perfil de rede social, assim como sua localização ao vivo. Um agressor pode recolher estes dados e usá-los para o cyberstalking.

Atividade de aprendizagem 2

Peça aos alunos que trabalhem em pares e que representem os seus respetivos parceiros enquanto os entrevistam durante 10 minutos. Convide-os a tentarem as suas respostas tentando obter as informações necessárias sobre a forma como se vestem, os dispositivos que têm consigo e quaisquer outros pormenores contextuais que possam ser úteis para os representar.

Atividade de aprendizagem 3

Peça aos alunos que percorram os seus feeds de redes sociais durante 1 minuto e contem todas as frases de chamariz, links e botões nos quais são convidados a clicar. Convide-os a fazerem uma reflexão em grupo sobre como cada um desses links representa ameaças potenciais e como eles devem decidir quando e quando não interagir com o conteúdo.

Unidade 3 - Dicas para proteção nas redes sociais

Atividade de aprendizagem 1

Distribua a cada aluno uma ou mais cartas com screenshots de publicações de redes sociais (inventadas) de diferentes plataformas e convide-os a identificar quais as informações confidenciais que se podem obter de uma única publicação e quais as possíveis ameaças que podem advir dessa publicação.

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

A UTILIZAÇÃO DAS REDES SOCIAIS

Módulo 6

O QUE É A PROTEÇÃO BAS REDES SOCIAIS

As diretrizes de proteção nas redes sociais destinam-se a impedir o acesso não autorizado às suas contas de redes sociais, proteger a sua identidade online contra identidade falsa ou roubo de dados e proteger a sua rede contra identidades maliciosas ou conteúdos de redes sociais.

Como as modalidades e os objetivos das ameaças das OSN geralmente dependem do tipo de plataforma, algumas práticas específicas para prevenir ameaças também devem ser tidas em conta.

PRÁTICAS GERAIS

Utilize uma palavra-passe forte: para manter a segurança das contas, os utilizadores devem escolher uma palavra-passe forte. Não deve ser demasiado curta, pois as palavras-passe curtas podem ser facilmente adivinhadas. Deve ser suficientemente longa e deve conter valores alfanuméricos com alguns caracteres especiais. Os utilizadores não devem utilizar a mesma palavra-passe que utilizam para outras contas porque, se de alguma forma um invasor descobrir essa palavra-passe, poderá comprometer todas as contas desse utilizador.

Limite a partilha de localização: Hoje em dia, a partilha de localização tornou-se uma tendência. Muitos sites de redes sociais também introduziram um recurso de geotagging, que assinala automaticamente a localização geográfica de um utilizador quando o utilizador carrega qualquer conteúdo multimédia nas redes sociais. O utilizador deve alterná-lo para manual para que não assinale a localização automaticamente. Os utilizadores devem carregar os seus conteúdos multimédia on-line com muito cuidado, pois podem conter metadados confidenciais, e é recomendável que o geotagging seja alternado para o modo manual em todos os seus dispositivos móveis e contas.

Seja seletivo com pedidos de amizade: observou-se que muitos utilizadores aceitam pedidos de amizade sem analisar o perfil completo de quem faz o pedido. As pessoas, geralmente, aceitam pedidos de amizade com base em amigos comuns. Se o solicitante tiver alguns amigos em comum, as pessoas aceitam. Por vezes, os atacantes tornam o seu perfil atraente deliberadamente ou podem fazer-se passar por uma conta. Portanto, se a pessoa que está a enviar um pedido de amizade for desconhecida, deve ignorar-se esse pedido de amizade. Pode ser uma conta falsa a tentar roubar informações confidenciais.

Tenha cuidado com o que partilha: os utilizador devem ter cuidado com as suas publicações, pois podem revelar as suas informações pessoais e, por vezes, as de outras pessoas também. Muitas organizações mantêm regras e regulamentos rígidos para partilha de informações e conteúdos multimídias. Existem muitos relatos de pessoas que sã o

Esta situação pode ser evitada se os funcionários estiverem bem informados sobre os protocolos da organização onde trabalham em relação a fotos, vídeos e mensagens que publicam online. Partilhar informações de forma ilegítima pode prejudicar a reputação de uma organização no mercado, os seus dados e a sua propriedade intelectual.

Tenha cuidado com links e aplicações de terceiros: Utilizadores ilegítimos podem obter acesso à conta de alguém e obter informações confidenciais partilhando um link malicioso.

Atualmente, os URL abreviados estão a tornar-se muito populares em várias plataformas de redes sociais. Estes URL abreviados podem ser ofuscados por códigos ou scripts maliciosos. Estes scripts tentam recolher as informações pessoais e confidenciais de um utilizador, o que pode servir para violar a privacidade desse utilizador. Além disso, os hackers podem aproveitar as vulnerabilidades presentes numa aplicação de terceiros integrada com muitas redes sociais populares. Um exemplo deste tipo de aplicação de terceiros são os jogos que podem ser reproduzidos em redes sociais on-line e que solicitam as informações públicas de um utilizador para consumir os seus serviços. Esta informação pode ser fornecida a estranhos ou a intervenções de terceiros. Para evitar este risco, os utilizadores devem ter cuidado ao instalar aplicações de terceiros no seu perfil.

IInstale software de segurança da Internet: Algumas ameaças cujo padrão é conhecido podem ser facilmente detetadas através de antivírus. Ameaças como cyber grooming e cyberbullying podem ser detetadas até certo ponto utilizando um software antivírus.

PRÁTICAS PARA PLATAFORMA DE PARTILHA MULTIMÉDIA

- Não se devem publicar informações confidenciais nas suas fotos ou legendas. Expor demasiadas informações privadas num perfil pode ser perigoso.
- A partilha de locais atuais nas redes sociais deve ser evitada. Os serviços de geotagging fornecidos por diferentes plataformas multimédia devem ser desativados manualmente.
- Se uma aplicação não for utilizada durante um período prolongado, é melhor revogar o acesso a essa aplicação. Existem muitas aplicações de terceiros que recorrem ás contas das redes sociais para fazer login. Por questões de segurança e privacidade, deve permitir-se o acesso apenas a aplicações fiáveis.
- Ative a autenticação de duas etapas para todas as suas contas de redes sociais sempre que possível. Isto fornece uma camada extra de segurança para a conta. Caso um adversário descubra a palavra-passe de um utilizador, ele ainda precisará de um segundo fator para se autenticar. O segundo fator consiste em um código exclusivo e sensível ao tempo que os utilizadores recebem via texto nos seus telemóveis.

A UTILIZAÇÃO DAS REDES SOCIAIS

Módulo 6

PRÁTICAS PARA FÓRUNS DE DISCUSSÃO

Deve prestar-se atenção ao clicar em links fornecidos por várias fontes. Pode ser m site suspeito a tentar obter as credenciais do utilizador.

Os utilizadores devem sempre prestar atenção ao URL do site. Sites nocivos podem parecer irresistivelmente indistinguíveis dos reais. O URL, no entanto, pode conter pequenas inconsistências, como uma pequena variação na ortografia (por exemplo, um '0' em vez de um 'o', indiscernível se for lido rapidamente) ou um nome de domínio alternativo.

Tenha cuidado com as comunicações que solicitam que o cliente aja prontamente, oferecendo algo que pareça irreal ou solicitando informações pessoais.

PRÁTICAS PARA PLATAFORMAS DE CONEXÃO SOCIAL

Os utilizador devem adquirir conhecimentos sobre as definições de privacidade e segurança de diferentes plataformas de redes sociais e usá-las. Cada plataforma disponibiliza secções de definições, configuração e privacidade destinadas a limitar quem e que grupos podem ver os diferentes aspetos do perfil do utilizador. A definição de privacidade disponibilizada pelos sites como definições padrão não deve ser deixada inalterada.

Quanto mais detalhes forem fornecidos, mais fácil será para um adversário utilizar essas informações para roubar a identidade ou cometer outros cibercrimes. Como tal, a partilha de informações deve ser limitada.

Antes de aceitarmos um pedido de amizade, devemos verificar completamente o perfil de quem faz o pedido. Podemos criar diferentes grupos para partilhar diferentes tipos de informações, como um grupo diferente para colegas e familiares.

PRÁTICAS PARA REDES PROFISSIONAIS

As redes profissionais são utilizadas principalmente para criar contactos e aumentar a visibilidade para possíveis empresas de recrutamento. Assim, para utilizarmos uma rede profissional com segurança, devemos procurar as informações fornecidas por outros utilizadores antes de os adicionarmos à nossa lista de contactos. Geralmente, um adversário não fornece muitos pormenores sobre a sua carreira.

O utilizador deve verificar se existe algum erro ortográfico ou gramatical no perfil de uma pessoa, pois se a pessoa está a candidatar-se a uma vaga de emprego, o perfil deve estar muito bem escrito e sem erros ortográficos ou gramaticais. Deve conter informações precisas e bem apresentadas sobre essa pessoa.

Verificar a consistência na carreira de uma pessoa pode ser uma boa prática se um utilizador pretender manter-se seguro numa rede profissional. Um perfil que muda constante e definitivamente num espaço de tempo curto é a parte mais utilizada como atração pelo invasor.

Devemos também cruzar as informações. Se uma pessoa afirma ser da empresa do empregador, o utilizador pode verificar o diretório da empresa e não deve hesitar em verificar junto do departamento de recursos humanos da empresa.

Atividade de aprendizagem 2

Peça aos alunos que expliquem quem eles acham que tem acesso à última publicação que fizeram na sua OSN favorita. Finalmente, ajude-os a verificarem as suas definições de privacidade e ver o que eles disseram que corresponde à verdade. Lance uma discussão em grupo sobre as respetivas conclusões.

Atividade de aprendizagem 3

Convide os alunos a olharem novamente para as cartas que receberam durante a **Atividade de Aprendizagem 1 desta Unidade** e pergunte-lhes se conseguem identificar riscos adicionais nas publicações das redes sociais apresentadas anteriormente. Pergunte-lhes o que fariam para mitigar esses riscos.

2. Resultados de aprendizagem para o módulo

Conhecimentos

Ciber-riscos e ciberameaças associados à utilização de redes sociais
Segurança de plataformas UGC (UGC = User Generated Content - Conteúdo gerado pelo utilizador)

Competências

Identificar diferentes tipos de ameças à cibersegurança

Aptidões

Prevenir e responder a ciberameaças nas redes sociais
Gerir palavras-passe complexas

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

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

MELHORAR A PREPARAÇÃO PARA A CIBERSEGURANÇA DO SETOR EUROPEU DO ENSINO E FORMAÇÃO PROFISSIONAL

MATERIAIS DE FORMAÇÃO

MATERIAL DE FORMAÇÃO DE SENSIBILIZAÇÃO PARA A CIBERSEGURANÇA PARA O SETOR DO EFP

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

INTRODUÇÃO

Desde o outono de 2021, relacionado com o Mês Europeu da Cibersegurança, até à primavera de 2022, os parceiros do projeto CYBER.VET.EU organizaram várias Game Jams nos países parceiros. Envolveram-se jovens que tiveram a oportunidade de estarem próximos dos temas de cibersegurança e de novas ferramentas.

O principal objetivo aqui foi resolver a necessidade de aumentar a sensibilização para a cibersegurança. Recorremos ao processo de "gamificação" com vista a obter uma solução fácil de adotar, rápida de implementar, escalável no tempo e inclusiva. O processo de gamificação, definido como "a aplicação de mecânicas de jogos a contextos não relacionados com jogos com o objetivo de induzir o envolvimento e aumentar os níveis de motivação", é uma forma comprovada de manter os utilizadores envolvidos em atividades de aprendizagem, com ótimos resultados mesmo num período curto de tempo graças ao aproveitamento do entretenimento que motiva os participantes a envolverem-se mais com o material e a praticarem. Como tal, este produto funcionará como uma combinação de diretrizes, formação e prática, com a característica de ser facilmente atualizável quando se adiciona novo material.

RESULTADOS DAS ATIVIDADES / GAME JAMS

- Maior consciência sobre segurança digital
- Maior consciência sobre segurança digital entre as comunidades dos participantes (família, amigos, colegas).
- Redução da taxa de sucesso de malware no seio das instituições Redução de eventos de fuga de dados
- Maior interesse pelo setor da cibersegurança como oportunidade de emprego.

ATIVIDADES

As atividades mais relevantes realizadas pelos parceiros espanhóis AEII e Inercia Digital:

Hackathon

GameJams

Dias de informações

Conferência internacional

Evento de disseminação

RESULTADOS

As sessões de Game Jam em Espanha proporcionaram alguns resultados úteis que podem ser vistos aqui:

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

Cybersecurity in Education

Os parceiros espanhóis AEII e Inercia Digital participaram online num Hackathon entre 20 e 22 de outubro de 2021, com 47 participantes, muitos deles especialistas em TI. https://www.comprometidosporelfuturo.com/proyectos# apoiado pela Boehringer Ingelheim em Espanha.

PROBLEMA PARA RESOLVER

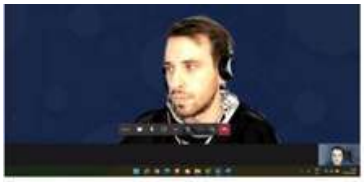
O ciberbullying é um dos principais riscos da Internet para os jovens. É comum encontrar publicações com conteúdos ofensivos para algumas pessoas e que são utilizadas com o intuito de assediar e gozar com as vítimas.

O ciberbullying provoca frequentemente perturbações graves nas vítimas, tais como perturbação de stress pós-traumático, depressão, pensamentos e comportamentos suicidas ou ansiedade.

Este desafio consiste em estudar e analisar o que os jovens sabem sobre segurança, assim como sensibilizá-los para os riscos que correm nos seus centros educativos e na vida quotidiana.
Este desafio procura, através da gamificação, a maior consciência de alunos e professores no dia a dia sobre questões relacionadas com a segurança na utilização de novas tecnologias.

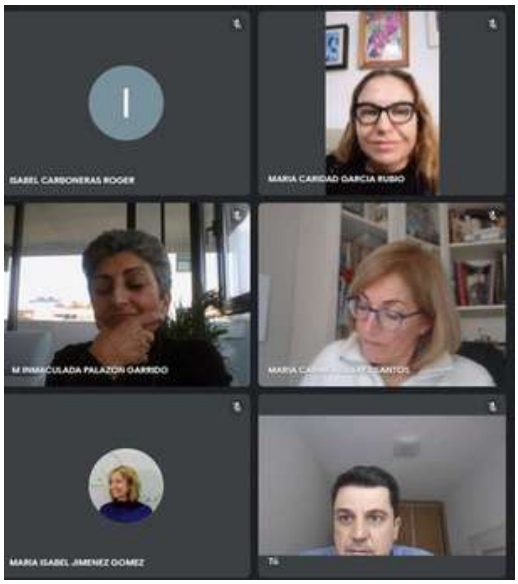
RESULTADOS

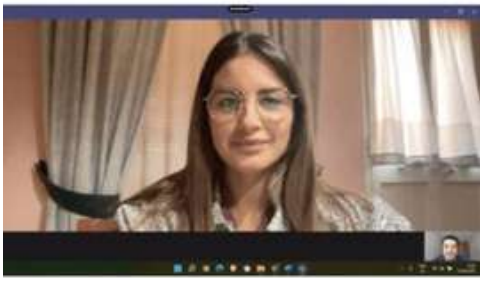
Jogo e animação ligados à cibersegurança na educação



Envolvimento da administração pública, escolas do EFP, especialistas de TI, professores, parceiro do projeto
Criação de pequenos vídeos

AEII / INERCIA DIGITAL [ES]





Em geral, após a realização de inúmeras pesquisas, o conhecimento de cibersegurança por parte de professores e alunos em centros de EFP ainda é reduzido em Espanha. Por este motivo, este projeto e outros idênticos são muito relevantes em Espanha.

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

GAME JAM

A NGO Nest Berlin, Extrafondente Open Source - EOS e IASIS realizaram uma sessão de Game Jam em fevereiro de 2022. A Game Jam teve início no sábado, dia 12, e durou 6 dias no total. As seleções nacionais desenvolveram e trabalharam em conjunto num rascunho de jogo (de um jogo online ou de tabuleiro).

Reuniu-se um júri independente a quem foi pedido que avaliasse o rascunho do jogo seguindo diretrizes comuns e um modelo de avaliação.

A equipa vencedora recebeu uma mentoria de 6 meses e recursos técnicos para desenvolver ainda mais a ideia do jogo.

SOBRE O JOGO

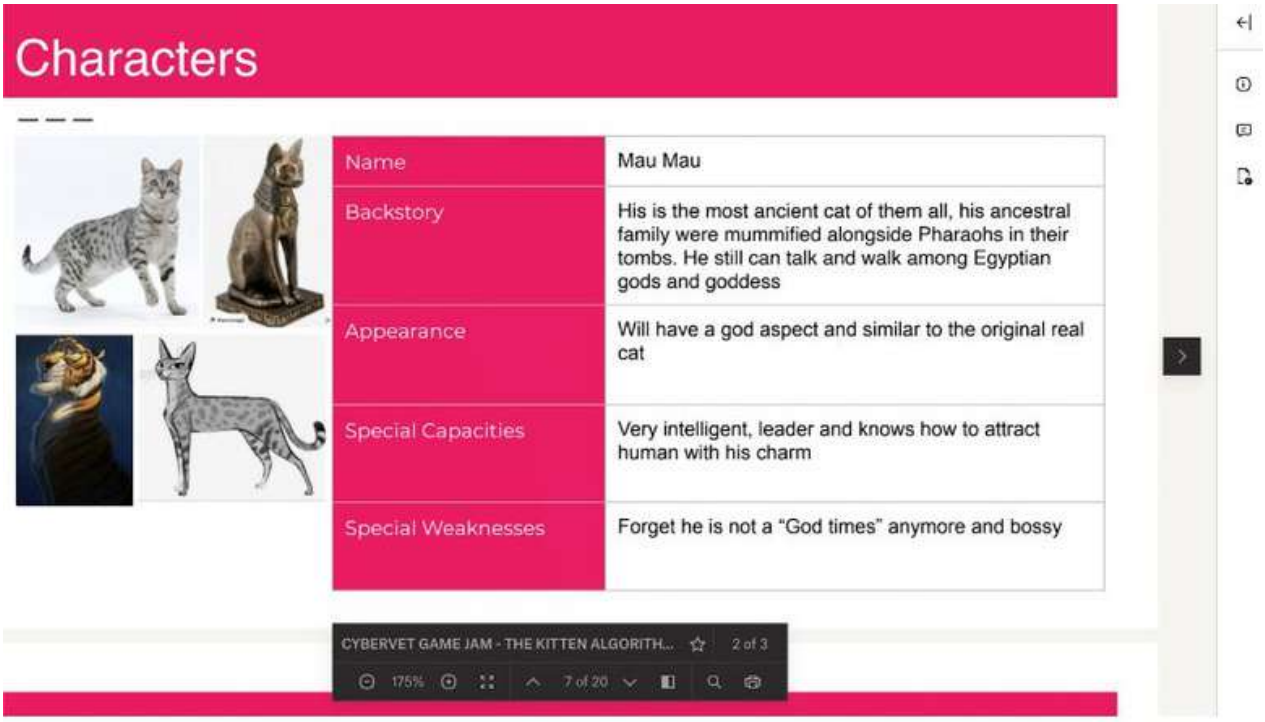
É um jogo de tabuleiro estratégico para 2 a 6 jogadores, que demora cerca de 30 a 60 minutos a ser jogado. Neste jogo, o jogador engana os humanos para os convencer de que é o melhor gato e ganha mais prestígio ao conseguir o maior número possível de servos de gatos humanos. Preste atenção, os outros gatos chefes tentarão ativamente sabotar o seu caminho para chegar aos humanos e ficarem eles com os louros. Não confie nas suas carinhas fofas!

O jogador perde o jogo se não tiver um número elevado de humanos como seus servos o se a 10ª rodada terminar e nenhum dos jogadores tiver, pelo menos, 4 humanos sob as suas ordens.

A dificuldade é que são 6 Chefes a tentarem enganar os humanos para serem seus servos e assim os chefes podem controlá-los, mas todos têm o mesmo objetivo e alguns podem até estar a ajudar os humanos a libertarem-se do controlo do gato.

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

Mau Mau



GAME JAM

O parceiro LECSA da Letónia organizou um evento Game Jam entre 27 de setembro e 1 de outubro de 2021. Devido às restrições epidemiológicas e diferentes localizações dos participantes, o evento foi organizado como um evento do tipo híbrido (presencial na Escola Técnica Saldus e via plataforma Zoom). Durante o evento, formaram-se 6 equipas (4-5 pessoas por equipa) para trabalharem no desenvolvimento de protótipos de jogos. Para alcançar alguns resultados tangíveis, o conceito Game Jam previu o desenvolvimento de dois tipos de jogos - jogos de computador e jogos de tabuleiro.

ATIVIDADES

Agosto - Setembro de 2021 foi dedicado ao planeamento e organização do evento (procura de especialistas em cibersegurança e desenvolvimento de jogos, distribuição de informações a potenciais participantes, planeamento da agenda e definição de critérios para o jogo, etc.)

Evento Multiplicador – Realidades nos Ciberataques (27.09.2021):
Introdução do projeto CYBER.EU.VET e palestra sobre as tendências nos ciberataques com Armins Palms, especialista em cibersegurança do CERT.LV (Instituto de Resposta a Incidentes de Segurança de TI da República da Letónia)
Número de participantes: 26 pessoas
Local: Escola Técnica de Saldus (cidade de Saldus) e plataforma ZOOM

Anúncio do Game Jam (27.09.2021): definição e discussão sobre os desafios reais em cibersegurança (avaliação de necessidades); formação de equipas, reunião com mentores e discussão sobre trabalhos futuros (workshop sobre o motor de jogo Unity), brainstorming sobre a ideia e o conceito do jogo.

Atividades de Game Jam em curso (28.09-30.09.2021): as equipas trabalharam no desenvolvimento de protótipos, sendo assegurada a consulta a mentores, se necessário

Apresentação do progresso (30.09.2021): apresentação sobre os conceitos do jogo e o progresso do trabalho para receber sugestões dos mentores.

Grande final (01.10.2021): quatro equipas apresentaram os seus resultados e os mentores avaliaram. Uma equipa, a desenvolver um jogo de computador, desistiu.
Conclusão do evento e discussão informal.
Número de participantes:
Local: Escola Técnica de Saldus e plataforma ZOOM

LECSA (LV)

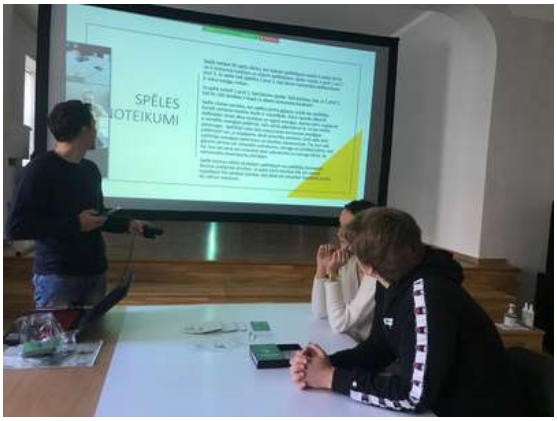
RESULTADOS

1.1. Protótipo de jogo online - The Virus

2. Jogo de tabuleiro - Cartas sobre segurança

3. Jogo de tabuleiro - Cyberwar

4.Jogo de cartas competitivo - Cyber Mind



EXEMPLO Cyber Mind - Um jogo de cartas competitivo

Este é um jogo de cartas educativo com elementos de questionário. A principal tarefa do jogo é ensinar os fundamentos da segurança quotidiana na Internet e aquilo que as pessoas se expõem quando fazem coisas tolas na Internet. Abrange tópicos como segurança na Internet e proteção de dados no contexto da utilização de redes sociais. No resultado do jogo, as pessoas (jogadores) devem ser capazes de reconhecer tentativas de fraude na vida real.

Desenvolvido pela equipa Veiksminieki (em letão: Pessoas de sucesso), alunos da Escola Técnica de Saldus durante o Game Jam na Letónia (outubro de 2021): Renars Ricards Hartmanis, Estere Ozoliņa, Sindija Diana Valtere e outros.

Nível: básico (para iniciantes). Grupo-alvo - alunos, estudantes, professores e pais

O jogo contém: 50 cartas, 2 blocos de saúde (para contar a saúde dos jogadores), 2 dados e carta de regras.

LECSA (LV)

GAME JAM

SOBRE

As tentativas de ciberataques em todo o mundo aumentam a cada dia que passa, como tal, o governo mundial teve a ideia de organizar um torneio para identificar pessoas que estão a trazer ciber-riscos e contra-atacá-las.

Jogo educativo que ajuda a aprender sobre os principais tipos de ciberataques, métodos de prevenção e eliminação, protegendo-se a si ou à sua equipa e contra-atacando o adversário. O objetivo do jogo é tirar todas as vidas do(s) adversário(s).

COMO JOGAR - JOGOS + REGRAS

Número de jogadores: 2 ou 4 pessoas (1 contra 1 ou 2 contra 2).

Cada jogador ou equipa (quando 2 contra 2) tem "100 vidas" (Saúde=HP) no início do jogo. A contagem da saúde é feita recorrendo a blocos de anotações pretos ou outras notas disponíveis.

Nomear uma pessoa para acompanhar e calcular o consumo de energia e saúde dos jogadores, se possível. Caso contrário, os jogadores fazem isso sozinhos.

Cada jogador recebe 5 cartas. Se o jogo for jogado 2 contra 2, ambos os jogadores terão "uma mão comum" na equipa ou 10 cartas juntas.

Existem três tipos de cartas: Cartas de ataque (vermelhas), Cartas de escudo (amarelas) e Cartas de Vida ou de Cura (verdes).

O jogo é jogado em rodadas. O jogador/equipa que obtiver o maior número no dado inicia o jogo.

Cada carta custa energia. No início de cada rodada, o jogador lança 2 dados para definir uma Energia que está indicada no topo da carta (a azul). As cartas têm de ser jogadas para que não exceda a sua quantidade de energia lançada.

O jogador/equipa que inicia a rodada pode atacar (com Cartas de Ataque), proteger-se (Cartas de Escudo) ou adicionar vida (Cartas de Cura), e os segundos só podem usar cartas de Ataque e Escudo para minimizar a sua vulnerabilidade de vida.

Lembre-se de que o número máximo de vidas por jogador/equipa durante o jogo pode ser de 100 HP (por exemplo, se a soma de vidas e energia após a rodada totalizar 110 HP, o seu número de vidas permanece – 100 HP).

O jogo termina assim que um jogador/equipa ficar sem todas as vidas (0 vidas).

Se o jogo ficar sem cartas, terá de baralhar as cartas da pilha novamente.

LECSA (LV)

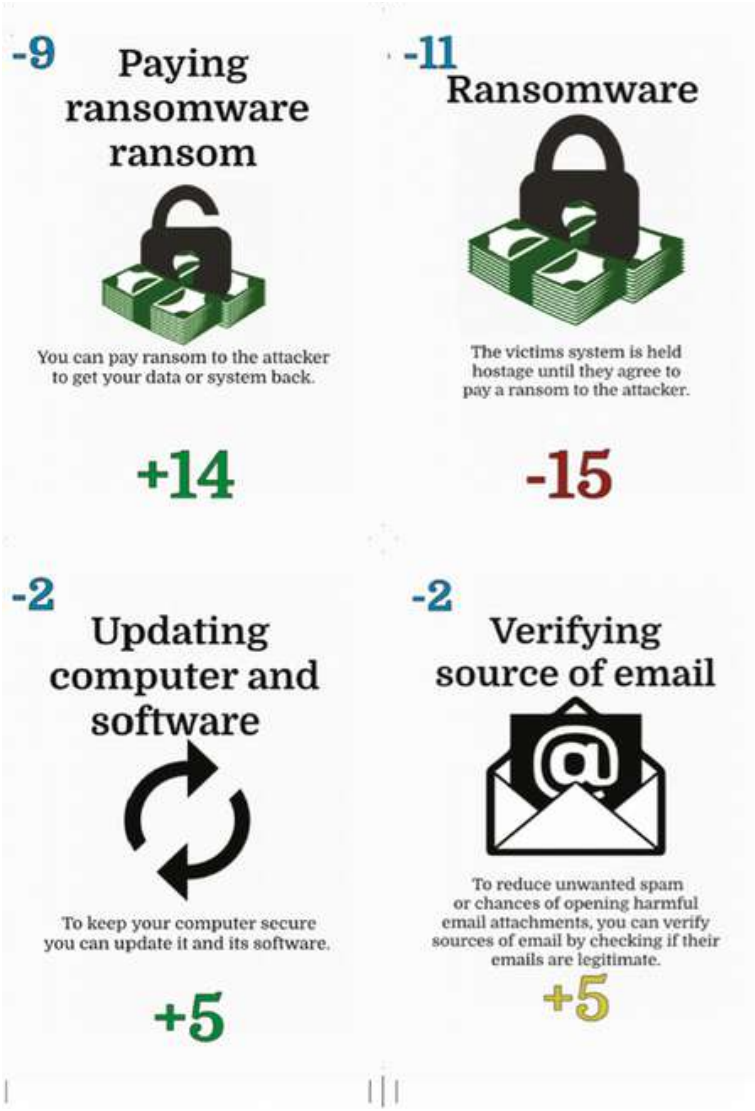
Exemplos de cartas

A **azul** – Energia

A **vermelho** - Cartas de ataque

A **amarelo** - Cartas de escudo

A **verde** - Cartas de cura



Exemplo para cálculo de saúde

EXEMPLO Cyberwar - Jogo de tabuleiro

Desenvolvido pela equipa Exodus (alunos da Escola Técnica de Saldus), líder da equipa Valdemārs Šperbergs.

2-6 jogadores< – > Adequado para maiores de 15

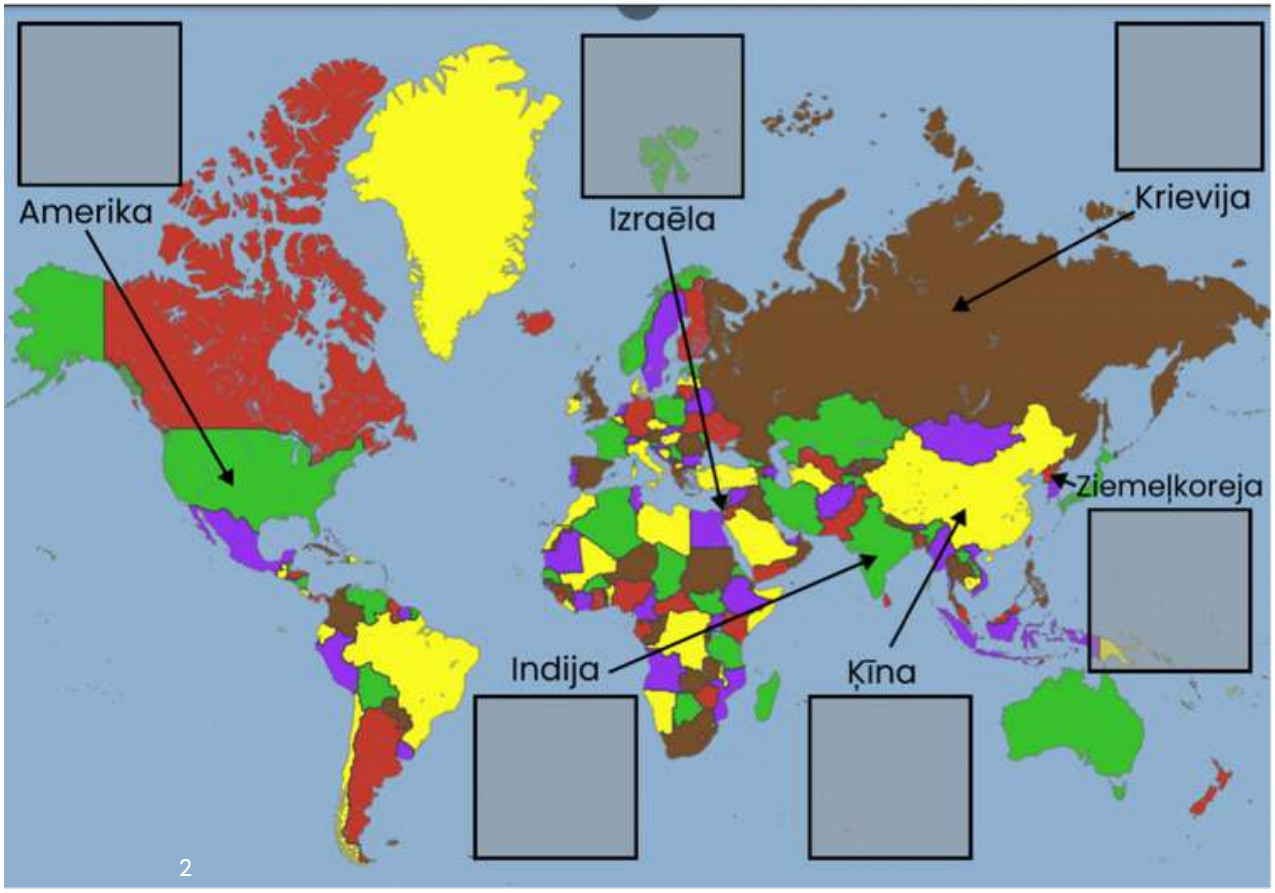
Um jogo de tabuleiro com uma forte ênfase em táticas e aleatoriedade (acaso).

Nível: jogo educativo para quem tem algum conhecimento sobre cibersegurança.

O jogo contém: Mapa-mundo, 2 dados, servidores, cartas com função "ataque", "defesa" ou "reação", legenda de vulnerabilidades.

SOBRE

O objetivo do jogo é proteger o país representado pelo jogador e atacar outros países para vencer a ciberguerra. No Cyberwar, cada jogador deve escolher um país para representar. Cada jogador tem um servidor com 3 vulnerabilidades. O objetivo do jogador é hackear servidores de outros países explorando duas das três vulnerabilidades ou corrigir duas das três vulnerabilidades no seu próprio servidor.



LECSA (LV)

COMO JOGAR

Os jogadores escolhem o país para representarem e colocam um objeto do servidor no local designado no mapa. Cada país tem os seus próprios bónus.

Cada jogador sorteia (pega) aleatoriamente 3 vulnerabilidades – uma de cada nível de dificuldade – e coloca-as viradas para baixo nos seus respetivos locais nos seus campos de servidor. As vulnerabilidades não são conhecidas pelos jogadores.

As vulnerabilidades têm 3 níveis de dificuldade. O nível de dificuldade também determina o número necessário para explorar uma vulnerabilidade (ver "Ataques"), assim como determina quantos movimentos serão necessários para corrigir a vulnerabilidade (ver "Defesa").

O jogo ocorre nas rodadas, as seguintes ações (movimentos) podem ser executadas – **Scanear, Ataque** e **Defesa**. Os jogadores determinam a sequência de jogadores lançando dois dados.

COMEÇAR

Cada jogador recebe 4 cartas no início de cada rodada. No fim da rodada, é possível manter 2 cartas ou trocá-las por outras já existentes.

A 1ª rodada é uma Rodada de Varredura na qual não é permitida nenhuma carta de Ataque ou Defesa. Nas rodadas posteriores, os jogadores podem optar por Scanear ou Atacar ou tentar reparar as suas vulnerabilidades (ver Defesa) O jogo continua rodada a rodada até que se alcance a vitória.

Scanear

O atacante escolhe um país para scanear a sua vulnerabilidade (por exemplo, "estou a scanear um segundo nível de vulnerabilidade russo").

Jogador scaneia – lança dois dados, aplicando o bónus do seu país representado, compara com o nível de dificuldade de vulnerabilidade + bónus do país da vítima.

Se o atacante tirar um número igual ou superior ao nível de dificuldade de vulnerabilidade da vítima, o atacante pode olhar para a vulnerabilidade scaneada.

Os bónus de país não são adicionados quando é o próprio a scanear.

Níveis de dificuldade

1º – o jogador deve tirar, pelo menos, o número 4 (excluindo os bónus do país)

2nd – player must roll at least 8 (excluding bonuses of the country)

3rd – player must roll at least 11 (excluding bonuses of the country).

ATAQUE

O jogador indica o alvo do ataque (por exemplo, "Eu ataco uma vulnerabilidade russa de nível 2") e revela a carta de ataque a todos os jogadores, colocando-a ao lado da vulnerabilidade.

O jogador lança o dado para ver se o ataque funciona comparando o número que tira com a dificuldade de vulnerabilidade + bónus (se o número tirado + bónus corresponder ou exceder a dificuldade, o ataque é bem-sucedido).

Os ataques podem ser forçados a recuar usando a Carta de Reação concebida para esse ataque. Cada ataque tem o seu próprio tipo de reação que pode ser jogado e o próprio tipo de vulnerabilidade para o qual funciona.

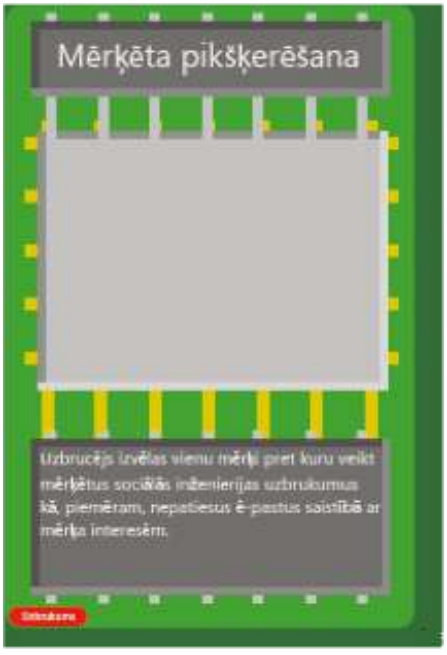
Se o ataque falhar ou for bloqueado por uma Carta de Reação - as cartas de Ataque e Reação jogadas permanecem na mesa até ao fim da próxima rodada e impedem o ataque por outros jogadores com o mesmo ataque pela mesma vulnerabilidade. Após a jogada, ambas as cartas voltam para o monte.

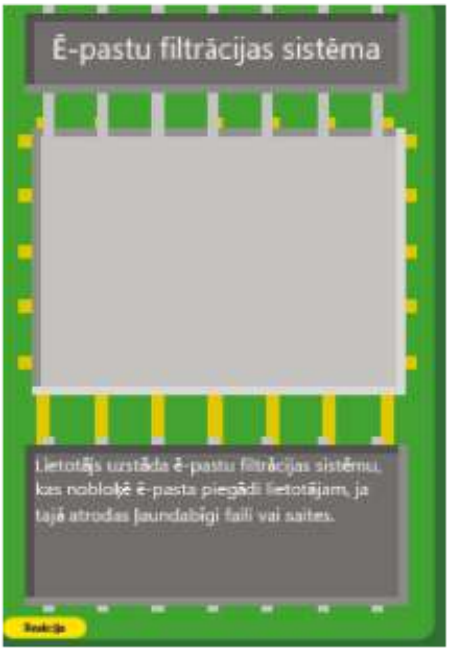
Níveis de dificuldade

1º – o jogador deve tirar, pelo menos, o número 4 (excluindo os bónus do país)

2º – o jogador deve tirar, pelo menos, 8 (excluindo os bónus do país)

3º – o jogador deve tirar, pelo menos, 11 (excluindo os bónus do país).





Defesa

Defesa – escolher o método certo contra uma vulnerabilidade específica. As Cartas de Reação param (cancelam) o ataque recebido (e todos os outros ataques direcionados à mesma vulnerabilidade) por 1 volta.

Para cancelar um ataque recebido, o jogador coloca uma Carta de Reação correspondente ao tipo de ataque (ver a tabela de vulnerabilidades) na carta de ataque
assim que o ataque é realizado.

Para começar a reparar um ferimento, o jogador coloca uma Carta de Defesa ao lado do ferimento a ser reparado.

Outros jogadores podem atacar este ferimento enquanto estiver na defesa (antes de a volta Defesa terminar). Quando o jogador tenta reparar um ferimento no seu servidor com uma Carta de Defesa, ele não pode atacar, mas pode tentar impedir ataques com Cartas de Reação. Para uma reparação completa, é necessário |nível de dificuldade + 1|
volta. A ação de scanear é permitida durante o período de reparação.

Se o método de defesa não for correto, o jogador salta 3 voltas e não pode usar cartas de defesa durante esse período (reações e ações de scanear são permitidas).

Bónus dos países

EUA: +2 scaneamento

Rússia: +2 para ataques

China: +2 para defesa contra ataques

Coreia do Norte: +2 para defesa contra scaneamento

Índia: +1 in all attacks, -1 against attacks

Israel: +3 em todos os ataques, -3 contra ataques

Vulnerabilities by levels

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

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

LECSA (LV)

SSH serveris

SSH serveris ar lietotājvārdu

Administrācijas panelis

Administrācijas panelis ar lietotājvārdu

Neapmācīts darbinieks

Ievainojams SMB protokols

XSS ievainojums

SQL injekcija

Rūtera panelis ar noklusējuma lietotājvārdu un paroli

XSS ievainojums ar filtru

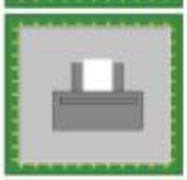
SQL injekcija ar filtru

Nepilnīgi nokonfigurēts ugunsmūris

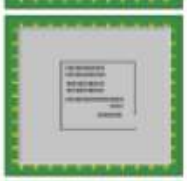
WiFi tīkls ar WEP drošību

Pakalpojuma atteices kļūda

Ievainojama OpenSSL programma



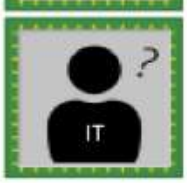
Ievainojama Print Spooler programma



Bufera pārpildes ievainojums

Vājš jaucējvērtības algoritms

Aizņemts priekšnieks



Slinks IT speciālists

LECSA (LV)

GAME JAM

DICAS E EXPERIÊNCIAS DA GAME JAM NA LETÓNIA

Durante o evento de 2 dias não é possível desenvolver um jogo de computador real, mas sim o primeiro protótipo, que poderá ou não ser desenvolvido dependendo da motivação dos participantes.

Prémios ou outros tipos de benefícios podem ajudar a envolver mais participantes e garantir melhores resultados (mais tangíveis) no fim (no nosso caso, pizza e bebidas foram fornecidas no fim do evento, apoio adicional dos mentores (por exemplo, colocando jogos na plataforma)).

Os mentores no desenvolvimento de jogos e questões de cibersegurança desempenham um papel importante na Game Jam, ao aconselhar e ajudar os participantes.

Planear com antecedência – pois este é um evento bastante complexo e requer um planeamento cuidadoso. Os organizadores devem ter em conta que algumas equipas podem ficar fora da competição (devido ao tempo limitado).

Por favor, ver as publicações do FB com os resultados do evento:
https://www.facebook.com/cybereuvetproject.eu/posts/138127645211214
https://www.facebook.com/saldustehnikums/posts/1780232175520378

O evento foi organizado pela LECSA em colaboração com Latvijas Universitāte | Ekonomikas un kultūras augstskola / EKA University of Applied Sciences | McĀbols | cert.lv | Coldwild Games | Saldus tehnikums!

MEATH PARTNERSHIP (IE)

ATIVIDADES

Reunião de informação de avaliação de necessidades com os alunos (formação de codificação numa instituição local de ensino de adultos)

Game Jam de 2 dias (sessão de informação online no 1º dia; 2º dia dedicado à Game Jam)

Evento Multiplicador – Manhã de Sensibilização para a Cibersegurança

DESCRIÇÃO E RESULTADOS

1) 1) Reunião de informação de avaliação de necessidades com os alunos
(Formação de codificação numa instituição local de ensino de adultos) Data: Outubro 2021

DESCRIÇÃO

Com o objetivo de disseminar o projeto e identificar os principais temas para a Game Jam, a equipa da Meath Partnership organizou uma sessão de informação com os alunos de uma turma de formação de Codificação local. A partilha de informações sobre Cibersegurança e discussão sobre as ameaças mais recentes foi seguida de uma sessão de brainstorming em grupo na qual os alunos foram divididos em dois grupos com vista a discutirem questões que levassem à identificação dos temas mais interessantes a explorar durante a Game Jam. Mais informações sobre a Game Jam e o projeto CYBER.EU.VET também foram partilhadas com os participantes do dia.

EXEMPLO PARA AVALIAÇÃO


YBER.VET.EU

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

Needs assessment meeting guidelines

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

MEATH PARTNERSHIP (IE)

RESULTADOS

Como resultado desta atividade, a equipe da Meath Partnership obteve uma maior compreensão do conhecimento geral dos alunos em relação à cibersegurança e ciberameaças, assim como informações recolhidas que foram posteriormente incluídas no processo de planeamento e implementação da Game Jam.

AVALIAÇÃO EM AÇÃO

MEATH PARTNERSHIP (IE)

GAME JAM

2) Game jam de dois dias
(sessão de informação online no 1º dia; 2º Dia dedicado à Game Jam)

DESCRIÇÃO

O DIA 1 foi dedicado às boas-vindas aos participantes e apresentação do projeto CYBER.EU.VET e à abertura da Game Jam, assim como à partilha de informações sobre os 2 temas identificados durante a reunião de avaliação de necessidades. Aos participantes foram oferecidas opções para trabalharem individualmente ou como parte de uma equipa. Também tiveram a oportunidade de tirar dúvidas ou ouvir mais esclarecimentos sobre os procedimentos
relacionados com o desenvolvimento dos jogos no dia 2.

O DIA 2 foi dedicado ao desenvolvimento dos jogos e os membros da nossa equipa e um especialista em suporte de TI estiveram disponíveis via Zoom para apoiar os participantes durante toda a duração da Game Jam entre as
9h e as 21h.
Os participantes foram convidados a fazerem o upload dos seus jogos na plataforma Itchio através de um perfil criado para efeitos deste evento: CYBER.EU.VET : Cybersecurity Game Jam - itch.io

RESULTADOS

Depois de os participantes partilharam os seus rascunhos de jogos com a equipa, um participante decidiu avançar e fazer o upload do jogo para uma avaliação mais aprofundada. Os restantes participantes decidiram não submeter os seus rascunhos, pois estavam em fases muito iniciais.

Click or not click

Online interactive cybersecurity game

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

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

Online interactive cybersecurity game:
https://itch.io/jam/cybereuvet-cybersecurity-gamejam

MEATH PARTNERSHIP (IE)

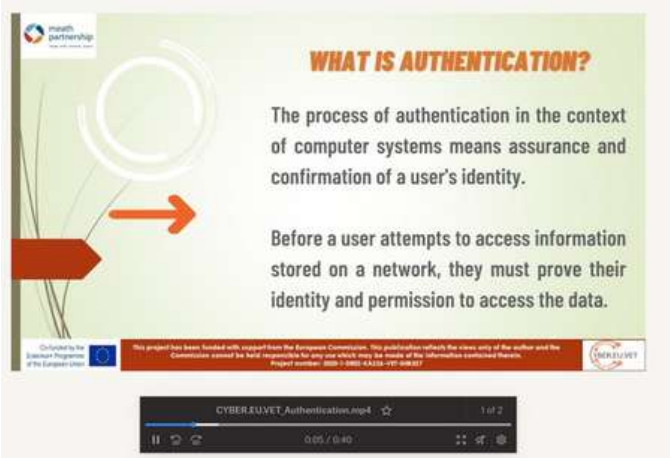
3) Evento Multiplicador – Manhã de Sensibilização para a Cibersegurança
Data: Novembro 2021

DESCRIÇÃO

O Evento Multiplicador foi realizado online Via Zoom com o objetivo de divulgar o projeto e as suas atividades. O evento foi amplamente divulgado entre as mais diversas partes interessadas ou envolvidas em Cibersegurança. O evento começou com uma apresentação e visão geral do projeto e do Game Jam, seguindo-se uma apresentação e discussão sobre Cibersegurança e partilha de informações práticas sobre como se manter online (foram possíveis as atuais ciberameaças e como eliminar possíveis ataques).

RESULTADOS

O Evento Multiplicador contribuiu para a divulgação do projeto e também criou a oportunidade de apresentar as concretizações alcançadas desde o início do projeto a um público mais alargado. Foi também uma grande oportunidade de partilhar informações práticas e conselhos relacionados com a cibersegurança com os participantes no evento.



COFAC / UNIVERSIDADE LUSÓFONA (PT)

GAME JAM

ATIVIDADES

1) Pós-graduação em Cyber & Ethical Hacking para futuros profissionais e professores no mercado Out 2021 – Fev 2022 (em parceria com uma consultora local chamada Cybersec Cybersec)

2) 2 sessões de Game Jam realizadas em janeiro de 2022 em escolas do EFP: Escola de Comércio de Lisboa :

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

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

3**)** Uma ciberformação de três dias e meio para alunos do ensino secundário em março de 2022 na Universidade Lusófona como parte do evento Tecweb - https://tecweb.ulusofona.pt

RESULTADOS

Evidência de relatório de divulgação onde se podem ver os diferentes testes que foram realizados durante um ano civil (abril de 2021 a abril de 2022). Neste relatório, podemos ver screenshots de publicações nas redes sociais, cartazes de diferentes eventos, questionários de sensibilização para a cibersegurança (disponíveis em português em https://docs.google.com/forms/d/e/1FAIpQLSeXACV_oeplRpTfbaC1NFKED76kRSYD6cT8cFMKjc7ohGMHZw/viewform)

DDurante os Cyberjams, também se criou, com base nos inquéritos de sensibilização para a cibersegurança, um conjunto de minijogos interativos/simples para o utilizador sobre situações simples realizadas.

TANDEM PLUS NETWORK – MEMBER IASIS [GR]

GAME JAM

Ferramenta de desenho de jogos (IASIS) - Cyberopolis

Este jogo é um jogo de tabuleiro destinado a pessoas interessadas em cibersegurança, com um máximo de 2 a 4 jogadores, e os seus principais aspetos são a confidencialidade e a integridade dos dados... e os tópicos abordados são o malware, phishing, ataques baseados na web, ataques de aplicações da web, spam, roubo de identidade, DDoS e Man in the middle...

Ver a imagem de ''Cyberopolis'' para compreender melhor os passos a seguir durante o jogo e quais os desafios a serem resolvidos...

Screenshots do jogo durante a sessão de Game Jam onde podemos ver o sucesso do jogo e o grande interesse demonstrado pelos participantes.

TANDEM PLUS NETWORK – MEMBER IASIS [GR]

VÍDEO - Preventing Cyberbullying

Este vídeo desenvolvido pelo parceiro grego aproxima os visitantes de diferentes formas de prevenir e combater o ciberbullying.

YBER.EU.VET

Funded by the European Union

AVISO LEGAL

Desenho
NGO Nest Berlin e.V.
Berlim, 2022

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