Módulo de aprendizagem

Cibercrime

Projeto: B-SAFE
Número: 2018-1CZ01-KA204-048148
Nome do autor: bit cz training
Última data de processamento: 28.10.2020

Cibercrime

Introdução

Certamente, já todos recebemos um *email* que a requerer a alteração de palavras-passe de contas bancárias ou a exigir o pagamento de faturas em atraso ou dívidas. Esses *emails* geralmente não têm uma aparência credível, não há uma identificação clara do remetente e a redação do texto tem muitas falhas. Mas muitas pessoas acabam por satisfazer a curiosidade muitas vezes por receio de estarem a negligenciar algo. A surpresa surge quando a sua conta bancária é acedida por intrusos e a dívida afinal é inválida. Por último, mas não menos importante, um dos exemplos de cibercrime mais comuns é a pirataria de *software*, ou seja, a utilização de uma cópia ilegal do *software*, sem respeito pelos direitos de autor e pelo seu preço. Estes são os exemplos da cibercriminalidade com que quase todas as pessoas que estão *online* contactam.

A cibercriminalidade é um fenómeno há muito estabelecido que está altamente relacionado com a conectividade global. Qualquer atividade criminosa que envolva um computador, quer como instrumento, alvo ou meio de perpetuação de outros crimes, insere-se na esfera do cibercrime. Uma definição generalizada de cibercrime é: "atos ilegais em que o computador é ou um instrumento ou um alvo ou ambos" (IT Act 2000).

O termo 'cibercrime' tem sido utilizado para descrever uma vasta gama de infrações, incluindo infrações contra dados e sistemas informáticos, falsificação e fraude relacionadas com computadores, infrações de conteúdo e infrações aos direitos de autor. A nossa crescente dependência de computadores e redes digitais torna a própria tecnologia num alvo tentador, quer para a obtenção de informação, quer como meio de causar perturbações e danos.

Relevância Prática – Assim poderás aplicar os conhecimentos e competências aqui adquiridos

Depois da análise deste módulo de aprendizagem, será possível apresentar definições dos principais termos relacionados com o crime no ciberespaço, reconhecer tipos e métodos de cibercrimes e apreender técnicas de proteção contra o crime vindo do espaço virtual. Também serão explorados os aspetos perigosos do crime cibernético, não só para os adultos, mas também para as crianças.

1.O papel do cibercrime na Internet

O cibercrime é o oposto da cibersegurança – compreende um enorme espetro de atividades prejudiciais e ilegais, levadas a cabo com recurso a computadores e à Internet. Este módulo de aprendizagem promove a compreensão do cibercrime e das medidas de proteção contra o mesmo, aplicáveis a adultos, crianças e organizações.

A maioria (mas não todos) os crimes cibernéticos são cometidos por cibercriminosos ou *hackers* que querem ganhar dinheiro. O cibercrime é levado a cabo por indivíduos ou organizações. Alguns cibercriminosos são metódicos, usam técnicas avançadas e são altamente qualificados tecnicamente. Outros são *hackers* principiantes. É raro o crime cibernético almejar o dano de computadores por outras razões que não o lucro. Contudo, as motivações para o crime podem ser políticas ou pessoais.

O que significa cibercrime? O cibercrime é definido como um crime em que um computador é o objeto do crime (*hacking*, *phishing*, *spamming*) ou é utilizado como uma ferramenta para cometer um crime (pornografia infantil, crimes de ódio).

Seguem-se alguns exemplos específicos de diferentes tipos de cibercrime:

- Fraude por *email* e pela Internet.
- Fraude de identidade (quando as informações pessoais são roubadas e usadas indevidamente).
- Roubo de dados financeiros ou de cartão bancário.
- Furto e venda de dados empresariais.
- Ciberextorsão (quando se exige dinheiro para evitar um ataque).
- Ataques de *ransomware* (um tipo de ciberextrorção).
- *Criptojacking* (quando os *hackers* extraem moedas criptográficas utilizando recursos alheios).
- Ciberespionagem (quando os *hackers* acedem a dados governamentais ou de empresas).

Quando falamos de crimes cibernéticos, de acordo com os exemplos acima mencionados, normalmente falamos de duas grandes categorias de infrações:

1. Um computador ligado a uma rede é o alvo da infração – aplica-se a ataques à confidencialidade, integridade ou disponibilidade da rede.

2. Uma infração cometida com a assistência de computadores ligados a uma rede e a tecnologias de informação e comunicação relacionadas - é o caso de ataques como roubo, fraude e falsificação.

O texto seguinte centra-se nas infrações cometidas com a ajuda de computadores.

Os crimes cibernéticos são compostos por vários grupos e categorias. Os diferentes tipos de cibercrimes são utilizados para descrever atos criminosos (tais como *phishing*, etc) e abrangem as categorias que se seguem.
Esta tipologia está centrada no objeto de proteção legal: "infrações contra a confidencialidade, integridade e disponibilidade de dados e sistemas informáticos", infrações relacionadas com o conteúdo e infrações relacionadas com os direitos de autor. A quarta categoria de "infrações relacionadas com informática" não se centra no objeto de proteção legal mas no método utilizado para cometer o crime. Podem existir algumas sobreposições entre categorias.

Categorias de cibercrime

Vamos agora examinar detalhadamente cada categoria:

Infrações contra a confidencialidade, integridade e disponibilidade de dados e sistemas informáticos

Todas as infrações nesta categoria são orientadas contra um dos três princípios legais de confidencialidade, integridade e disponibilidade.

- Acesso ilegal (*hacking*, *cracking*)
- Interceção ilegal (a interceção sem direito)
- Interferência de dados (introdução de códigos maliciosos, por exemplo, vírus)
- Interferência do sistema (introdução, transmissão, danificação, eliminação, deterioração, alteração ou supressão de dados informáticos, por exemplo, vírus que param ou abrandam os sistemas informáticos)

Exemplo
Em 2017, o ataque *WannaCry*, alegadamente lançado pela Coreia do Norte, desencadeou um tipo de resgate que não só bloqueou o conteúdo dos dispositivos dos utilizadores, como também se disseminou rapidamente. O *WannaCry* infetou 300.000 computadores em todo o mundo e foi exigido aos utilizadores que pagassem centenas de dólares para que se procedesse à desencriptação e restauração dos seus dados.

Infrações relacionadas com informática

Esta categoria abrange muitas infrações que requerem um sistema informático para serem cometidas. Ao contrário da categoria anterior, estas infrações amplas normalmente não são tão rigorosas em termos de proteção dos princípios legais.

- Fraude relacionada com a informática
- Falsificação relacionada com computadores

- *Phishing*
- Roubo de identidade
- Uso indevido de dispositivos

Exemplo
Em 2013-2016, a Yahoo sofreu uma violação de dados que levou ao roubo de 3 mil milhões de contas de utilizadores. Em alguns casos, os atacantes obtiveram informações privadas e senhas, passíveis de ser usadas para aceder a contas de utilizadores noutras plataformas *online*. Muitos destes dados estão atualmente disponíveis, gratuitamente ou por um preço, na *dark web*.

Infrações relacionadas com o conteúdo

Esta categoria abrange:

- Material erótico ou pornográfico
- Pornografia infantil
- Conteúdo xenófobo - racismo, discurso de ódio, glorificação de violência
- Insultos relacionados com símbolos religiosos
- Apostas ilegais e jogos *online*
- Calúnias e informação falsa
- *Spam* e ameaças associadas

O desenvolvimento de instrumentos jurídicos para lidar com esta categoria é muito mais influenciado pelas abordagens nacionais, que estão mais aptos a considerar os seus princípios culturais e jurídicos basilares. No que toca a conteúdos ilegais, os sistemas de valores e os sistemas jurídicos diferem muito entre sociedades.

Exemplo
Um pedófilo, ou seja, uma pessoa que se excita sexualmente com crianças, Matthew Falder, um académico britânico com um doutoramento da Universidade de Cambridge, foi acusado em 2017 de mais de 137 delitos cometidos contra 46 indivíduos, os quais incluíam o incentivo intencional à violação e actividade sexual com um membro da família menor, a incitação à exploração sexual de uma criança e a posse e distribuição de pornografia infantil, entre outros delitos (Dennison, 2018; Vernalls e McMenemy, 2018). Ele chantageou as suas vítimas para cometerem atos humilhantes, degradantes e abusivos contra si próprios (por exemplo, automutilação e lamber uma escova de sanita suja) e contra outros e gravou estes actos em imagens e vídeos (Davies, 2018; Dennison, 2018). Partilhou então as imagens e vídeos em *websites* de '*hurt core*' (como o *site Hurt 2 the Core*, agora extinto), especializados em violação, assassinato, sadismo, tortura, e conteúdo pedófilo (McMenemy, 2018).

Infrações relacionadas com direitos de autor

A digitalização abriu a porta a novas violações dos direitos de autor. As violações mais comuns dos direitos de autor incluem a troca de canções, ficheiros e *software* protegidos por direitos de autor em plataformas de partilha de ficheiros ou através de serviços de alojamento de partilha e a evasão aos sistemas de gestão de direitos digitais (DRM - *Digital Rights Management*). Esta é a categoria do cibercrime mais frequente e é geralmente tolerada por toda a sociedade mas todos devemos reconhecer que este é um ato ilegal com possíveis consequências, afeto a um comportamento incorreto.

Exemplo
Os exemplos mais frequentes de infrações relacionadas com os direitos de autor são a utilização de cópias ilegais de *software* em computadores pessoais ou o *download* da música ou filmes a partir de espaços públicos *online* (por exemplo *ShareRapid e MegaRapid*).

1.Aplicar conhecimento

Exercício de VERDADEIRO/FALSO

Situação: Se uma música ou filme é publicada na Internet, legalmente posso fazer um *download*.
Tarefa: Escolhe a opção certa considerando o princípio do verdadeiro/falso:

a) Verdadeiro
b) Falso

Exercício de ESCOLHA ÚNICA

Tarefa: Escolher a opção certa usando o princípio de escolha única: apenas uma frase é verdadeira.
Escolher as categorias corretas do cibercrime.

a) Infrações relacionadas com informática
b) Roubo físico de um computador, *tablet* ou telemóvel
c) Infrações relacionadas com o conteúdo
d) Infrações relacionadas com direitos de autor

Exercício de CORRESPONDÊNCIA DE RESPOSTAS

Tarefa: *Correspondência de respostas – selecione a opção correta do menu e arraste para a parte correta do texto*

_____ abrangem muitas infrações que requerem um sistema informático para serem cometidas. Ao contrário da categoria anterior, estas infrações amplas normalmente não são tão rigorosas em termos de proteção dos princípios legais.

_____ inclui violações de instrumentos legais mais influenciadas pelas abordagens nacionais, que estão mais aptas a considerar os seus princípios culturais e jurídicos basilares. No que toca a conteúdos ilegais, os sistemas de valores e os sistemas jurídicos diferem muito entre sociedades.

_____ incluem a troca de canções, ficheiros e *software* protegidos por direitos de autor em plataformas de partilha de ficheiros ou através de serviços de alojamento de partilha e a evasão aos sistemas de gestão de direitos digitais (DRM).

Infrações relacionadas com informática; Infrações relacionadas com o conteúdo; Infrações relacionadas com direitos de autor

2. Os métodos e exemplos do cibercrime

Até agora, foram apresentadas as quatro categorias que se distinguem quando se trata de crimes cibernéticos. Agora queremos analisar mais de perto **os papéis dos computadores no cibercrime e os métodos de ataque no ciberespaço**:

Os computadores desempenham quatro papéis nos crimes - servem como **objetos, sujeitos, ferramentas e símbolos**. Os computadores são objetos de crime quando são alterados ou roubados. Os computadores desempenham o papel de sujeitos quando são o contexto em que os crimes tecnológicos acontecem. Os ataques de vírus informáticos enquadram-se nesta categoria. Quando ocorrem crimes premeditados os computadores são os sujeitos dos ataques. O terceiro papel dos computadores no crime é como ferramentas, permitindo aos criminosos produzir informações falsas ou planear e controlar os crimes. Finalmente, os computadores são também utilizados como símbolos para enganar as vítimas.
O mais comum é o computador assumir a forma de sujeito. Os principais métodos de utilização de um computador como sujeito criminal são:

- *Malware*
- *Hacking*
- *Spam*
- *Phishing*
- Ataques distribuídos de negação de serviços (DDoS – *Distributed Denial of Service*, em inglês)

O principal método de ataque

Definição
O ***malware*** é um rótulo geral atribuído a *software* malicioso que se espalha entre computadores e interfere com as operações informáticas. O *malware* pode ser destrutivo, por exemplo, apagando ficheiros ou causando falhas no sistema, mas também pode ser utilizado para roubar dados pessoais.

Há muitas **formas de *malware***. Algumas delas são as seguintes:

- Os **vírus** podem causar disfunções leves do computador, mas também podem ter efeitos mais graves em termos de danificar ou apagar *hardware*, *software* ou ficheiros.

- Os ***worms*** são programas auto-replicáveis, que podem propagar-se autonomamente, dentro e entre computadores, sem necessitarem de um hospedeiro ou de qualquer acção humana. O impacto dos *worms* pode, portanto, ser mais severo do que os vírus, destruindo redes inteiras.
- Os ***Trojans*** são formas de *malware* que parecem ser programas legítimos, mas que facilitam o acesso ilegal a um computador. Conseguem desempenhar funções, tais como roubar dados, sem o conhecimento do utilizador e podem enganar os utilizadores, realizando uma tarefa de rotina enquanto realizam acções ocultas e não autorizadas.
- ***Spyware*** é um *software* que invade a privacidade dos utilizadores ao recolher informações sensíveis ou pessoais de sistemas infectados e ao monitorizar os *websites* visitados.

Definição
O ***hacking*** (também apelidado de pirataria informática) é um processo comum que resulta na violação da privacidade e da informação confidencial de alguém. Os pontos fracos de um sistema ou as lacunas de uma rede são identificados e os detalhes privados são acedidos. Por conseguinte, o *hacking* é também conhecido como uma intrusão não autorizada.

Contudo, o *hacking* nem sempre é visto como roubo e pode até ser utilizado para causas produtivas. Esse tipo de *hacking* que envolve boas intenções é conhecido como *hacking* ético. Este tipo de *hacking* é feito para proteger o sistema operativo.

Os *hackers* podem ser agrupados em diferentes categorias, tais como *White Hat* (chapéu branco), *Black Hat* (chapéu preto), e *Grey Hat* (chapéu cinzento), com base na sua intenção de *hacking* de um sistema.

Hackers White Hat (chapéu branco) – *Hackers* éticos
Estes *hackers* não têm intenção de prejudicar um sistema, mas sim de tentar descobrir debilidades num computador ou num sistema em rede, como parte de testes de penetração e avaliações de vulnerabilidade. O *hacking* ético é legal e é um dos trabalhos mais exigentes disponíveis na indústria das Tecnologias da Informação. Várias empresas contratam *hackers* éticos para conduzirem testes de penetração e avaliações de vulnerabilidade.

Hackers Grey Hat (chapéu cinzento)
São uma mistura de *hackers Black Hat* e *White Hat*. Agem sem intenção maliciosa mas, para se divertirem, exploram uma fraqueza de segurança num sistema ou rede informática sem a permissão ou conhecimento do proprietário. Pretendem chamar a atenção dos proprietários para a debilidade securitária e obter apreço ou uma pequena recompensa por parte dos proprietários.

Hackers Black Hat (chapéu preto) – *crackers*
Estes *hackers* pirateiam para obter acesso não autorizado a um sistema e prejudicar as suas operações ou roubar informação sensível. O *hacking* de *Black Hats*, considerado pirataria informática, é sempre ilegal devido à sua intenção maliciosa que inclui roubar dados empresariais, violar a privacidade, danificar o sistema operativo, bloquear a comunicação em rede, etc.

Definição

O ***spam*** é correio electrónico não solicitado ou lixo electrónico, normalmente enviado em massa para inúmeros destinatários em todo o mundo e está frequentemente relacionado com produtos farmacêuticos ou pornografia. O *email* de *spam* é também utilizado para enviar *emails* de *phishing* ou *malware* e pode ajudar a maximizar potenciais retornos para os criminosos.

O crime está a afastar-se dos métodos tradicionais como a violência, as drogas ou os assaltos, ao passo que a criminalidade através da Internet está a tornar-se mais prevalecente. Isto vai de encontro à tendência resultante do aumento dos negócios e comunicação *online*. As vítimas do cibercrime podem perder tudo o que tem valor - segurança, paz, dinheiro ou propriedade.

Estudo

O primeiro estudo a examinar o impacto emocional da cibercriminalidade, mostra que as vítimas tendem a sentir-se zangadas (58%), irritadas (51%) e enganadas (40%), e em muitos casos, culpam-se a si próprias por serem atacadas. Apenas 3% pensam que isso não lhes vai acontecer, e quase 80% não esperam que os cibercriminosos sejam levados à justiça - resultando numa relutância irónica em agir e numa sensação de impotência.

Definição

Phishing **-** Uma campanha de *phishing* involve *emails* de *spam* ou outras formas de comunicação, enviadas em massa, com a intenção de enganar os destinatários para que façam algo que prejudique a sua segurança ou a segurança da organização para a qual trabalham. As mensagens das campanhas de *phishing* podem conter anexos infectados ou ligações a sites maliciosos. Também é possível que peçam ao recetor que divulgue informações confidenciais.

Exemplo

Um famoso exemplo de um esquema de *phishing* teve lugar durante o Campeonato do Mundo de Futebol de 2018. De acordo com relatórios da Inc, o esquema de *phishing* do Mundial de 2008 envolveu *emails* enviados a adeptos de futebol, os quais tentaram atrair os adeptos com falsas viagens gratuitas a Moscovo, onde o Campeonato do Mundo estava a ser organizado. As pessoas que abriram e clicaram nos *links* contidos nestes *emails* tiveram os seus dados pessoais roubados.

Definição

Os **Ataques distribuídos de negação de serviços** (**DDoS -** Distributed DoS attacks) são um tipo de ataque cibernético que os cibercriminosos utilizam para derrubar um sistema ou rede. Por vezes, dispositivos IoT (Internet das coisas) interligados são utilizados para lançar ataques DDoS. Um ataque DDoS sobrecarrega um sistema através de um dos protocolos de comunicação padrão que utiliza para enviar *spam* ao sistema com pedidos de ligação.

Exemplo

Um exemplo famoso deste tipo de ofensiva é o ataque DDoS de 2017, no *website* da Lotaria Nacional do Reino Unido. Isto levou o *site* e a aplicação móvel da lotaria a ficarem *offline*, impedindo os cidadãos do Reino Unido de jogar.

Os cibercrimes mais frequentemente cometidos incluem os seguintes:

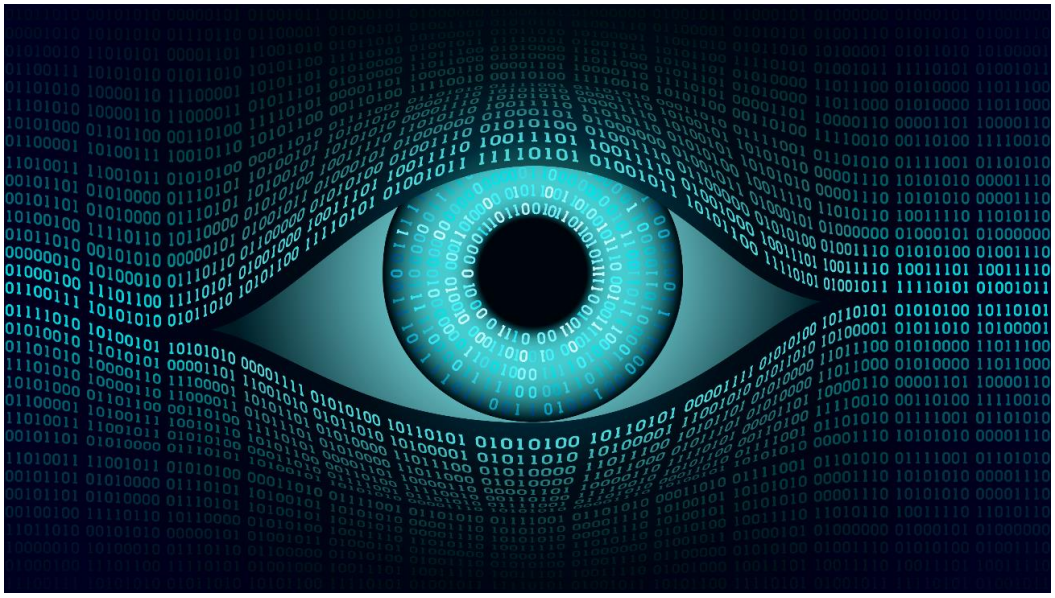
Personificação *online*

Este crime é um dos mais comuns. Para este ato criminoso é habitual utilizar o nome, endereço de domínio, número de telefone ou qualquer outra informação identificativa de outra pessoa sem consentimento e causar danos ou cometer fraude, o que é um crime.

Exemplo
A Claire começou a ser assediada por estranhos depois de alguém ter feito um *post* na Internet a oferecer serviços sexuais em seu nome. A publicação continha informação privada, incluindo o seu número de telefone e endereço domiciliário.

Ciberstalking

A perseguição física pode assumir várias formas, incluindo seguir fisicamente uma pessoa, observá-la secretamente, ligar persistentemente e enviar mensagens de texto manipulativas, entre outros meios para abordar a vítima de forma inesperada. A diferença da perseguição cibernética é que esta última está dependente da tecnologia online, como o *email*, redes sociais, mensagens instantâneas, dados pessoais disponíveis *online* - tudo na Internet pode ser utilizado pelos *cyberstalkers* para fazer um contacto inapropriado com as suas vítimas.



Exemplo
Depois de o John e a sua namorada se separarem, ele começou a persegui-la, tendo colocado um telemóvel pré-pago com GPS debaixo do carro dela. O John rastreava os movimentos da sua ex-namorada e seguiu-a entrando na sua conta de telemóvel *online*. John também telefonava à sua ex mais de 200 vezes por dia.

Ciberbullying

O ciberbullying acontece quando as pessoas usam as redes sociais ou a Internet para intimidar, assediar, ameaçar ou depreciar os outros. Em geral, se uma pessoa utiliza a Internet ou qualquer outra forma de comunicação eletrónica para ameaçar, assediar ou assustar outra pessoa, essa conduta pode ser um crime.

Exemplos

Enquanto viaja com a sua equipa de hóquei, um dos jogadores tira uma foto embaraçosa de uma rapariga que conheceu no ringue. Depois publica a foto no Facebook e envia-a a todos os outros jogadores da equipa. A foto é então difundida.

Três dos companheiros de equipa do Paul enviam-lhe mensagens, culpando-o pela perda da equipa e dizendo-lhe que ele não sabe jogar. O Paul tem medo de dizer ao seu treinador e aos seus pais e, por isso, sofre de *bullying* em silêncio durante toda a época de hóquei. Ele não regressa ao hóquei na época seguinte.

Qual é a diferença entre ciberbullying e *ciberstalking*?

Ciberbullying	*Ciberstalking*
O ciberbullying implica um contacto constante com a pessoa; dizer coisas danosas à pessoa ou divulgar informações falsas sobre a pessoa. Por exemplo, o infrator cria um grupo do Facebook intitulado "Eu odeio..." e convida todos os amigos a juntarem-se ao grupo.	*Ciberstalking* é uma obsessão por descobrir o máximo possível sobre uma pessoa (sem realmente lhe perguntar). Por exemplo, o infrator descobre onde a pessoa nasceu, se a pessoa é casada, etc.

Roubo de identidade e roubo de dados

O *roubo de identidade* é o ato de roubar informações pessoais e identificativas com o intuito de cometer atos ilegais, tais como: abrir uma linha de crédito, alugar uma casa, comprar bens ou serviços, ou cometer fraude ou extorsão relacionada com leilões ou salários.

O *furto de dados* é o ato de possuir ilegalmente dados sensíveis, o que inclui informações não encriptadas de cartões de crédito armazenadas em empresas, segredos comerciais, propriedade intelectual, código-fonte, informações de clientes e registos de empregados.

Example
O Marriott foi *hackeado* em 2018, quando 383 milhões de registos de hóspedes e mais de 5 milhões de números de passaportes foram roubados, o que levou a um aumento em frequência e gravidade das violações de dados. Estes dados podem ser vendidos no mercado negro e qualquer pessoa pode fazer uso delas e utilizar outra identidade.

Crimes financeiros

Esta categoria inclui atividades que geram lucro desonestamente para todos os envolvidos na conduta em questão. Consiste na exploração de informação privilegiada ou na aquisição da propriedade de outra pessoa através do engano, para assegurar um benefício material. O crime financeiro geralmente compreende o seguinte: fraude, branqueamento de capitais, suborno e corrupção, entre muitos outros.

Exemplo
Alguns crimes financeiros recentes de grande visibilidade incluem o escândalo Enron, a empresa de energia que cometeu fraude e corrupção generalizadas e o escândalo de investimento do Bernie Madoff, quando Madoff fingiu ter uma empresa de investimento bem-sucedida, mas na realidade ele estava apenas a roubar dinheiro a novos clientes e a dá-lo a clientes mais antigos (a isso chama-se um esquema Ponzi e Madoff geria o maior da história). Madoff foi condenado por numerosos crimes, incluindo branqueamento de capitais e vários tipos diferentes de fraude.

O cibercrime é frequentemente cometido por alguém que se encontra próximo das vítimas - por exemplo, dentro de uma empresa atacada. Este tipo de cibercrime é chamado fraude interna e refere-se a um tipo de fraude que é cometida por um indivíduo contra uma organização. Neste tipo de fraude, o autor da fraude envolve-se em atividades que são concebidas para defraudar, desviar propriedade, contornar os regulamentos, leis ou políticas de uma empresa. Por exemplo, a fraude interna envolve atividades tais como a não comunicação intencional de transações, a realização de transações não autorizadas e a marcação intencionalmente errada de posições.
A fraude interna pode ser dividida em duas grandes categorias: desvio de fundos e roubo de identidade. No caso de desvio de fundos, o dinheiro é retirado diretamente das organizações e no caso de roubo de identidade, as informações pessoais de um cliente são desviadas pelo funcionário para obter lucro. Exemplos de fraude interna incluem:

- Roubo do dinheiro de um cliente
- Abuso do crédito de um cliente
- Lavagem de dinheiro
- Fraude de compras
- Roubo de dados

Por outro lado, as atividades fraudulentas de pessoas externas à empresa chamam-se fraude externa. Envolvem o roubo de dinheiro ou de ações por pessoas externas à empresa. Exemplos de fraude externa incluem:

- Roubo de identidade - assumir o controlo de uma identidade virtual da pessoa
- Falsificação dos dados da fatura - alterando o número de conta do beneficiário
- Falsificação dos detalhes da encomenda para que as mercadorias sejam entregues no destino errado
- Imitação da voz de uma pessoa ou falsificação da sua assinatura
- Falsificação de *emails*

Os ciberataques têm vários propósitos, desde os moderados aos mais impiedosos, sendo os 4 mais típicos:

- Vandalismo (ataques comuns a *websites* governamentais)
- Propaganda (divulgação de notícias políticas, principalmente através da Internet)
- Recusa de acesso (ataques contra, por exemplo, forças armadas que usam computadores e satélites para as comunicações)
- Ataques em rede contra infraestruturas (ataques aos sistemas de transmissão das empresas de indústrias como engenharia de energia, indústria do gás, indústria do aquecimento, indústria petrolífera e infraestruturas de comunicação, sensíveis aos ciberataques, etc.)

1.Aplicar conhecimento

Exercício de ESCOLHA ÚNICA

Situação: O que são ataques distribuídos de negação de serviços (DDoS - Distributed DoS attacks)?
Tarefa: Escolher a opção certa usando o princípio de escolha única: apenas uma frase é verdadeira.

a) Quando são enviados em massa *emails* de *spam* ou outras formas de comunicação
b) Um tipo de ataque de cibernético que os cibercriminosos utilizam para derrubar um sistema ou rede

c) Correio eletrónico não solicitado ou lixo eletrónico normalmente enviado em massa para imensos destinatários em todo o mundo
d) Utilização ou acesso não autorizado a computadores ou recursos de rede, para explorar vulnerabilidades de segurança identificadas nas redes

Exercício de ESCOLHA ÚNICA

Situação: O que faz um *hacker* "*grey hat*"?
Tarefa: Escolher a opção certa usando o princípio de escolha única: apenas uma frase é verdadeira.

a) Espalha informações falsas sobre outra pessoa
b) É uma pessoa que tenta roubar informação de identificação pessoal
c) É uma pessoa que obtém acesso a um sistema de alguém sem autorização, apenas por diversão
d) É uma pessoa que é responsável por muitos crimes financeiros através da Internet

Exercício de ESCOLHA ÚNICA

Situação: O que é a fraude interna?
Tarefa: Escolher a opção certa usando o princípio de escolha única: apenas uma frase é verdadeira.

a) A fraude interna é cometida pelos fornecedores no caso de não fornecerem a tempo o serviço ou mercadoria acordada.
b) A fraude interna envolve atividades como o aliciamento ou o ciberstalking.
c) A fraude interna é cometida por funcionários em caso de realização de transações financeiras não autorizadas.
d) A fraude interna é cometida por clientes da empresa através da apresentação de uma queixa injustificada.

3.Impacto do cibercrime

Os computadores também podem ser usados para cometer crimes do domínio real e físico (violações de direitos de propriedade, fraudes de cartões de crédito, fraudes de transferência de fundos eletrónicos, pornografia, etc.) e até mesmo terrorismo. Os terroristas utilizam frequentemente a tecnologia para planear e executar as suas atividades criminosas. A essa prática chamamos ciberterrorismo. O aumento da interação internacional e a utilização generalizada das tecnologias de informação tem facilitado o crescimento da criminalidade e do terrorismo. Devido aos avanços na tecnologia de comunicação, as pessoas não precisam de estar num determinado país para organizar um crime dessa natureza. Assim, os terroristas e os criminosos conseguem encontrar lacunas de segurança nos sistemas de maneira a operacionalizar as suas atividades a partir de locais inesperados, em vez do seu país de residência.

A maioria dos futuros incidentes internacionais terão uma dimensão cibernética. Por conseguinte, é oportuno considerar a avaliação destes ataques. Nos dias que correm, há debates sobre a possibilidade da escalada dos incidentes para um conflito de guerra insustentável, onde pode ocorrer morte, destruição, ferimentos pessoais ou danos materiais. O problema é que a atribuição de ações a um determinado estado é quase impossível. É difícil reconhecer um atacante em particular sem uma cooperação precisa do Estado em cujo território o atacante se encontra.

Para os indivíduos

Violações de dados, roubo de identidade, problemas com dispositivos: o cibercrime pode ter um grande impacto nos indivíduos. Qualquer indivíduo pode ter de lidar com cobranças suspeitas no seu cartão de crédito resultantes de um roubo de identidade, um ataque chantagista exigindo centenas ou milhares para libertar ficheiros pessoais e custos dispendiosos para voltar a dar acesso aos dados causados por *criptojacking* ou *botnets*. As consequências podem ser ainda piores do que prejuízos monetários quando o ciberbullying, incluindo o assédio sexual, é uma fonte de tormentas.

Para as empresas e governos

Tanto as empresas como as organizações de saúde e os governos podem sofrer com a perda de dados sensíveis, enormes encargos financeiros e danos à própria marca. Os ataques de resgates contra pequenas e médias empresas em 2019 exigiram, em média, $5.900 para desbloquear os seus ficheiros ou sistemas. Para além disso, em algumas situações, o tempo de inatividade imputado por estes ataques custou às empresas afetadas, em média, $141.000. Isto para não falar dos ataques de resgate aos governos, tal como o ataque que levou o condado de Jackson, na Geórgia (EUA), a pagar $400.000 para restaurar os seus sistemas e infraestruturas tecnológicas.

Outro termo bastante usado neste contexto é guerra cibernética. Vejamos estes dois termos em pormenor:

O que é o ciberterrorismo?	O que é uma guerra cibernética?
O conceito de cibercrime é muitas vezes confundido com ciberterrorismo. O ciberterrorismo é sempre mais severo do que outros comportamentos levados a cabo no ou através do ciberespaço. A NATO define o ciberterrorismo como um "ciberataque que usa ou explora redes informáticas ou de comunicação para causar destruição ou perturbação suficientes para gerar medo ou intimidar uma sociedade por forma a atingir um objetivo ideológico".	A guerra cibernética envolve a utilização e o ataque a computadores e redes num cenário de guerra. Esta prática envolve operações ofensivas e defensivas relacionadas com a ameaça de ciberataques, espionagem e sabotagem. A guerra cibernética define-se como as "ações de um Estado-nação para penetrar nos computadores ou redes de outra nação de modo a causar danos ou perturbações".

Exemplo
As guerras cibernéticas, incluindo ataques a redes, ganharam alguma relevância adicional desde o 11 de setembro. Os ataques de 11 de setembro incitaram uma discussão intensiva sobre a utilização das tecnologias de informação e comunicação por terroristas. Esta discussão foi facilitada por relatos de que os infratores usaram a Internet na preparação do ataque. Apesar de os ataques não terem sido ciberataques, a Internet desempenhou um papel importante na preparação da infração. Neste contexto, foram descobertas diferentes formas de utilização da Internet pelas organizações terroristas.

2.Aplicar conhecimento

Exercício de ESCOLHA ÚNICA

Objetivo específico associado: OE_ Saber o papel do cibercrime na Internet_01_07: Saber explicar o que é uma guerra cibernética.

Situação: Qual é o pior tipo de ciberataque que ocorre num contexto de crimes reais e físicos?
Tarefa: Escolher a opção certa usando o princípio de escolha única: apenas uma frase é verdadeira.

a) Fraude de cartão de crédito
b) Pornografia
c) Ciberterrorismo
d) Roubo de identidade

Exercício de ESCOLHA MÚLTIPLA

Tarefa: Escolher as opções corretas usando o princípio da escolha múltipla: pode haver mais do que uma resposta certa.
Qual o impacto que o cibercrime pode ter para a pessoa?

a) Roubo de identidade
b) Desemprego
c) Problemas de saúde
d) Violações de dados

Exercício de PREENCHER O ESPAÇO

Tarefa: Selecione a opção correta do menu e arraste para a parte correta do texto

_____ podem sofrer com a perda de dados sensíveis, enormes encargos financeiros, e danos à marca

4.Possibilidades de prevenção e proteção

Tudo desde dinheiro roubado, roubo de dados pessoais e/ou financeiros, perda de produtividade e danos e destruição de dados empresariais ou individuais críticos é classificado como crime cibernético. Infelizmente, os *hackers* e outros indivíduos que cometem cibercrimes estão a tornar as suas práticas cada vez mais sofisticadas.

Quais são as melhores maneiras de proteger computadores e dados pessoais?

A melhor forma de proteção contra a cibercriminalidade é a prevenção. Para a segurança *online*, é importante ter em mente cinco pontos-chave: **Precaução, Prevenção, Proteção, Preservação e Perseverança**.

Estes pontos são fundamentais em todas as seguintes recomendações para a segurança *online*:

1. Evitar a divulgação de informações pessoais na Internet e em *emails*
2. Considerar cuidadosamente o envio de qualquer fotografia *online* - qualquer pessoa pode utilizá-la em qualquer altura noutro contexto
3. Utilizar palavras-passe fortes
4. Utilizar e manter atualizado o *software* antivírus
5. Evitar o envio do número do cartão de crédito e de palavras-passe por *email*
6. Prestar atenção aos sites visitados pelas crianças
7. Manter uma cópia de segurança dos dados para prevenir a perda de informação devido a ataques de vírus
8. Utilizar um programa de segurança que permita controlar os *cookies*
9. Manter o *software* e o sistema operativo atualizados
10. Nunca abrir anexos em *emails* de *spam*
11. Não clicar em *links* vindos de *emails* de *spam* ou em *websites* não confiáveis
12. Contactar diretamente as empresas no caso de surgirem pedidos suspeitos
13. Monitorizar continuamente os extratos bancários
14. Ser cauteloso com os *websites* visitados

Como perceber quais *websites* são seguros?

As 3 dicas de segurança dos *websites* descritas de seguida são úteis para afastar incertezas e identificar se um *site* é ou não digno de confiança. Primeiro, serão apresentadas algumas dicas de verificações visuais simples que darão informações úteis num relance. Depois, serão sugeridas ferramentas de segurança de *websites* que poderão dar apoio no sentido de informar e orientar para a redução de riscos. Finalmente, serão cedidas diretrizes para pesquisar com maior detalhe este tema, caso ainda existam algumas dúvidas. A partir de agora, vamos ser atentos e voltar a divertir-nos enquanto navegamos na *Web*.

1 - Verificações visuais de segurança de *websites*

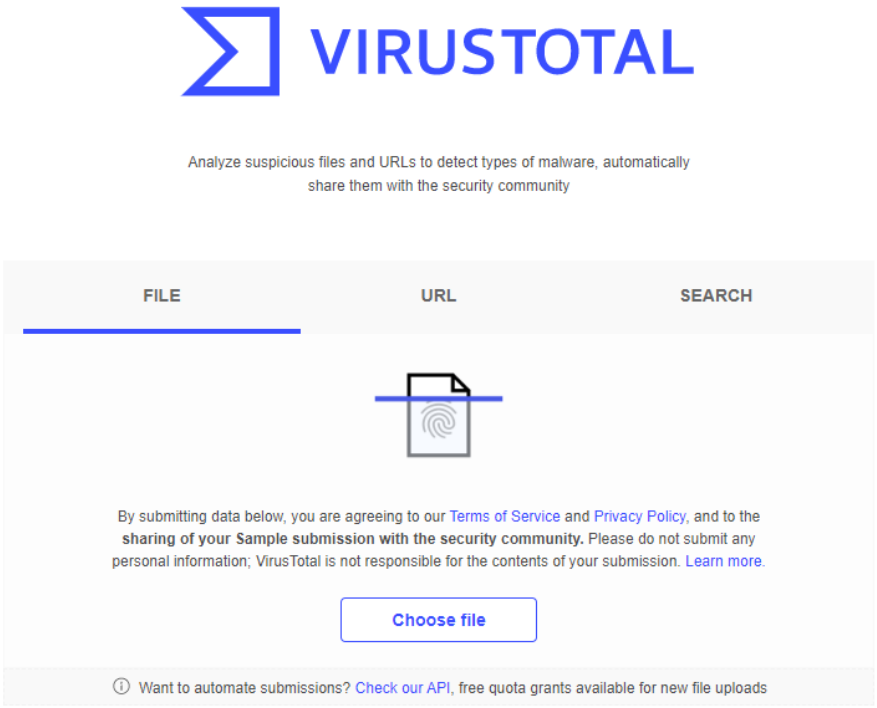
- Verificar duas vezes os URLs - Começando com a dica mais simples, esta consiste em simplesmente olhar para o URL e perceber se parece legítimo. Antes de clicar em qualquer link, é importante passar o cursor por cima do mesmo e olhar para o canto inferior esquerdo do ecrã, onde o URL é exibido. O principal truque do *phishing* é parecer o mais autêntico possível. À primeira vista, o URL pode parecer genuíno, mas uma inspeção mais atenta pode revelar um '1' no lugar de um 'l', ou um '.net' em vez de um '.com'. É necessário treinarmo-nos para verificar a legitimidade de cada URL antes de clicar no mesmo ou introduzir qualquer informação pessoal como um nome de utilizador ou uma palavra-passe.
- Confirmar o '*https*' - As letras que se encontram no início de cada URL representam o Protocolo de Transferência de Hipertexto (HTTP - *Hypertext Transfer Protocol*). Esta é a base para a forma como os dados são comunicados na *web*. E embora seja extremamente útil, também é facilmente hackeável. A adição de um 'S' (como em 'https') e o ícone do cadeado que o acompanha permitem perceber que a página é segura. Os *websites* com um cadeado na barra de endereços e o prefixo https são encriptados e têm um certificado SSL de confiança, garantindo basicamente uma ligação segura entre o *website* e o navegador. Se não for possível verificar a segurança de uma ligação através do https, recomenda-se prudência, e a não divulgação de informação pessoal.

Note-se também que os criminosos cibernéticos fazem tudo ao seu alcance para apresentarem as suas criações como o mais legítimas possíveis, por isso, ainda que os *websites* https sejam mais seguros, podem facilmente estar a ser manipulados por um vigarista. Portanto, na eventualidade de ainda existir desconfiança sobre um *site* https, é aconselhado que se empreguem as ferramentas de segurança abaixo, para verificar a segurança de um *site*.

2 - Ferramentas de segurança de *websites*

- Utilizar as ferramentas integradas do navegador - As primeiras ferramentas com que devemos estar familiarizados são aquelas já presentes no *browser*. É importante estar a par das definições de privacidade e segurança. É provável que as configurações padrão sejam mais relaxadas do que convêm. Se for o caso, deve-se ajustar manualmente as regras e definições conforme as preferências pessoais: bloquear *popups*, impedir *downloads* automáticos, não permitir o rastreio. As opções irão variar dependendo do *browser* de escolha.

- Executar uma verificação de segurança *online* - Existem várias plataformas para este efeito, mas uma das mais recomendadas é a VirusTotal, pela sua posição imparcial. Estas ferramentas *online* utilizam *scanners* antivírus e outras soluções de segurança para examinar um *website* em busca de quaisquer ameaças. Basta introduzir o URL em questão na barra de pesquisa do *site* e os resultados são obtidos instantaneamente. Com a simples introdução de um URL, a VirusTotal dirá se o *site* é suspeito.



- Instalar ferramentas de segurança na *web* - Para se conseguir uma total confiança na segurança do *website*, é pertinente apostar em conjuntos de segurança cibernética de topo de gama (por exemplo, Avast Free Antivirus, McAfee, AVG, Windows Defender). À segurança nos *websites* também se pode agregar o benefício da privacidade, optando-se por uma rede privada virtual.

3 - Pesquisa rápida sobre segurança dos *websites*

- Verificar os detalhes de contacto do *website* - Se foram implementados todos os passos descritos acima mas mantém-se a incerteza, então o melhor a fazer é voltar atrás e investigar mais sobre o *website* em questão. Ou seja, encontrar a seção de 'Contactos' no *site* e contactar os responsáveis. Dependendo da resposta (se houver resposta), será mais fácil perceber se se trata ou não de uma operação legítima.
- Verificar se o antivírus usado tem um Certificado Anti-*Phishing* - Nem todos têm. É pertinente procurar *websites* de terceiros que testem o anti-*phishing*, como o AV-Comparatives, por exemplo. Estes testam os produtos antivírus contra URLs de *phishing* (que tentam extrair informações pessoais) e verificam se há falsos positivos quando se trata de *sites* bancários legítimos, para se certificarem de que a ferramenta de segurança sabe a diferença.
- Verificar se o URL tem uma política de privacidade - isto não tem nada que saber. Se um *website* não tem uma política de privacidade, isso é um sinal de alerta no que toca a saber se a empresa é legítima ou não.

- Procurar o proprietário do domínio do *website* utilizando uma pesquisa *WHOIS* - Também é possível pesquisar quem é o proprietário de um determinado domínio, verificando os registos públicos disponíveis através de uma pesquisa *WHOIS*. Deste modo é possível saber tudo sobre o domínio, incluindo quem o registou e quando.

Uma resposta empresarial ao cibercrime

Para as empresas, a melhor abordagem contra o cibercrime é preparar um plano sólido de resposta a possíveis incidentes. Muitas vezes o planeamento não é suficiente - o pessoal e as ferramentas de segurança devem estar sempre a postos para executar a estratégia definida. Um plano de resposta a incidentes, de acordo com o enquadramento do SANS, inclui:

- Preparação - codificar a política de segurança, identificar tipos de incidentes críticos de segurança, preparar um plano de comunicação e documentar papéis, responsabilidades e processos para cada um deles. É crucial recrutar membros para a equipa de resposta a incidentes de segurança informática (CSIRT) e treiná-los.
- Identificação - utilizar ferramentas de segurança para detetar com precisão comportamentos anormais no tráfego de rede, pontos terminais, aplicações ou contas de utilizadores e recolher rapidamente provas para decidir o que fazer em relação ao incidente.
- Contenção - isolar os sistemas afetados, limpá-los e gradualmente voltar a pô-los *online*.
- Erradicação - identificar a principal causa do incidente e fazer de tudo para garantir que a questão não se repete. Consertar medidas de segurança danificadas que deixam entrar os atacantes, retificar vulnerabilidades e assegurar a limpeza de *malware* de todos os pontos terminais.
- Recuperar - restaurar os sistemas de produção, tendo o cuidado de evitar outro ataque semelhante. Implementar testes para assegurar que os sistemas estão a funcionar como deve ser.
- Lições aprendidas - até duas semanas após o incidente, é pertinente revê-lo com a equipa para compreender o que correu bem e o que não correu, e melhorar o plano de resposta ao incidente.

A UE tenta combater o cibercrime recorrendo a uma vasta gama de meios. Em 2005, o Conselho Europeu adotou a estratégia antiterrorista da UE para combater o terrorismo e tornar a Europa mais segura. A estratégia inclui quatro pilares: prevenir, proteger, perseguir, responder.

Para combater e lutar contra a cibercriminalidade a diferentes níveis, a UE implementou as seguintes ações legislativas:

- 2001 - Decisão-Quadro relativa ao combate à fraude e à contrafação, que define os comportamentos fraudulentos que os Estados da UE devem considerar como infrações penais puníveis.
- 2002 - Diretiva *ePrivacy*, que define a regulamentação das comunicações eletrónicas na UE, de modo a aumentar a privacidade dos indivíduos e entidades.
- 2011 - Uma diretiva sobre o combate à exploração sexual de crianças *online* e pornografia infantil, que aborda os novos desenvolvimentos no ambiente *online*, entre os quais, o aliciamento (infratores que se fazem passar por crianças para atrair menores para o abuso sexual).

- 2013 - **Uma diretiva sobre ataques contra os sistemas de informação**, que visa combater os ciberataques em grande escala para reforçar as leis nacionais sobre cibercriminalidade e introduzir sanções penais mais duras.

As organizações internacionalmente ativas procuram contribuir para a luta contra a cibercriminalidade. Existem duas grandes organizações a operar na UE:

Centro Europeu do Cibercrime - EC3 apoia os estados membros nos seus esforços de desmantelamento e perturbação das redes de cibercrime e ajuda-os a desenvolver ferramentas e dar formação.

A Agência da União Europeia para a Segurança Cibernética (ENISA) trabalha para dar aconselhamento e soluções para melhorar as capacidades de segurança cibernética. É um centro de especialização para os estados membros e instituições da UE que procuram aconselhamento em assuntos relacionados com a segurança das redes e da informação.

3. Aplicar conhecimento

Exercício de ESCOLHA ÚNICA

Tarefa: Escolher a opção certa usando o princípio de escolha única: apenas uma frase é verdadeira.
O que é o Certificado anti-*phishing*?

a) Verifica a existência de falsos positivos quando se trata de web*sites* bancários legítimos, para ter a certeza de que o *website* utilizado é fidedigno
b) Verifica se um *website* não tem uma política de privacidade
c) Verifica se um *website* ou *link* é seguro com https
d) Verifica o verdadeiro proprietário do *website*

Exercício de VERDADEIRO/FALSO

Tarefa: Escolhe a opção certa considerando o princípio do verdadeiro/falso:

A adição de um "S" como em "https" (e do ícone do cadeado) confirma a maior segurança de um *website*.

a) Verdadeiro
b) Falso

Exercício de ESCOLHA ÚNICA

Tarefa: Escolher a opção certa usando o princípio de escolha única: apenas uma frase é verdadeira.

O que é o VirusTotal?

a) Um programa antivírus que se pode instalar no computador
b) Um navegador *web*
c) Uma ferramenta para verificação *online* da segurança na *web*
d) O Protocolo de Transferência de Hipertexto

5. O impacto do cibercrime na vida

A Internet pode ser um **ambiente perigoso para as crianças e também para os adultos**. Especialmente neste período digital em que as redes sociais como o Facebook, Instagram ou a Internet em geral desempenham um papel fundamental no nosso quotidiano. Proteger especialmente as crianças na Internet requer uma elevada consciência dos riscos, bem como competências avançadas em tecnologias da informação - é importante que os pais saibam quais os perigos que se escondem na Internet, e como os proteger contra eles.

Seguem-se os seis maiores riscos que as crianças enfrentam *online*:

- Ciberbullying
- *Download* acidental de *malwares*
- Aliciamento (infratores que se fazem passar por crianças para atrair menores para o abuso sexual)
- *Phishing*
- Publicação de informação privada
- "Amigos" de *chatrooms*

No entanto, não são só as crianças que são confrontadas com ameaças virtuais. O ecossistema do cibercrime é enorme e há imensas formas através das quais os cibercrimosos podem interagir diretamente com qualquer indivíduo. Os cibercriminosos atacam a ignorância humana, o desconhecimento e a fragilidade das pessoas, o que pode causar danos à identidade e às finanças. De que é que as pessoas devem estar cientes? Os criminosos concebem conscientemente as suas armadilhas, tirando partido das fraquezas humanas ou do comportamento humano, como por exemplo:

- Vontade individual de confiar nos outros
- Sugestão de urgência ou importância de uma mensagem
- Sinais de legitimidade ou autoridade numa mensagem ou indivíduo (marca idêntica à marca oficial de um indivíduo ou organização para cultivar a confiança)
- Medo de situações de elevado stress ou ansiedade
- Conveniência (a decisão mais fácil pode não ser a mais segura)
- Tendência dos indivíduos para partilhar dados de identidade pessoal *online* (especialmente em formas de meios de comunicação social, incluindo Facebook, Twitter, LinkedIn)
- Falta de familiaridade com novas formas de tecnologia que abrem os indivíduos ao risco
- A subestimação individual da situação

Se uma pessoa perpetuar os comportamentos mostrados acima, enfrentará um risco mais elevado de se tornar vítima de ciberroubo. O roubo cibernético é um tipo de crime que envolve o roubo de informações financeiras ou pessoais através da utilização de computadores. Os ladrões cibernéticos são sofisticados e são capazes de violar medidas de segurança.
Na primeira fase, o infrator deve primeiramente adquirir uma identidade informática estrangeira. Isto é frequentemente feito através do roubo de dados eletrónicos (palavras-passe, dados de acesso, etc.), geralmente através de cópias não autorizadas (*skimming*), *phishing* enganoso ou *hacking*. A isto chama-se roubo de identidade. Na segunda fase, o atacante utiliza indevidamente a identidade. O objetivo é geralmente o benefício próprio. Em alguns casos, o objetivo pode ser simplesmente prejudicar a vítima, por exemplo atuando sob o seu nome em redes sociais como o Facebook.

A defesa não é complicada - é importante seguir algumas regras simples:

1. Monitorizar a conta
2. Comprar em *sites* seguros - se houver um ícone de cadeado verde antes do "https", o *site* é seguro
3. Ter cuidado ao abrir *emails* não confiáveis

Impacto nos indivíduos, nas empresas e na sociedade

A cibercriminalidade tem um **impacto direto e significativo no emprego, inovação, crescimento económico e investimento**. Além disso, o roubo de IP constitui pelo menos 25% dos custos da cibercriminalidade e representa uma ameaça especialmente elevada para a tecnologia militar. Duas áreas do cibercrime que são difíceis de medir são o roubo de IP (endereço IP) e a perda de oportunidades.

Os indivíduos e as empresas podem sofrer **perdas financeiras significativas** devido ao cibercrime, sendo o roubo o impacto mais óbvio. A perda de negócios também pode ser significativa no caso de ataques de negação de serviço a grandes empresas.

A tecnologia pode tornar a vida mais fácil, mas também nos deixa vulneráveis ao risco. Como resultado, a segurança cibernética é a principal prioridade e afeta imenso a nossa vida diária e o nosso trabalho. As violações da segurança cibernética podem ser catastróficas para as organizações e seus empregados ou base de clientes.

Os danos causados por ciberataques e roubos cibernéticos podem extravasar do alvo inicial para outras empresas que a esse estejam ligadas economicamente, ampliando assim os danos para a economia. As empresas tendem a partilhar vulnerabilidades cibernéticas comuns, fazendo com que as ameaças cibernéticas sejam correlacionadas entre empresas.

O crime afeta toda a gente e, no futuro, o cibercrime e a segurança cibernética vão afetar ainda mais as pessoas. Ninguém está seguro - é algo que impacta os ricos e os pobres:

- Qualquer pessoa que tenha um telemóvel no bolso.
- Qualquer pessoa que tenha uma conta bancária.
- Qualquer pessoa que armazene ficheiros importantes no seu computador.
- Qualquer pessoa cujo nome conste de uma base de dados de marketing direto.

O cibercrime não é um cenário de um futuro remoto. Está a acontecer todos os dias, neste preciso momento. Os ladrões cometem crimes cibernéticos para roubar o dinheiro das pessoas e a sua identidade. Com essas identidades, o ladrão pode contrair empréstimos, contrair créditos, acumular dívidas e, depois, fugir sem deixar rasto. Pode demorar anos a reabilitar uma identidade roubada. Um vírus pode destruir os ficheiros de alguém e uma base de dados perdida pode resultar na receção de chamadas de vendas indesejadas.

A segurança cibernética é importante para a segurança nacional – para protegermos este nosso belo país.

- Há segredos de estado que devem permanecer secretos.
- A segurança pessoal dos nossos líderes é muito importante.
- A base de dados de impressões digitais e a base de dados dos Assuntos Internos devem ser seguras.
- Os terroristas não podem ser capazes de impedir o comércio nacional e mundial recorrendo a dados sensíveis.

Mas a **segurança nacional não pode sobrepor-se à nossa liberdade pessoal** que tanto lutámos para alcançar:

- A nossa liberdade de expressão é crucial.
- Uma imprensa livre incita a responsabilização das pessoas.
- A privacidade pessoal assegura a democracia.
- A liberdade de fazer coisas *online* sem vigilância.

4. Aplicar conhecimento

Exercício de ESCOLHA ÚNICA

Tarefa: Escolher a opção certa usando o princípio de escolha única: apenas uma frase é verdadeira.

Quem pode ser afetado pela cibercriminalidade?

a) Qualquer pessoa que lide com contas móveis, contas *online* ou contas bancárias.
b) Apenas crianças
c) Apenas empresas
d) Apenas instituições públicas

Exercício de ESCOLHA ÚNICA

Tarefa: Escolher a opção certa usando o princípio de escolha única: apenas uma frase é verdadeira.

O que é o ciberroubo?

a) Uma obsessão em descobrir o máximo que puder sobre a pessoa
b) O uso ou exploração de redes informáticas ou de comunicação para causar destruição ou perturbação suficientes para gerar medo ou intimidar uma sociedade por forma a atingir um objetivo ideológico
c) Dizer coisas ofensivas a uma pessoa ou espalhar informações falsas sobre a mesma
d) Roubo de informação financeira ou pessoal através da utilização de computadores

Exercício de VERDADEIRO/FALSO

Tarefa: Escolhe a opção certa considerando o princípio do verdadeiro/falso: apenas uma frase é verdadeira.

A cibersegurança não é importante para a segurança nacional.

a) Verdadeiro
b) Falso

Fontes

Fonte: http://www.ijeset.com/media/0002/2N12-IJESET0602134A-v6-iss2-142-153.pdf
Fonte: https://study.com/academy/lesson/finance-crime-definition-comparisons-examples.html
Fonte: https://www.avast.com/c-cibercrime
Fonte: NATO science for peace and security series, 2008
Fonte: CLARKE, Richard A. Cyber War, HarperCollins (2010) ISBN 9780061962233
Fonte: CNN, News, 04.08.2004, disponível em: www.cnn.com/2004/US/08/03/terror.threat/index.html.

Para uma visão geral, ver: Sieber/Brunst, Cyberterrorism – the use of the Internet for terrorist purposes, Council of Europe Publication, 2007; Gercke, Cyberterrorism, How Terrorists Use the Internet, Computer und Recht, 2007
Fonte: EU counter-terrorism strategy
Fonte: https://www.avast.com/c-website-safety-check-guide
Fonte: https://www.europol.europa.eu/about-europol/european-cibercrime-centre-ec3
Fonte: https://www.enisa.europa.eu/
Fonte: https://arxiv.org/pdf/1811.06624.pdf

Para relembrar

Resumo

A utilização de tecnologia informática, sistemas de informação e tecnologia da informação, bem como a sua integração em quase todos os setores da atividade humana é um fenómeno dos dias de hoje. Não existe quase nenhuma área da atividade humana onde a tecnologia da informação ou da comunicação não é utilizada.

Infelizmente, o aumento do progresso tecnológico impulsiona também uma maior possibilidade de ocorrerem crimes. O crime pode ser cometido de muitas formas, sendo que os cibercrimes mais frequentemente cometidos incluem:

- ***Malware*** - rótulo geral para *software* malicioso que se espalha entre computadores e interfere com as operações informáticas
- ***Hacking*** - processo comum que resulta na violação da privacidade e da informação confidencial de uma pessoa
- ***Spam*** - correio eletrónico não solicitado ou lixo eletrónico normalmente enviado em massa para inúmeros destinatários em todo o mundo
- ***Phishing*** - *emails* de *spam*, ou outras formas de comunicação, enviados em massa com a intenção de enganar os destinatários para que façam algo que prejudique a sua segurança ou a segurança da organização para a qual trabalham
- **Ataques DoS distribuídos (DDoS)** - o ataque sobrepõe um sistema usando um dos protocolos de comunicação padrão que utiliza para enviar spam ao sistema com pedidos de ligação

Contudo, o ***hacking*** **nem sempre é visto como roubo e pode ser utilizado para causas produtivas**. Esse tipo de *hacking* que envolve boas intenções é conhecido como ***hacking*** **ético**. Este tipo de *hacking* é feito para proteger o sistema operativo.

Os cibercrimes mais frequentemente cometidos incluem:

- **Falsificação online** - utilizar o nome, endereço de domínio, número de telefone ou qualquer outra informação de identificação de outra pessoa sem consentimento
- ***Ciberstalking*** - obsessão em descobrir o máximo possível sobre uma pessoa
- **Ciberbullying** - dizer coisas que magoam a pessoa ou espalhar informações falsas sobre a pessoa
- **Roubo de identidade** - roubo de informação de identificação pessoal para cometer atos ilegais
- **Roubo de dados** - posse ilegal de dados sensíveis, incluindo informação não encriptada de cartão de crédito armazenada nas empresas
- **Crimes financeiros** - abrange os seguintes: fraude, branqueamento de capitais, suborno, corrupção e muitos outros

Os impactos da cibercriminalidade podem ser devastadores devido aos danos na reputação, ao elevado risco de perda de dados e ao impacto financeiro para:

- Crianças
- Adultos
- Empresas
- Estados/governos

O cibercrime pode ter não só um impacto financeiro, mas também um impacto desonesto sobre indivíduos ou empresas. Os negócios, bem como as organizações de saúde e os governos, podem também sofrer a perda de dados sensíveis, enormes encargos financeiros, e danos à marca.
As maiores ações planeadas do cibercrime tendem a ser designadas como ciberterrorismo ou mesmo guerra cibernética. O ciberterrorismo é sempre mais severo do que outros comportamentos que são levados a cabo através do ciberespaço. O ciberterrorismo caracteriza-se por ser um ciberataque que faz uso ou explora redes informáticas ou de comunicação para causar destruição ou perturbação suficientes por forma a gerar medo ou intimidar uma sociedade para um objetivo ideológico. A guerra cibernética envolve a utilização e o ataque a computadores e redes num cenário de guerra. Esta prática envolve operações ofensivas e defensivas relacionadas com a ameaça de ciberataques, espionagem e sabotagem.

Um instrumento crucial na luta contra os crimes cibernéticos é a prevenção e o esclarecimento. Finalmente, a literacia informática é um elemento essencial na prevenção da utilização das tecnologias da informação e da comunicação. Devemos preparar não só as crianças, mas também os adultos e as empresas para os perigos do ciberespaço e tentar fornecer-lhes os conhecimentos necessários para a utilização segura das tecnologias de informação.

Para a segurança *online*, cinco pontos-chave a ter em mente são: Precaução, Prevenção, Proteção, Preservação e Perseverança.

Estes pontos são fundamentais em todas as seguintes recomendações para a segurança *online*:

1. Evitar a divulgação de informações pessoais na Internet e em *emails*
2. Considerar cuidadosamente o envio de qualquer fotografia *online* - qualquer pessoa pode utilizá-la em qualquer altura noutro contexto
3. Utilizar palavras-passe fortes
4. Utilizar e manter atualizado o *software* antivírus
5. Evitar o envio do número do cartão de crédito e de palavras-passe por *email*
6. Prestar atenção aos *websites* visitados pelas crianças
7. Manter uma cópia de segurança dos dados para prevenir a perda de informação devido a ataques de vírus
8. Utilizar um programa de segurança que permita controlar os *cookies*
9. Manter o *software* e o sistema operativo atualizados
10. Nunca abrir anexos em *emails* de *spam*
11. Não clicar em *links* vindos de *emails* de *spam* ou em *websites* não confiáveis
12. Contactar diretamente as empresas no caso de surgirem pedidos suspeitos
13. Monitorizar continuamente os extratos bancários
14. Ser cauteloso com os *websites* visitado

Como posso reconhecer os *websites* seguros?

1 - Verificações visuais de segurança de *websites*
2 - Ferramentas de segurança de *websites*
3 - Pesquisa rápida sobre segurança dos *websites*

A Internet está repleta de esquemas de *phishing*. Nenhuma marca está a salvo de ser falsificada e nenhum utilizador está imune de se tornar um alvo. Mais do que nunca, precisamos de assumir a responsabilidade pela nossa própria segurança *online*. É preciso seguir as dicas acima e manter sempre a vigilância. A informação de que necessitamos está aqui mas a nossa melhora defesa *online* reside em cada um de nós.

As respostas corretas estão assinaladas a negrito

Situação: Se uma música ou filme é publicada na Internet, legalmente posso fazer um *download*.
Tarefa: Escolhe a opção certa considerando o princípio do verdadeiro/falso:

e) Verdadeiro
f) Falso

Situação: Escolher a opção certa usando o princípio de escolha única: apenas uma frase é verdadeira. Escolher as categorias corretas do cibercrime.

e) Infrações relacionadas com informática
f) Roubo físico de um computador, *tablet* ou telemóvel
g) Infrações relacionadas com o conteúdo
h) Infrações relacionadas com direitos de autor

Situação: *Correspondência de respostas – selecione a opção correta do menu e arraste para a parte correta do texto*

_____ abrangem muitas infrações que requerem um sistema informático para serem cometidas. Ao contrário da categoria anterior, estas infrações amplas normalmente não são tão rigorosas em termos de proteção dos princípios legais.

_____ inclui violações de instrumentos legais mais influenciadas pelas abordagens nacionais, que estão mais aptas a considerar os seus princípios culturais e jurídicos basilares. No que toca a conteúdos ilegais, os sistemas de valores e os sistemas jurídicos diferem muito entre sociedades.

_____ incluem a troca de canções, ficheiros e *software* protegidos por direitos de autor em plataformas de partilha de ficheiros ou através de serviços de alojamento de partilha e a evasão aos sistemas de gestão de direitos digitais (DRM).

Infrações relacionadas com informática; Infrações relacionadas com o conteúdo; Infrações relacionadas com direitos de autor

Situação: O que são ataques distribuídos de negação de serviços (DDoS - Distributed DoS attacks)?
Tarefa: Escolher a opção certa usando o princípio de escolha única: apenas uma frase é verdadeira.

a) Quando são enviados em massa *emails* de *spam* ou outras formas de comunicação
b) Um tipo de ataque de cibernético que os cibercriminosos utilizam para derrubar um sistema ou rede
c) Correio eletrónico não solicitado ou lixo eletrónico normalmente enviado em massa para imensos destinatários em todo o mundo
d) Utilização ou acesso não autorizado a computadores ou recursos de rede, para explorar vulnerabilidades de segurança identificadas nas redes

Situação: O que faz um *hacker* "*grey hat*"?
Tarefa: Escolher a opção certa usando o princípio de escolha única: apenas uma frase é verdadeira.

a) Espalha informações falsas sobre outra pessoa

b) Tenta roubar informação de identificação pessoal
c) Obtém acesso a um sistema de alguém sem autorização, apenas por diversão
d) É responsável por muitos crimes financeiros através da Internet

Situação: O que é a fraude interna?
Tarefa: Escolher a opção certa usando o princípio de escolha única: apenas uma frase é verdadeira.
a) A fraude interna é cometida pelos fornecedores no caso de não fornecerem a tempo o serviço ou mercadoria acordada.
b) A fraude interna envolve atividades como o aliciamento ou o ciberstalking.
c) A fraude interna é cometida por funcionários em caso de realização de transações financeiras não autorizadas.
d) A fraude interna é cometida por clientes da empresa através da apresentação de uma queixa injustificada.

Situação: Qual é o pior tipo de ciberataque que ocorre num contexto de crimes reais e físicos?
Tarefa: Escolher a opção certa usando o princípio de escolha única: apenas uma frase é verdadeira.
a) Fraude de cartão de crédito
b) Pornografia
c) Ciberterrorismo
d) Roubo de identidade

Situação: Qual o impacto que o cibercrime pode ter para a pessoa?
Tarefa: Escolher as opções corretas usando o princípio da escolha múltipla: pode haver mais do que uma resposta certa.
a) Roubo de identidade
b) Desemprego
c) Problemas de saúde
d) Violações de dados

Tarefa: Correspondência de respostas – selecione a opção correta do menu e arraste para a parte correta do texto
_____ podem sofrer com a perda de dados sensíveis, enormes encargos financeiros, e danos à marca
Empresas

Situação: O que é o Certificado anti-*phishing*?
Tarefa: Escolher a opção certa usando o princípio de escolha única: apenas uma frase é verdadeira.
a) Verifica a existência de falsos positivos quando se trata de web*sites* bancários legítimos, para ter a certeza de que o *website* utilizado é fidedigno
b) Verifica se um *website* não tem uma política de privacidade
c) Verifica se um *website* ou *link* é seguro com https
d) Verifica o verdadeiro proprietário do *website*

Situação: A adição de um "S" como em "https" (e do ícone do cadeado) confirma a maior segurança de um *website*.
Tarefa: Escolhe a opção certa considerando o princípio do verdadeiro/falso:
a) Verdadeiro
b) Falso

Situação: O que é o VirusTotal?
Tarefa: Escolher a opção certa usando o princípio de escolha única: apenas uma frase é verdadeira.

a) Um programa antivírus que se pode instalar no computador
b) Um navegador *web*
c) Uma ferramenta para verificação *online* da segurança na *web*
d) O Protocolo de Transferência de Hipertexto

Situação: Quem pode ser afetado pela cibercriminalidade?
Tarefa: Escolher a opção certa usando o princípio de escolha única: apenas uma frase é verdadeira.

a) Qualquer pessoa que lide com contas móveis, contas *online* ou contas bancárias.
b) Apenas crianças
c) Apenas empresas
d) Apenas instituições públicas

Situação: O que é o ciberroubo?
Tarefa: Escolher a opção certa usando o princípio de escolha única: apenas uma frase é verdadeira.

a) Uma obsessão em descobrir o máximo que puder sobre a pessoa
b) O uso ou exploração de redes informáticas ou de comunicação para causar destruição ou perturbação suficientes para gerar medo ou intimidar uma sociedade por forma a atingir um objetivo ideológico
c) Dizer coisas ofensivas a uma pessoa ou espalhar informações falsas sobre a mesma
d) Roubo de informação financeira ou pessoal através da utilização de computadores

Situação: A cibersegurança não é importante para a segurança nacional.
Tarefa: Escolhe a opção certa considerando o princípio do verdadeiro/falso: apenas uma frase é verdadeira.

a) Verdadeiro
b) Falso