Curso de

Segurança Digital

Segurança Digital

Sobre o curso

Cada vez mais estamos dependentes da Internet para efetuarmos nossos compromissos do dia-a-dia. Além disso, ela é uma fonte quase infinita de informações. Mas, como filtrar isso? Como permanecer seguro em um mundo digital onde todos os nossos dados pessoais ficam salvos em bancos de dados? Como manter seu dispositivo limpo de vírus e se livrar dos diversos golpes aplicados na grande rede? Neste curso, você terá um guia de sobrevivência da internet.

Carga horária
9 horas

Quantidade de aulas
6 aulas

Programas Utilizados

O que aprender com este curso?

Você aprenderá os diferentes tipos de ataques efetuados por hackers e crackers e como se proteger deles. Também aprenderá sobre os mais variados tipos de golpes aplicados na internet e a forma de se proteger de cada um, além da instalação e manutenção de softwares de proteção.

Conteúdo programático

Aula 1 – A era Digital

Aula 2 – Tipos de Golpes Digitais

Aula 3 – Os três maus comuns

Aula 4 – Aplicativos Falsos

Aula 5 – Senhas de Segurança

Aula 6 – A importância de sistemas de Segurança

SUMÁRIO

Segurança Digital

A Era Digital

Aula

01

1. Aula 1 – A Era Digital

Há alguns anos atrás sofremos uma transformação para a Era industrial. Naquela época, meados do século XVIII, o trabalhador rural fazia grande parte do trabalho braçal pesado do campo. Nesse tempo, o trabalho começou a se tornar mecanizado, isto é, o que antes era feito com as mãos do produtor rural, passou a ser feito com maquinário agrícola.

Essa mudança na produção repercutiu na ordem econômica, política e social da época. A era industrial marca o início do desenvolvimento do capitalismo industrial assim como o crescimento da produção de massa e o surgimento das novas populações urbanas.

Porém, após a década de 90 passamos a viver em uma nova era. A chamada Era da Informação ou Era Digital.

Nesta nova era o trabalhador industrial está sendo – cada vez mais – substituído pelo Trabalhador do conhecimento. Isto é, um trabalhador que alia o trabalho manual com conhecimento.

Cada vez mais o conhecimento é imprescindível em nossa sociedade. Inclusive já é considerado o bem mais valioso.

Para nos adaptarmos a esta realidade precisamos estar atentos à informação.

Saber onde buscar as informações que precisamos sem nos arriscarmos é indispensável para a internet.

Precisamos estar atentos a cada momento e – assim como acontece no mundo real – há pessoas que tentam se aproveitar de nossos momentos de vacilo para tirar proveito disso.

1.1. Dados pessoais e informações pessoais

Quando acessamos a rede global e inserimos nossas informações pessoais para criar um cadastro em um site, ou efetuar uma compra estamos confiando naquele site.

Lembre-se sempre disso, suas informações pessoais e seus dados devem sempre estar guardados a sete chaves.

É muito fácil para qualquer criminoso pegar os dados de seu cartão de crédito, junto com seus dados pessoais e efetuar qualquer compra em qualquer site, com o bônus de estar sentado atrás de um computador e não manter sua identidade inviolável.

Portanto, sempre que for efetuar um cadastro ou disponibilizar suas informações em qualquer site na internet, verifique várias vezes a procedência daquele site.

Você está em um site confiável? Você conhece aquele site? É sua primeira compra nele?

Tudo isso deve ser levado em conta antes de fornecer os dados de seu cartão de crédito.

Além disso jamais efetue compras por e-mail nem por links enviados por terceiros (caso você não os conheça muito bem).

1.2. Tipos de ameaças encontradas na internet

Bem, sabemos que a internet nos proporciona acesso a uma infinidade de informações. Mas, estas informações muitas vezes podem vir junto com ameaças.

Isso porque, enquanto você está navegando na internet, criminosos virtuais podem estar tentando utilizar diversos tipos de truques para ameaçar você.

Estes truques vão desde furto de dados bancários e cartões de crédito, extorsão, roubo de senha de acesso e até mesmo a contaminação do computador com o intuito de derrubar serviços.

É fundamental que você mantenha os olhos bem abertos enquanto navega na internet e evite algumas práticas que podem lhe levar a cair em uma armadilha.

Para evitar estes problemas, primeiro, precisamos conhece-los.

Segue uma lista de alguns dos truques sujos e arquivos maliciosos que alguns golpistas utilizam para roubar dados ou apenas causar o mau a pessoas não informadas que navegam pela rede.

Vírus

Todos os dias, diversos tipos de vírus surgem na rede mundial de computadores. Malwares, trojans, adwares e outras aplicações maliciosas que, juntas, têm o objetivo de prejudicar o internauta. Seja furtando informações, espionando, ou destruindo o equipamento do usuário, os hackers costumam ser ardilosos na hora de espalhar ameaças online. Para se proteger, aposte em um bom antivírus e um firewall, mantendo-os sempre atualizados.

Furto de dados e identidade

Phishing é o nome dado à artimanha dos criminosos para "pescar" os dados pessoais ou bancários do usuário. Com essas informações, ele pode realizar compras ou clonar uma identidade para abrir cadastros, realizar transações bancárias ou criar contas falsas em perfis sociais.

Para que isso não aconteça, evite ao máximo compartilhar informações pessoais como senhas, nomes de usuário, informações bancárias ou números de cartão de crédito em links duvidosos de e-mails ou sites que não contam com certificados de segurança – que podem ser conferidos pelo cadeado na barra de endereço. Ao comprar em lojas virtuais, pesquise e opte sempre por e-commerces com boas reputações.

Espionagem

Alguns hackers mal-intencionados são capazes de ligar a webcam ou o microfone de notebooks e smartphones de outros usuários com o objetivo de espionar quem está do outro lado da tela.

Há também criminosos que invadem redes sociais para identificar informações relacionadas à vida pessoal do usuário, como locais que costuma frequentar e fotos de seus parentes. É muito importante elevar o nível de privacidade de conta para quem pode visualizar as informações do perfil, especialmente para crianças e adolescentes. Também é recomendado cobrir os componentes de áudio e vídeo com uma fita adesiva sempre que não estiverem em uso.

Aplicativos falsos

Alguns criminosos utilizam aplicativos em formas de jogos ou ferramentas para invadir dispositivos móveis, em uma abordagem conhecida como man-in-the-middle.

Essa modalidade de ataque intercepta dados enviados digitalmente e também pode ser executada por meio de aplicativos duvidosos disponíveis para download nas lojas dos sistemas operacionais.

Com isso, o hacker mal-intencionado, consegue obter senhas, números de cartões de crédito, informações de login, etc. Portanto, ao baixar um aplicativo, fique atento aos comentários dos usuários e, principalmente, às permissões de acesso que o mesmo solicita.

1.3. Protegendo-se das Fake News

Fake News são notícias falsas publicadas por veículos de comunicação como se fossem informações reais. Esse tipo de texto, em sua maior parte, é feito e divulgado com o objetivo de legitimar um ponto de vista ou prejudicar uma pessoa ou grupo (geralmente figuras públicas).

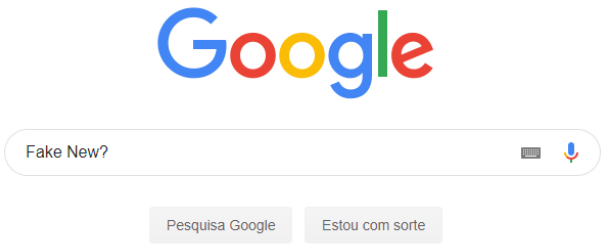
As Fake News têm um poder viral incrível! Isto é, elas espalham-se rapidamente. Portanto, devemos tomar muito cuidado para não espalhar notícias antes de saber suas verdadeiras fontes, além de estarmos nos tornando vítimas de uma Fake New também estamos ajudando a disseminar a mentira.

O poder de persuasão das Fake News é maior em populações com menor escolaridade e que dependem das redes sociais para obter informações. No entanto, as notícias falsas também podem alcançar pessoas com mais estudo, já que o conteúdo está comumente ligado ao viés político.

1.4. Como checar a veracidade das informações recebidas na rede

Para checar se uma notícia ou informação é real você pode utilizar o maior site de pesquisas do mundo, o Google.

Acessando o site www.google.com, você poderá pesquisar se algo é verdade ou não.

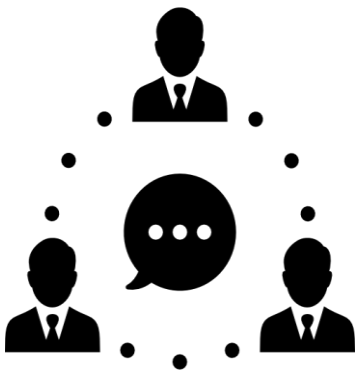


É claro que, ainda que o site possa lhe mostrar diversos resultados ainda é preciso um tanto de bom senso para identificar o que é verdade e o que é mentira.

Existem diversos sites espalhados pela internet que possuem como único intuito proteger as pessoas contra essas mentiras.

Você também pode pesquisar em sites de jornalismo sério sobre a notícia recebida para verificar sua veracidade.

Muitas vezes, basta um pouco de tempo e de boa vontade para evitarmos espalhar notícias que podem causar danos e até mesmo mudar a vida de pessoas que as recebem.



1.5. Exercícios de Conteúdo

1) O que é a era digital?

2) O que é engenharia social?

3) Como checar a veracidade das informações na rede?

4) Como se proteger de Fake News?

5) Quais as intenções dos aplicativos falsos?

1.6. Exercícios de Fixação

1) Entre no site do Google e procure pela veracidade da informação: “Só usamos 10% do nosso cérebro”. Anote a resposta

2) Entre no site do Google e descubra a verdade sobre a informação: “O frio causa resfriados”. Anote a resposta.

3) Entre no site do Google e descubra a verdade sobre a informação: “Álcool não deve ser consumido junto com remédios tarja preta”.

2. Aula 2 – Tipos de golpes digitais

Ao navegarmos na internet é preciso sempre estar muito atento.

Atentos aos links que clicamos, aos sites que navegamos, ao conteúdo que estamos absorvendo, às pessoas que estamos conversando e notícias que estamos espalhando.

Isso porque existem diferentes crimes virtuais sendo aplicados por criminosos que buscam obter vantagens às custas das vítimas desatentas.

O importante é o entendimento de que em todos os golpes já aplicados o problema foi acarretado por descuidos com a segurança, como pouco cuidado nos sites acessados, ou falta de malícia para identificar falsas informações, promoções ou ofertas de emprego irrealistas.

Como dito anteriormente "não existe almoço grátis nem televisão 4k por R$ 400,00".

2.1. Golpes mais comuns

Sites maliciosos

Por falta de segurança, alguns sites acabam expostos a ações de criminosos que os invadem e colocam códigos maliciosos para prejudicar a empresa, gestores ou o público que os acessam.

Além disso, há sites criados exclusivamente com o objetivo de enganar o público. Geralmente eles exibem ofertas muito tentadoras para atrair usuários e podem se valer do nome e identidade visual de um e-commerce que tenha boa reputação. Na ânsia de comprar o produto a um preço muito baixo, o consumidor esquece de checar fatores básicos como a URL correta do site e selos de segurança, como o Selo Site Blindado, e acaba caindo em um golpe.

Roubo de identidade

Assim como no ambiente offline, existem golpes na internet focados em roubar a identidade digital de outra pessoa para obter algum tipo de privilégio ou realizar uma ação.

Os criminosos podem abrir um perfil social em nome da vítima, enviar e-mails em nome de outra pessoa e etc. Neste caso, elas podem se apropriar da confiança que há em relação à vítima para se passar por ela, pedindo ajuda em dinheiro aos amigos, enviando arquivos com vírus e etc.

Dependendo das informações obtidas, pode ser ainda que outras pessoas façam cadastros e compras no nome da vítima.

Falsas oportunidades de emprego

Páginas falsas de empresas que divulgam muitas oportunidades de emprego e promessas de dinheiro fácil também compõem a lista de crimes virtuais já registrados.

Receber para fazer algo muito desejado, como degustar ovos de Páscoa, ou ganhar grandes quantias de dinheiro apenas fazendo determinado curso, ou trabalhando de casa, são algumas artimanhas utilizadas para atrair e enganar as vítimas.

Falsos boletos e faturas

Boletos falsos enviados por e-mail ou mesmo falsas faturas de serviço ou de cartão de crédito são outro dos principais golpes da internet.

É muito importante checar se aquele boleto ou fatura é realmente esperado e se os dados são legítimos. É possível checar os números iniciais do código de barra, por exemplo, para ver se eles conferem com o do banco correspondente que é citado no boleto.

Romance falso

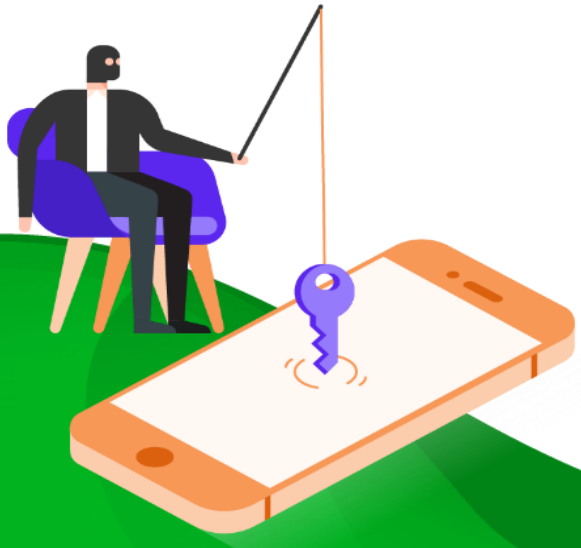
Romance falso ou "romance sacammer" é um dos crimes virtuais que têm sido utilizados em sites como Facebook e sites de encontros românticos.

Nestes golpes da internet, a pessoa mal-intencionada irá seduzir a vítima em busca de um romance cultivando uma relação de confiança e intimidade com ela. Depois, os golpistas sentem maior liberdade de começar a pedir dinheiro a quem seduziram ou informações pessoais e bancárias.

E-mails de recadastramento

Outro golpe que é muito aplicado são os e-mails de recadastramento.

Neles, uma instituição financeira pede que você se recadastre para continuar utilizando o Internet Banking (banco online que é uma comodidade comum do dia-a-dia.



E-commerce sites de venda falsos

Prática antiga e bastante difundida pela imprensa, porém, ainda presente na internet.

Não raramente recebemos anúncios de ofertas incríveis.

São produtos com procura alta a preços extremamente atrativos.

Encontrou essas características? Então fuja!

Os criminosos virtuais utilizam algumas ferramentas disponíveis na internet, e têm acesso aos termos mais buscados na rede.

Programas como Google Analytics, Google Adwords, Google Trends, Facebook Insights, Facebook Ads, entre outros, são mecanismos que fornecem aos empreendedores virtuais meios para saber o que está em evidência na internet.

2.2. Como se Proteger dos golpes feitos pela internet

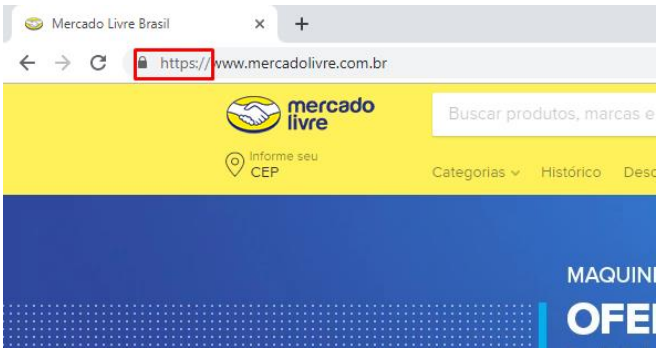
Para cada tipo de golpe aplicado existe uma forma de se proteger para evitar maiores danos.

Todas elas, de uma forma ou de outra, envolvem: atenção, bom senso e nada de ingenuidade.

Isso porque todos os golpes digitais baseiam-se em um único fato, você não viu que era falso.

Portanto, para evitar futuras dores de cabeça, comece por desconfiar de tudo até que seja provado o contrário.

Viu uma promoção boa demais para ser verdade? Desconfie, muito! Recebeu um e-mail de seu banco? Ligue para ele, não responda o e-mail muito menos clique em algum link que possa ser fornecido por ele. Entrou em algum site de cadastramento ou que peça dados importantes? Verifique a barra de URL, confirme o endereço do site, verifique se o site tem certificado de segurança "HTTPS".



Nunca seja pego desprevenido e você não terá problemas com golpes via internet.

2.3. Fatos interessantes e estatísticos sobre fraudes

Segundo a Serasa Experian, somente no Brasil, ocorrem em média 17 tentativas de fraude por segundo contra o consumidor.

Os mais variados golpes são aplicados contra os mais diversos setores da economia.

Empresas de telefonia, setor de serviços, seguradoras, bancos e financeiras são os alvos preferidos dos fraudadores.

A maioria esmagadora das tentativas de fraude ocorrem no ambiente virtual, ou seja, pela internet.

Em 2015, quase 1,7 milhões (1.695.181) de tentativas de fraudes contra o consumidor foram identificadas.

Em 90% dos casos os golpes apelam para o lado sensível ou emotivo da vítima. Isto é, o golpista sempre irá tentar levar-lhe pela emoção. Todos os golpes são facilmente identificáveis caso a vítima haja com a razão, pare e pense antes de tomar qualquer decisão.

A grande maioria dos golpes é evitado apenas por pedir a opinião para outra pessoa. Fique atento e não deixe que outras pessoas escolham sua forma de pensar e de agir.

Além disso, o bom senso ainda é o melhor remédio para estes tipos de golpes.

2.4. Exercícios de Conteúdo

1) Os golpes aplicados na internet se baseiam em quais premissas de falha da vítima?

2) Qual a forma mais simples de atrair alguém via e-mail ou link de rede social com promessas tentadoras?

3) Quais os meios mais utilizados para aplicar golpes?

4) Qual a melhor forma de se proteger dos golpes aplicados via internet?

5) O que fazer quando recebemos um e-mail de um suposto banco ofertando algo ou cobrando algo?

2.5. Exercícios de Fixação

1) Procure no Google pelo site “Mercado livre” e acesse-o.
2) Cheque se você acha que esse site é seguro e anote os seus motivos.
3) Procure no Google pelo site “Youtube”.
4) Cheque se você acha que esse site é seguro e anote seus motivos.

3. Aula 3 – Os três maus comuns

Vírus, SPAM e DDoS figuram entre os maus mais comuns trazidos por Crackers e Hackers mal-intencionados.

Eles servem para as mais diversas proezas e sempre irão prejudicar você.

Por isso, você precisa estar sempre seguro, com Firewall e Antivírus atualizados e instalados em seu dispositivo.

Além do que, é preciso que esteja sempre consciente dos lugares onde clica, as páginas que acessa e os downloads que procura.

3.1. Os tipos de vírus mais comuns

Os vírus de computador ganharam esse nome por sua capacidade de "infectar" diversos arquivos em um computador. Eles se propagam para outras máquinas quando os arquivos infectados são enviados por e-mail ou levados pelos próprios usuários em mídias físicas, como unidades USB, HD externos, etc.

O primeiro vírus de computador, batizado de "Brain", foi desenvolvido em 1986. Cansados de clientes que pirateavam softwares de sua loja, dois irmãos alegam ter desenvolvido o vírus para infectar o setor de inicialização dos disquetes dos ladrões de software. Quando os discos eram copiados, o vírus era passado adiante.

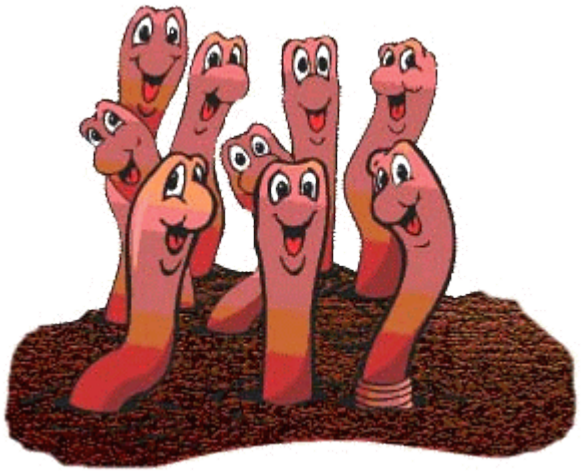
Hoje em dia cada vez mais vírus são criados e sua tecnologia vem se aprimorando em uma luta constante contra os antivírus que tentam barra-los.

Por isso a atualização de um antivírus é muito importante, pois sempre que entra um vírus novo na rede é adicionado ao antivírus uma “vacina”, uma forma de detecção e neutralização do mesmo.

Existem alguns tipos de vírus mais comuns e é importante sabermos seu funcionamento para identificarmos uma possível infecção. São eles:

Worms

De forma diferente dos vírus, os worms não precisam da ajuda humana para se propagar e infectar: eles infectam uma vez e depois usam as redes de computadores para se propagar para outras máquinas, sem a ajuda dos usuários. Com a exploração das vulnerabilidades de rede, como pontos fracos nos programas de e-mail, os worms podem enviar milhares de cópias suas na esperança de infectar novos sistemas, onde o processo começa novamente. Embora muitos worms apenas "consumam" recursos do sistema, reduzindo seu desempenho, muitos deles contêm "cargas" maliciosas criadas para roubar ou excluir arquivos.



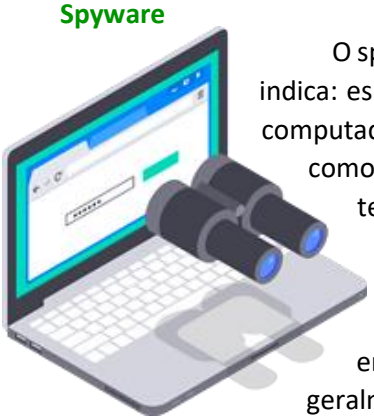
Este tipo de vírus é muito perigoso e deve ser neutralizado com rapidez ou consegue facilmente fugir de controle e infectar diversos dispositivos da mesma rede ou de seus contatos pessoais.

Adware

Um dos incômodos mais comuns da presença on-line é o adware. Os programas enviam anúncios automaticamente para os computadores host. Entre os tipos rotineiros de adware estão os anúncios pop-up em páginas da Web e a publicidade dentro de programas, que geralmente acompanham softwares "gratuitos". Embora alguns programas de adware sejam relativamente inofensivos, outros usam ferramentas de rastreamento para coletar informações sobre sua localização ou seu histórico de navegação, para depois veicular anúncios direcionados em sua tela.

Conforme observado pela BetaNews, foi detectada uma nova forma de adware capaz de desativar seu software antivírus. Como o adware é instalado com o conhecimento e o consentimento da pessoa, esses programas não podem ser chamados de malware: geralmente, são identificados como "programas potencialmente indesejados".

Spyware



O spyware faz o que o nome indica: espiona o que você faz no computador. Ele coleta dados como pressionamentos de teclas, hábitos de navegação e até informações de login que depois são enviados a terceiros, geralmente os criminosos virtuais. Ele também pode modificar configurações de segurança específicas em seu computador ou interferir nas conexões de rede. Segundo a TechEye, as formas emergentes de spyware podem permitir que as empresas rastreiem o comportamento do usuário em diversos dispositivos sem o seu consentimento.

Ransomware

O ransomware infecta seu computador, criptografa dados sigilosos, como documentos pessoais ou fotos, e exige um resgate pela liberação. Se você se recusar a pagar, os dados serão excluídos. Algumas variantes de ransomware bloqueiam todo o acesso ao computador. Elas podem alegar ser de autoridades legais legítimas e sugerir que você foi pego fazendo algo ilegal. Em junho de 2015, o Internet Crime Complaint Center do FBI recebeu queixas de usuários relatando prejuízos de US$ 18 milhões por conta de uma ameaça comum de ransomware, chamada CryptoWall.

Cavalos de Troia

Geralmente chamados de "cavalos Troia", esses programas se escondem mascarados como arquivos ou softwares legítimos. Depois de baixados e instalados, os cavalos de Troia alteram o computador e realizam atividades maliciosas sem o conhecimento ou consentimento da vítima.

3.2. O que é SPAM e como preveni-los

Spam é o termo usado para referir-se aos e-mails não solicitados, que geralmente são enviados para um grande número de pessoas.

A Internet causou grande impacto na vida das pessoas, tornando-se um veículo de comunicação importante, evoluindo para revolucionar a maneira de fazer negócios e buscar e disponibilizar informações. Ela viabiliza a realidade da globalização nas diversas áreas da economia e do conhecimento. Por outro lado, esse canal acabou absorvendo diversas práticas, boas e ruins.

O spam é uma das práticas ruins. Ele ficou famoso ao ser considerado um tormento para os usuários de e-mail, impactando na produtividade de funcionários e degradando o desempenho de sistemas e redes. No entanto, poucos se lembram de que já enfrentaram algo semelhante, antes de utilizar o e-mail como ferramenta de comunicação.

As cartas de correntes para obtenção de dinheiro fácil, encontradas nas caixas de correio, as dezenas de panfletos recebidos nas esquinas e as ligações telefônicas oferecendo produtos são os precursores do spam. A principal diferença, extremamente relevante, é o fato de que para enviar cartas ou panfletos e ligar para nossas casas, o remetente tinha de fazer algum

investimento. Este muitas vezes inviabilizava o envio de material de propaganda em grande escala.

Para evitar o recebimento de Spam os domínios de e-mail oferecem ferramentas para que você bloqueie determinado remetente enviando-o para sua lista de spam.

3.3. Ataques DDoS e computadores zumbis

Ataque DDos (Distributed Denial of Service ou negação distribuída de serviço) é um tipo de ofensiva na qual centenas ou milhares de computadores sobrecarregam um sistema – rede, site, servidor, aplicativo, etc -, o deixando indisponível.

Através de requisições simultâneas e massivas, essas máquinas saturam a capacidade do servidor, o que, consequentemente, o tira do ar. Assim, os visitantes reais não conseguem acessar o serviço.

Mas o que isso tem a ver com zumbis? Bem, são eles que fazem o trabalho sujo.

Para mobilizar a quantidade de computadores necessários para os ataques DDoS, o hacker precisa submeter outras máquinas a seu comando, os transformando em escravos. Um único computador pode comandar centenas de escravos mestres que, por sua vez, controlam milhares ou milhões de escravos zumbis, os levando a atacar um mesmo servidor simultaneamente conforme a sua vontade.

Geralmente, essas máquinas se tornam zumbis de duas formas: voluntariamente ou por infecção viral. Existem vários vírus que podem infectar a máquina e torna-la um zumbi.

Além desses métodos, o hacker ainda pode usar falhas nos sistemas e engenharia social para conseguir escravizar computadores e montar seu exército.

Lembrando que nem sempre esse ataque ao servidor é direcionado. A infecção pode ser feita através de aplicações vulneráveis não atualizadas do servidor que permitem que informações sensíveis sejam indexadas e gerem padrões. Com os padrões gerados, os bots podem utilizar mecanismos de buscas para explorar de forma maliciosa essas vulnerabilidades.

3.4. Exercícios de Conteúdo

1) Quais são os três maus comuns?

2) Fale um pouco sobre o que é SPAM.

3) Fale um pouco sobre o que é vírus.

4) Fale um pouco sobre o que é um ataque DDoS.

5) O que são dispositivos zumbis?

3.5. Exercícios de Fixação

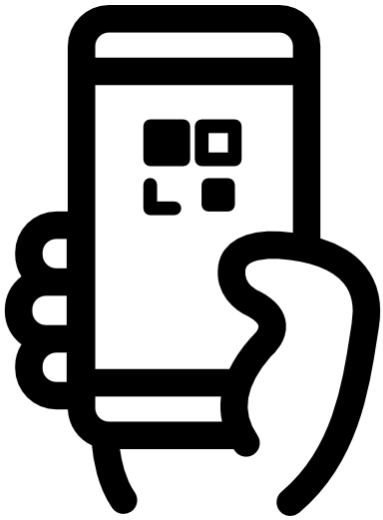
1) Procure na internet sobre o vírus “Sexta-feira 13” e anote suas curiosidades, a forma com que foi utilizado e o número de pessoas afetadas.
2) Procure na internet sobre o grupo “Anonymous” e os ataques de DDoS que eles já efetuaram.

4. Aula 4 – Aplicativos falsos

Aplicativos falsos nos enganam geralmente usando o mesmo ícone e nome, para induzi-lo a fazer o download e, em seguida, bombardeá-lo com anúncios (ou pior, malware).

O Google Play Protect e o recurso Granular Permissions no Android são apenas dois deles. Mesmo assim, aplicativos Android falsos ou aplicativos com malware e adware são completamente inevitáveis. De um jeito ou de outro, esses proprietários de aplicativos conseguem encontrar seu caminho na Play Store e, pior, ficam lá.

A pergunta é: como você identifica aplicativos falsos de aplicativos genuínos na Google Play Store? O que você pode fazer para garantir que nem você nem qualquer outro usuário do Android instalem esses aplicativos em seus dispositivos?



4.1. Identificando aplicativos falsos

O primeiro passo para identificar um arquivo falso é diferenciando-o nos resultados da pesquisa.

O primeiro passo envolvido no download e instalação de um aplicativo é pesquisar o nome do aplicativo. Enquanto na maioria dos casos, haveria apenas uma versão do aplicativo. Se alguém estiver tentando imitar e falsificar um aplicativo popular, ele definitivamente tentará copiar o nome e o ícone do aplicativo.

Portanto, quando você pesquisa um aplicativo específico na Google Play Store e obtém muitos resultados com o mesmo nome ou ícone do aplicativo, provavelmente a maioria deles é falsa. Você deve verificar pelo menos alguns desses fatores mencionados abaixo que podem levantar alguns sinais de alerta:

- O nome do desenvolvedor do aplicativo;
- O número de downloads que tem;
- Classificações do utilizador, para identificar se é uma aplicação genuína ou falsa;

A Google Play Store adicionou recentemente “Data de publicação” para todos os aplicativos da Play Store. Agora, você também pode verificar se o aplicativo já existe há algum tempo ou se foi adicionado recentemente à Play Store.

Quando o download do aplicativo for em seu computador ou outro dispositivo cheque estes pontos:

- O nome do usuário que disponibilizou o arquivo (em caso de torrente);
- O tamanho do arquivo (checar se bate com o tipo de arquivo baixado);
- O número de downloads que o aplicativo possui.

Outra forma de verificar a veracidade de aplicativos é checando a analise feita por pessoas que já efetuaram o download deste aplicativo.

4.2. Fake News, o que são e como identifica-las

Não caia em informações e notícias falsas e muito menos as espalhe por aí.

Antes de passar adiante uma notícia ou apenas aceita-la como verdade siga estes passos:

Analise

Antes de compartilhar um texto, é importante lê-lo com calma. Observe se ele possui palavras em letras maiúsculas, exclamações, abreviações, erros de ortografia e excesso de adjetivos. Desconfie se houver muitas opiniões, títulos sensacionalistas e dados sem indicar a fonte.

Pesquise

As pistas para descobrir fake news vão além do texto. Sites com nomes parecidos com o de veículos conhecidos, que não identificam seus autores e não possuem informações de contato são suspeitos. Às vezes, os especialistas consultados nem existem.

Use o Google!

Confirme

Cheque se a notícia saiu em algum outro jornal, revista ou site. Tome cuidado, pois um conteúdo falso nem sempre é 100% mentiroso. Às vezes é só um trecho usado fora de contexto ou uma matéria muita antiga compartilhada como nova. Essa manipulação contribui para a desinformação.

Denuncie

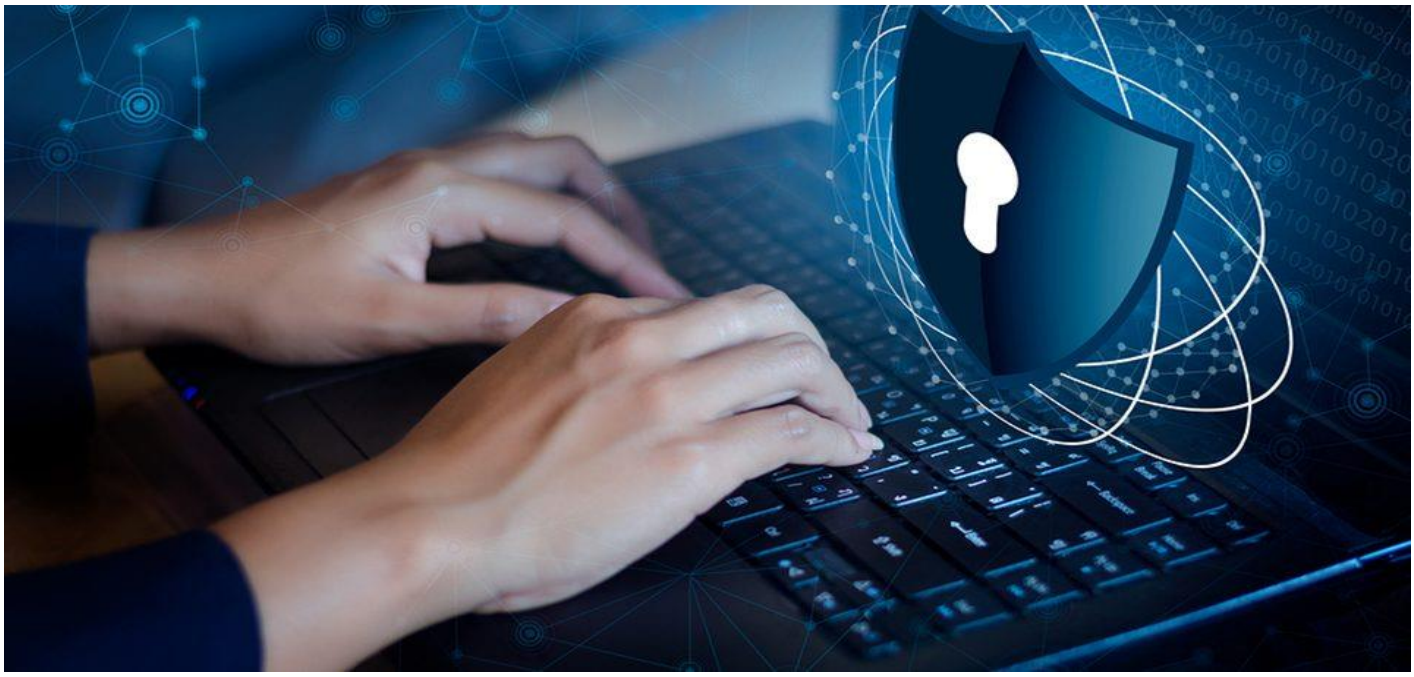
No Facebook, é possível classificar o conteúdo suspeito como “falso”: basta clicar nos três pontinhos do canto direito da publicação. As agências de checagem de fatos especializadas em confirmar ou desmentir discursos políticos, vídeos e até correntes de WhatsApp possuem formulários de denúncia.

4.3. Exercícios de Conteúdo

1) O que são aplicativos (apps) falsos?

2) Como identificar um aplicativo falso?

3) O que são Fake News?



4) O que fazer quando descobrimos uma Fake News?

5) O que fazer quando recebemos uma notícia estranha?

4.4. Exercícios de Fixação

1) Entre no site da Google Play, procure pelo aplicativo “WhatsApp” e veja as informações sobre ele.
2) Anote as seguintes informações sobre o WhatsApp: empresa desenvolvedora, número de downloads, nota recebida pelo aplicativo.
3) Ainda no site da Google Play, procure pelo aplicativo “Netflix”.
4) Identifique pelo menos um Netflix que você ache que possa ser falso e anote os motivos.

5. Aula 5 – Senhas de segurança

Quando se trata de segurança é sempre aconselhado termos o maior cuidado, não é mesmo?

Infelizmente isso acaba não acontecendo com algumas senhas que utilizamos no nosso dia-a-dia.

As senhas são nossas chaves digitais que nos permitem abrir contas e guardar nossos dados pessoais.

Por isso é muito importante as usarmos da forma mais segura possível.

5.1. Criando senhas fortes

Ter diferentes senhas para diferentes serviços é obrigatório bem como atualizá-las frequentemente.

Seguindo estes passos abaixo você conseguirá criar senhas fortes e impedir que as pessoas descubram suas senhas simplesmente tentando as combinações mais lógicas.

Crie diferentes senhas para diferentes serviços

Imagine se a mesma chave abrisse a porta do seu carro, da sua casa e do seu escritório. A lógica é bastante óbvia. Se um hacker consegue entrar em um lugar, ele pode entrar em outro e assim por diante. É essencial ter uma chave diferente para um bloqueio diferente.

Altere as suas senhas regularmente

A mesma lógica se aplica. Manter o mesmo cadeado em sua porta por anos e anos é realmente um convite para um ladrão. Em algum momento, o cadeado é adulterado, o código é quebrado. Altere as suas senhas regularmente.

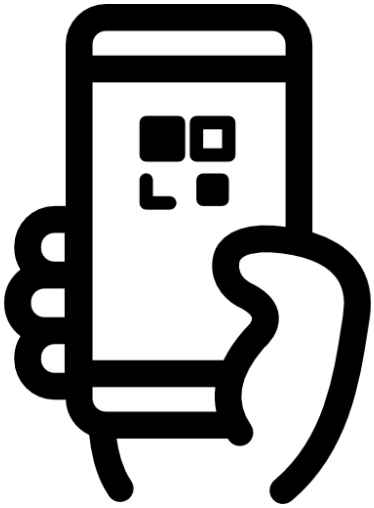
Alguns aplicativos têm configurações para lembrá-lo de alterar suas senhas com frequência. Por exemplo, se você estiver usando o Windows, pode optar por mudar sua senha de login do Windows com frequência usando as opções de senha na Política de Segurança Local. Basta selecionar Política de Senha em Políticas de Conta. Clique duas vezes em Tempo Máximo da Senha no painel direito, insira o número de dias que deseja passar entre as senhas e clique em OK. Agora, esse é um lembrete inteligente.

Escolha a senha certa

As senhas devem ter no mínimo 8 caracteres e conter uma combinação de números, símbolos, letras maiúsculas, letras minúsculas e um espaço. Eles não devem ser repetitivos, nem ser uma palavra ou ID real.

Opte pela verificação em duas etapas

O Gmail, juntamente com o Facebook, oferece essa forma perfeita de manter sua segurança intacta. Ao fazer login, ele simplesmente pede que você insira um código que envia para o seu celular. Rápido, inteligente e funcional.



5.2. Criando backups para restauração

Como ter a certeza que nossos dados estarão sempre seguros e disponíveis? Como definição, backup é o ato de copiar arquivos, pastas ou discos inteiros (físicos ou virtuais) para sistemas de armazenamento secundários, buscando a preservação dos dados em caso de qualquer problema.

Somos todos reféns de nossas informações, sejam elas apenas uma lista de contatos do celular ou milhares de prontuários médicos armazenados dentro de grandes servidores.

O objetivo de montar um procedimento de backup, corporativo ou residencial, é ter uma ou mais cópias de segurança fora do sistema principal, seja ele apenas um celular ou um sistema de armazenamento profissional para recuperação dos dados em caso de desastre.

Muitas empresas e usuários domésticos tem utilizado equipamentos como discos externos, pen-drives, drives de mídias ópticas ou sistemas baseados em fita para duplicar suas informações. Além disso, com a redução dos preços da transmissão de dados por cabo ou satélite (banda larga), alguns usuários têm enviado e mantido seus dados como agendas, vídeos e fotos em servidores de terceiros, também conhecidos como servidores de nuvem.

5.3. Quando fazer backup?

Atribuir valor a qualquer tipo de informação pessoal pode ser um processo subjetivo, pois cada usuário atribuirá a importância de manter seus backups pessoais atualizados de acordo com suas próprias experiências.

Geralmente você fará backup de seus arquivos mais importantes com uma periodicidade maior do que de arquivos ou aplicativos que não utilize tanto.

É aconselhado efetuar um backup geral uma vez por semana de seus arquivos e contatos do smartphone e computador e quando se tratarem de arquivos ou documentos de grande importância, atualiza-los com frequência máxima (toda vez que efetuar alguma alteração)

Também é aconselhado que se tenha um backup em mais de um local diferente, um backup na nuvem e um em um dispositivo de disco externo, por exemplo (pendrive, HD externo, etc.).

5.4. Exercícios de Conteúdo

1) O que são senhas de segurança e para que servem?

2) Como criar senhas fortes?

3) É importante criar diferente senhas para diferentes serviços? Por que?

4) Para que servem os backups?

5) Onde podemos efetuar nossos backups?

5.5. Exercícios de Fixação

1) Crie uma conta no G-mail e coloque uma senha que você consiga lembrar com letras, números e símbolos.
2) Passe os contatos do seu smartphone para seu chip.

6. Aula 6 - A importância de sistemas de segurança

A instalação de um bom antivírus está no topo da lista dos principais cuidados a serem tomados para proteger dispositivos, como computadores e smartphones, de ameaças virtuais.

Contudo, engana-se quem pensa que basta instalar o software de proteção e nunca mais atualizá-lo, acreditando que estará em segurança para sempre!

A atualização é recomendada para tudo. Seja os aplicativos do dispositivo ou o próprio sistema operacional.

Ao contrário do que muitos pensam, a renovação não serve deixar o seu aparelho mais lento, obrigando a trocá-lo com maior frequência. Mas sim, para a aplicação de melhorias aperfeiçoadas pelos desenvolvedores.

Nos softwares de proteção, a atualização é responsável por trazer defesas às novas ameaças que vão surgindo no mercado.

Essa é uma precaução global, feita com a ajuda da International Computer Security Association (ICSA), organização que atua localizando ameaças e malwares recentes. As descobertas são analisadas minuciosamente e, os dados, enviados aos desenvolvedores dos programas de proteção virtual em todo o mundo, para que possam criar soluções e proteger os usuários.

Dessa forma, a atualização do antivírus é fundamental para garantir uma proteção de longo prazo. Afinal, novas ameaças são inventadas a cada dia e, quem não se atualiza, fica vulnerável.

6.1. O comportamento do usuário auxilia na prevenção

Sim, o antivírus é um aliado fundamental para o dispositivo ficar longe de ataques.

Porém, um comportamento consciente e cuidadoso do usuário é a melhor prevenção que o computador ou smartphone pode ter contra os programas maliciosos.

Isso porque, mesmo com as atualizações, os criminosos digitais não param de criar novos meios de atingir os dispositivos. Então, quando encontram uma brecha no antivírus e um usuário desatento, o ataque é inevitável.

Por isso, lembre-se de adotar os seguintes cuidados:

- Instale um bom antivírus e atualize-o com frequência;
- Sempre atualize os aplicativos e o sistema operacional;
- Não clique em links suspeitos ou de origem desconhecida, mesmo que tenham sido enviados por pessoas conhecidas;
- Faça downloads somente de sites confiáveis.

6.2. O que é um Firewall?

Um firewall é um dispositivo de segurança da rede que monitora o tráfego de rede de entrada e saída e decide permitir ou bloquear tráfegos específicos de acordo com um conjunto definido de regras de segurança.

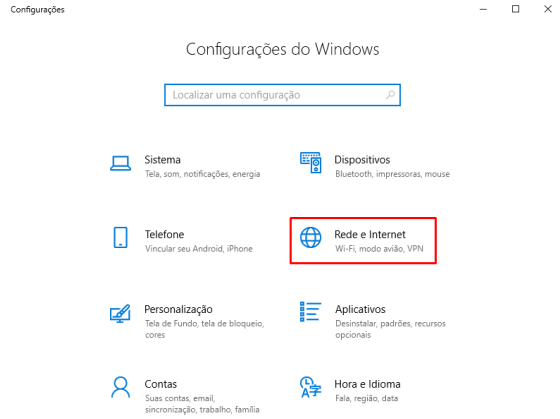
Os firewalls têm sido a linha de frente da defesa na segurança de rede há mais de 25 anos. Eles colocam uma barreira entre redes internas protegidas e controladas que podem ser redes externas confiáveis ou não, como a Internet.

6.3. Como configurar o Firewall do Windows

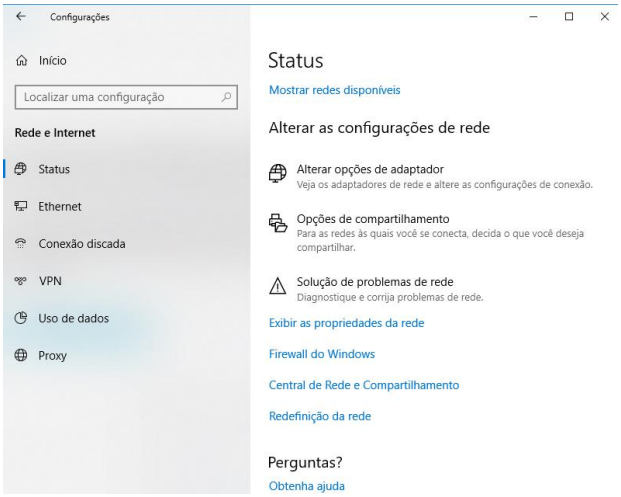
Para acessar o Firewall do Windows, você precisa clicar no menu iniciar.

Em seguida, clique sobre a opção “configurações”.

Com o menu de configurações aberto, clique em “Rede e internet”.



Em seguida, clique em “firewall do Windows”.



Na tela a seguir, você terá opções de configuração de rede, domínio, configurações de permissão do firewall, solução de problemas, notificações e configurações avançadas.

Clicando em “Permitir um aplicativo pelo Firewall” você poderá selecionar algum aplicativo de uma lista para permitir que funcione sem passar pelo Firewall.

6.4. Exercícios de Conteúdo

1) O que é imprescindível para termos a proteção de nosso antivírus?

2) Para que serve a atualização do antivírus?

3) O que é o Firewall?

4) É importante atualizarmos o sistema operacional? Por que?

5) Quando queremos acessar um aplicativo e o Firewall não permite o que podemos fazer?

6.5. Exercícios de Fixação

1) Entre no site do Avast.
2) Instale o Avast antivírus.
3) Acesse o Firewall do Windows.
4) Procure pelo aplicativo “Conteúdo da Microsoft” dentro das permissões e tire um print da tela.
5) Copie e cole o print da tela no paint.