Título 1 - Riscos na internet: A segurança na internet envolve a proteção contra diversos riscos que os usuários podem enfrentar ao navegar online. Esses riscos incluem o acesso a conteúdos impróprios, contato com pessoas mal-intencionadas, furto de identidade, e invasão de privacidade.

1

É essencial proteger os funcionários contra o acesso a conteúdos impróprios ou ofensivos durante o uso da internet. Para isso, a empresa deve utilizar **filtros de conteúdo que bloqueiem sites inadequados** e **monitorar as atividades online.** Implementar softwares de filtragem de conteúdo e **ensinar os funcionários sobre**

os riscos de acessar conteúdos impróprios. Supervisão constante e **diálogo aberto sobre o uso seguro da internet** são fundamentais.

2

Existem pessoas que se aproveitam do anonimato na internet para aplicar golpes, tentando se passar por outras pessoas e cometendo crimes. Funcionários da empresa podem ser alvo de pessoas mal-intencionadas. Para se proteger, é crucial **verificar a identidade de contatos online** e **estar informado sobre os riscos**. Ensinando **sobre os perigos de interagir com desconhecidos online** e promover a verificação de identidade. Utilizar ferramentas de segurança, como **autenticação em duas etapas**, para proteger suas contas e dados da empresa.

3

O furto de identidade pode ocorrer quando alguém tenta se passar por um funcionário da empresa e executar ações em seu nome, colocando em risco a reputação da empresa. Para proteger a mesma, mantenha dados pessoais e corporativos seguros e **utilize autenticação em duas etapas**. Tomar medidas de segurança, como **senhas fortes** para proteger suas contas. Evitar compartilhar informações em plataformas públicas e estar **atento a sinais de roubo de identidade**.

4

A divulgação de informações pessoais e corporativas pode comprometer a privacidade dos funcionários e da empresa. Para a proteção, é importante **gerenciar quem tem acesso aos dados** e ajustar as configurações de privacidade. Revisar e **ajustar regularmente as configurações de privacidade** em todas as plataformas utilizadas pela empresa. Evitar compartilhar informações sensíveis e **estar ciente das políticas de privacidade** dos sites que você e a empresa utiliza.

Título 2 - Cuidados e benefícios: Para se proteger, é essencial adotar cuidados como senhas seguras, utilizar conexões seguras **(HTTPS)** e estar atento a golpes e fraudes. Manter senhas fortes e únicas para cada serviço utilizado pela empresa ajuda a prevenir acessos não autorizados. Apesar dos riscos, a internet oferece inúmeros benefícios, como acesso a informações, serviços bancários, compras online e comunicação eficiente entre equipes e com clientes. Esses benefícios podem ser aproveitados de forma segura e consciente, permitindo que a empresa desfrute das vantagens da internet sem comprometer sua segurança.

2.0 Golpes na Internet:

Golpes na internet são cada vez mais comuns e sofisticados, incluindo ataques como phishing e ransomware. Casos notáveis incluem o ataque WannaCry em 2017 e o roubo de dados da Equifax no mesmo ano. Para se prevenir, use senhas fortes e exclusivas, ative a autenticação de dois fatores e mantenha tudo atualizado. Fique atento a links e anexos suspeitos e verifique a segurança dos sites. No Brasil, aproximadamente 3 em cada 10 pessoas já foram vítimas de golpes online. Informar-se sobre essas táticas pode reduzir significativamente os riscos. Mantenha-se seguro!

2.1 Furto de identidade (*Identity theft*):

O furto de identidade, conhecido como identity theft, é quando alguém se pas sa por outra pessoa para obter vantagens. Isso pode acontecer no mundo físico ou o nline. No dia a dia, alguém pode abrir uma empresa ou conta bancária em seu nome. Na internet, a ameaça é maior: golpistas criam perfis falsos em redes sociais, acessa m e-mails ou falsificam mensagens.

Quanto mais você compartilha sobre sua vida, mais fácil é para um criminoso roubar sua identidade. Eles usam técnicas como malwares, ataques de força bruta e interceptação de tráfego.

Prevenção:

Para proteger seus dados de hackers, sempre os armazene em locais seguros e evite compartilhar suas senhas com pessoas não confiáveis. Crie senhas aleatórias e não relacionadas às suas informações pessoais. Utilize a autenticação de dois fatores para adicionar uma camada extra de segurança. Mantenha seus dispositivos e softwares atualizados, pois as atualizações frequentemente incluem correções de segurança importantes. Um gerenciador de senhas pode ajudar a criar e armazenar senhas seguras. Fique atento a e-mails e links suspeitos, já que hackers muitas vezes usam phishing para obter suas informações. Monitore regularmente suas contas para verificar atividades suspeitas e, se necessário, tome medidas imediatamente.

2.2 Fraude de antecipação de recursos *(Advance fee fraud)*

A fraude de antecipação de recursos, ou advance fee fraud, envolve golpistas que induzem vítimas a fornecer informações confidenciais ou realizar pagamentos adiantados, prometendo um benefício futuro. As vítimas são enganadas através de mensagens eletrônicas ou sites fraudulentos com histórias mirabolantes. Após fornecer os recursos, a pessoa descobre que o benefício prometido não existe e que foi vítima de um golpe, perdendo seus dados ou dinheiro para os golpistas.

Loteria internacional: Você recebe um e-mail falando que você foi o ganhador de uma loteria internacional, mas para você resgatar o prêmio tem que informar seus dados pessoais

Crédito fácil: Uma oferta de empréstimo com taxas de juros muito baixas chega por e-mail. Após suposta aprovação, pedem um depósito bancário para cobrir despesas.

Doação de animais: Ao buscar um animal de raça cara, você encontra sites oferecendo doação. Após contato, solicitam dinheiro para transporte.

Oferta de emprego: Uma proposta de emprego tentadora chega ao seu celular, mas, para efetivar a contratação, pedem detalhes da sua conta bancária.

Noiva russa: Alguém deixa recados insinuando um possível relacionamento amoroso. Esta pessoa, geralmente da Rússia, sugere um encontro, mas precisa de ajuda financeira para viajar.

Prevenção:

A melhor forma de se prevenir contra golpes é identificar as mensagens suspeitas. Essas mensagens geralmente oferecem grandes quantias, pedem sigilo nas transações, solicitam respostas rápidas, usam termos como "urgente" e "confidencial" no assunto e têm erros gramaticais e de ortografia devido ao uso de tradutores automáticos. Para evitar ser vítima, sempre questione por que você foi escolhido para receber a proposta e desconfie de situações em que se pede um

pagamento com a promessa de um retorno maior. Nunca responda a essas mensagens, pois isso pode confirmar que seu e-mail é válido, aumentando a chance de ser alvo de outros golpes ou spam.

2.3 Phishing

Phishing é uma fraude onde golpistas tentam obter dados pessoais e financeiros de usuários através de técnicas e engenharia social. Eles enviam mensagens eletrônicas que se passam por comunicações oficiais de instituições conhecidas, como bancos ou empresas populares. Essas mensagens atraem a atenção do usuário com promessas de vantagens financeiras ou ameaças de consequências graves, como o cancelamento de contas bancárias.

Os golpistas induzem o usuário a fornecer informações pessoais e financeiras por meio de páginas falsas que imitam sites oficiais, instalação de códigos maliciosos ou preenchimento de formulários contidos nas mensagens. Exemplos comuns de phishing incluem páginas falsas de comércio eletrônico ou Internet Banking, onde o usuário é direcionado para um site falso que solicita seus dados; páginas falsas de redes sociais ou companhias aéreas, onde o usuário é induzido a fornecer seu nome de usuário e senha; mensagens contendo formulários para preenchimento de dados pessoais e financeiros; e mensagens com links para códigos maliciosos que, ao serem executados, instalam software malicioso no computador do usuário.

O termo “phishing” vem do inglês “fishing”, fazendo uma analogia com o uso de “iscas” (mensagens eletrônicas) para “pescar” senhas e dados financeiros dos usuários. As mensagens de phishing podem variar conforme os temas em destaque no momento, explorando campanhas de publicidade, serviços e assuntos populares.

Prevenção:

Para evitar golpes online, é importante estar atento a mensagens suspeitas, es pecialmente aquelas que solicitam informações pessoais, instalação de programas o u cliques em links. Questione por que instituições com as quais você não tem contat o estariam enviando mensagens.

Desconfie de mensagens que apelam demasiadamente pela sua atenção ou a meaçam caso não execute as ações sugeridas. Mensagens confiáveis nem sempre s ão provenientes de remetentes confiáveis, pois podem ser enviadas de contas invadi das ou perfis falsos.

Ao acessar links, prefira digitar o endereço diretamente no navegador e verifiq ue se a página utiliza uma conexão segura. Golpistas costumam ofuscar o link real, mas você pode visualizar o endereço verdadeiro ao posicionar o mouse sobre o link.

Utilize programas antimalware, firewalls pessoais e filtros antiphishing para au mentar a segurança. Sempre verifique as informações no certificado da página, princ ipalmente em sites de comércio eletrônico e internet banking, para garantir a autenti cidade.

Além disso, acesse diretamente o site oficial da instituição para confirmar a ve racidade das mensagens recebidas, uma vez que a maioria das empresas não envia e-mails indiscriminados aos seus usuários.

2.3.1 *Pharming*

Pharming é um tipo específico de phishing que redireciona a navegação do usuário para sites falsos através de alterações no serviço de DNS (Domain Name System). Q uando você tenta acessar um site legítimo, seu navegador é redirecionado de forma transparente para uma página falsa. Isso pode acontecer devido ao comprometiment o do servidor de DNS do seu provedor, pela ação de códigos maliciosos que alteram o comportamento do DNS no seu computador, ou pela ação direta de um invasor q ue acessa as configurações de DNS do seu computador ou modem de banda larga.

Prevenção:

Para evitar golpes online, desconfie de redirecionamentos inesperados ao digi tar uma URL, especialmente se o novo site tentar abrir arquivos ou instalar programa s. Certifique-
se de que sites de comércio eletrônico ou internet banking utilizem conexões segura s ao solicitar dados pessoais ou financeiros. Sempre verifique se o certificado do site corresponde ao do site verdadeiro para garantir sua autenticidade. Mantenha-
se alerta e proteja suas informações online.

2.4 Golpes de comércios eletrônicos

Golpes de comércio eletrônico são fraudes em que golpistas, visando obter vantagens financeiras, exploram a relação de confiança entre as partes envolvidas em uma transação comercial. A seguir, apresentamos alguns desses golpes.

2.4.1 Golpe do site de comercio fraudulento

Esse tipo de golpe é conhecido como fraude de comércio eletrônico. Nele, o golpista cria um site fraudulento com o objetivo específico de enganar possíveis clientes. Após efetuarem os pagamentos, os clientes não recebem as mercadorias. Para aumentar as chances de sucesso, o golpista costuma utilizar artifícios como envio de spam, propaganda via links patrocinados, anúncios de descontos em sites de compras coletivas e ofertas de produtos muito procurados com preços abaixo dos praticados pelo mercado.

Além do comprador, que paga, mas não recebe a mercadoria, esse tipo de golpe pode ter outras vítimas. Uma empresa séria pode ter seu nome vinculado ao golpe, um site de compras coletivas pode ser responsabilizado se intermediou a compra, e uma pessoa física pode ter sua identidade usada para a criação do site ou para a abertura de empresas fantasmas.

Prevenção:

Para evitar cair em golpes de comércio eletrônico, é importante tomar algumas precauções. Primeiro, faça uma pesquisa de mercado, comparando o preço do produto no site com os valores obtidos na pesquisa e desconfie se ele for muito abaixo dos praticados pelo mercado. Pesquise na internet sobre o site antes de efetuar a compra para ver a opinião de outros clientes e acesse sites especializados em tratar reclamações de consumidores insatisfeitos para verificar se há reclamações referentes a essa empresa.

Fique atento a propagandas recebidas através de spam e seja cuidadoso ao acessar links patrocinados. Procure validar os dados de cadastro da empresa no site da Receita Federal. Além disso, não informe dados de pagamento caso o site não

ofereça conexão segura ou não apresente um certificado confiável. Essas medidas podem ajudar a proteger você de fraudes online.

2.4. golpes envolvendo sites de compras coletivas

Sites de compras coletivas têm sido frequentemente utilizados em golpes de comércio eletrônico fraudulentos. Esses sites apresentam riscos próprios, principalmente devido à pressão imposta ao consumidor para tomar decisões rápidas, sob pena de perder a oportunidade de compra. Golpistas criam sites fraudulentos e anunciam produtos nesses sites de compras coletivas, conseguindo assim muitos vítimas em pouco tempo.

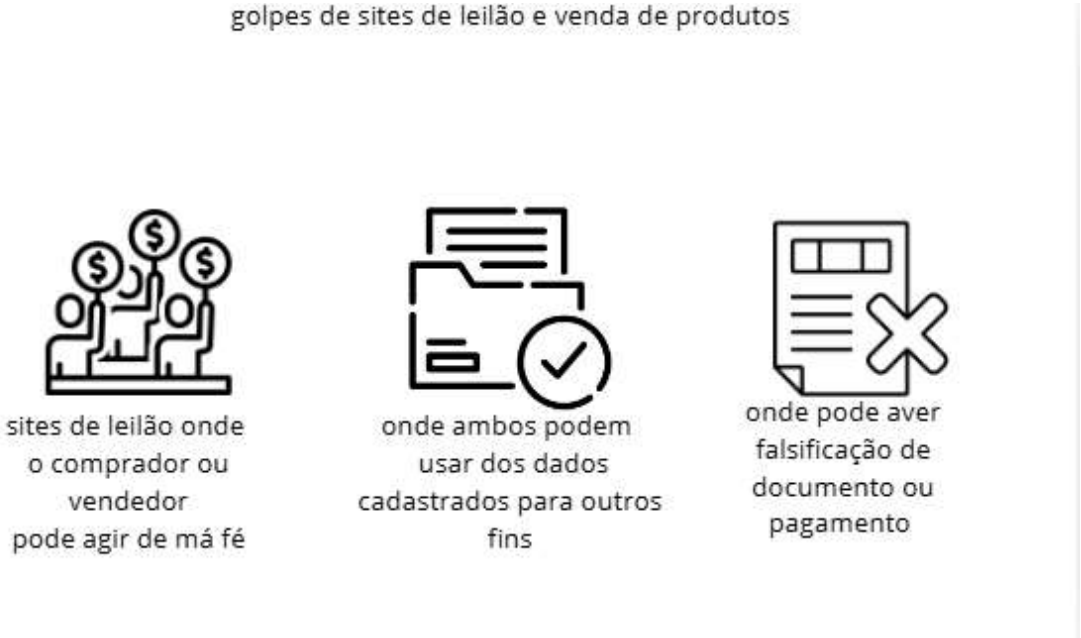
Além disso, sites de compras coletivas podem ser usados como tema de mensagens de phishing. Golpistas enviam mensagens que parecem ser do site verdadeiro, induzindo o usuário a acessar uma página falsa e fornecer dados pessoais, como número de cartão de crédito e senhas. Esses golpes exploram a confiança dos consumidores e a urgência das ofertas para obter informações sensíveis.

Prevenções:

Para evitar cair em golpes ao usar sites de compras coletivas, é importante não comprar por impulso apenas para garantir o produto ofertado. Seja cauteloso e faça pesquisas prévias, pois há casos de produtos anunciados com desconto que, na verdade, apresentam valores superiores aos de mercado. Pesquise na internet sobre o site de compras coletivas antes de efetuar a compra para ver a opinião de outros clientes e observar se a forma como possíveis problemas foram resolvidos foi satisfatória. Além disso, siga as dicas para se prevenir de golpes envolvendo

phishing e sites de comércio eletrônico fraudulentos. Essas medidas podem ajudar a proteger você de fraudes e garantir uma experiência de compra mais segura.

2.4.2 golpes de sites de leilão e venda de produtos



O golpe do site de leilão e venda de produtos ocorre quando um comprador ou vendedor age de má-fé e não cumpre com as obrigações acordadas, ou utiliza os dados pessoais e financeiros envolvidos na transação para outros fins. Por exemplo, o comprador pode tentar receber a mercadoria sem realizar o pagamento ou fazê-lo por meio de transferência de uma conta bancária ilegítima ou furtada. O vendedor, por sua vez, pode tentar receber o pagamento sem entregar a mercadoria, ou entregar um produto danificado, falsificado, com características diferentes do anunciado, ou adquirido de forma ilícita, como contrabando ou roubo de carga. Além disso, tanto o comprador quanto o vendedor podem enviar e-mails falsos em nome do sistema de gerenciamento de pagamentos para comprovar a realização do pagamento ou o envio da mercadoria, quando na realidade isso não ocorreu.

Prevenção:

Para evitar golpes ao comprar produtos online, é importante fazer uma pesquisa de mercado, comparando o preço do produto com os valores obtidos na pesquisa e desconfiar se ele for muito abaixo dos praticados pelo mercado. Marque encontros em locais públicos caso a entrega dos produtos seja feita pessoalmente. Acesse sites especializados em tratar reclamações de consumidores insatisfeitos e que os colocam em contato com os responsáveis pela venda, para avaliar se a forma como o problema foi resolvido foi satisfatória. Utilize sistemas de gerenciamento de pagamentos, pois além de dificultarem a aplicação dos golpes, impedem que seus dados pessoais e financeiros sejam enviados aos golpistas. Procure confirmar a

realização de um pagamento diretamente em sua conta bancária ou pelo site do sistema de gerenciamento de pagamentos, não confiando apenas em e-mails recebidos, pois eles podem ser falsos. Verifique a reputação do usuário, já que muitos sites possuem sistemas que medem a reputação de compradores e vendedores por meio da opinião de pessoas que já negociaram com este usuário. Acesse os sites, tanto do sistema de gerenciamento de pagamentos como o responsável pelas vendas, diretamente do navegador, sem clicar em links recebidos em mensagens. Mesmo que o vendedor lhe envie o código de rastreamento fornecido pelos Correios, não utilize essa informação para comprovar o envio e liberar o pagamento, pois até que você tenha a mercadoria em mãos, não há nenhuma garantia de que o que foi enviado é realmente o que foi solicitado.

2.5 boato (*Hoax*)

Um boato, ou hoax, é uma mensagem com conteúdo alarmante ou falso que geralmente aponta como autora alguma instituição, empresa importante ou órgão governamental. Esses boatos podem causar diversos problemas, como a disseminação de códigos maliciosos, a propagação de desinformação, e a ocupação desnecessária de espaço nas caixas de e-mails dos usuários. Além disso, eles podem comprometer a credibilidade e reputação das pessoas ou entidades mencionadas, bem como de quem repassa a mensagem, pois ao fazer isso, a pessoa está supostamente endossando o conteúdo. Boatos também podem aumentar a carga de servidores de e-mail e o consumo de banda de rede necessários para a transmissão e processamento das mensagens. Por fim, eles podem sugerir ações que, se realizadas, podem causar sérios danos, como apagar arquivos importantes do sistema operacional do computador.

Prevenção:

Boatos geralmente se propagam pela boa vontade e solidariedade de quem os recebe, pois as pessoas tendem a confiar no remetente, sem verificar a procedência ou a veracidade do conteúdo. Para evitar a distribuição de boatos, é crucial conferir a origem dos e-mails e, mesmo que venham de alguém conhecido, certificar-se de que a mensagem não é um boato. Boatos costumam apresentar características como afirmar que não são boatos, sugerir consequências trágicas se uma determinada tarefa não for realizada, prometer ganhos financeiros ou prêmios mediante a realização de alguma ação, conter erros gramaticais e de ortografia, e apresentar informações contraditórias.

3.0 ataques na internet

Ataques na Internet ocorrem com diversos objetivos, visando diferentes alvos e utilizando variadas técnicas. Qualquer serviço, computador ou rede acessível via Internet pode ser alvo de um ataque, assim como qualquer computador com acesso à Internet pode participar de um ataque. Os motivos dos atacantes variam desde simples diversão até ações criminosas. Alguns exemplos incluem demonstração de poder, onde o atacante mostra a uma empresa que ela pode ser invadida ou ter seus serviços suspensos para vender serviços ou chantageá-la; prestígio, onde o atacante se vangloria por invadir computadores ou tornar serviços inacessíveis; motivações financeiras, onde informações confidenciais são coletadas para aplicar golpes; motivações ideológicas, onde sites são invadidos ou tornados inacessíveis por divulgarem conteúdo contrário à opinião do atacante; e motivações comerciais, onde sites e computadores de empresas concorrentes são invadidos para comprometer sua reputação ou impedir o acesso dos clientes. Para alcançar esses objetivos, os atacantes utilizam diversas técnicas.

3.1 exploração de vulnerabilidades

Uma vulnerabilidade é uma condição que, quando explorada por um atacante, pode resultar em uma violação de segurança. Exemplos de vulnerabilidades incluem falhas no projeto, na implementação ou na configuração de programas, serviços ou equipamentos de rede. Um ataque de exploração de vulnerabilidades ocorre quando um atacante utiliza uma vulnerabilidade para executar ações maliciosas, como invadir um sistema, acessar informações confidenciais, disparar ataques contra outros computadores ou tornar um serviço inacessível.

3.2 varreduras em redes (*scan*)

A varredura em redes, também conhecida como scan, é uma técnica utilizada para realizar buscas detalhadas em redes com o objetivo de identificar computadores ativos e coletar informações sobre eles, como serviços disponíveis e programas instalados. Com essas informações, é possível associar vulnerabilidades aos serviços e programas detectados. Essa técnica pode ser usada de forma legítima, por pessoas autorizadas, para verificar a segurança de computadores e redes, permitindo a tomada de medidas corretivas e preventivas. No entanto, também pode ser utilizada de forma maliciosa por atacantes, que exploram as vulnerabilidades encontradas para realizar atividades maliciosas, como a propagação de códigos maliciosos e ataques de força bruta.

3.3 falsificação de e-mails*(e-mails spoofing)*

A falsificação de e-mail, ou e-mail spoofing, é uma técnica que envolve a alteração dos campos do cabeçalho de um e-mail para que pareça ter sido enviado de uma origem específica, quando na verdade foi enviado de outra. Isso é possível devido às características do protocolo SMTP (Simple Mail Transfer Protocol), que permite a falsificação de campos como “From:” (endereço do remetente), “Reply-To” (endereço de resposta) e “Return-Path” (endereço para onde são reportados erros no envio).

Essa técnica é frequentemente utilizada para a propagação de códigos maliciosos, envio de spam e golpes de phishing. Atacantes usam endereços de e-mail coletados de computadores infectados para enviar mensagens que parecem ser de pessoas conhecidas, induzindo os destinatários a clicar em links ou executar anexos maliciosos. Exemplos comuns incluem e-mails que parecem ser de alguém conhecido solicitando a execução de um arquivo anexo, de um banco pedindo informações da conta bancária, ou de um administrador de serviço de e-mail solicitando informações pessoais sob ameaça de bloqueio da conta.

Você pode perceber que seu endereço de e-mail foi falsificado se começar a receber respostas de e-mails que nunca enviou, mensagens aparentemente enviadas por você mesmo, ou mensagens de devolução de e-mails que você não enviou, reportando erros como usuário desconhecido ou caixa de entrada lotada.

3.4 interceptações de tráfego *(sniffing)*

A interceptação de tráfego, ou sniffing, é uma técnica que envolve a inspeção dos dados que trafegam em redes de computadores, utilizando programas específicos chamados sniffers. Essa técnica pode ser usada de forma legítima por administradores de redes para detectar problemas, analisar o desempenho e monitorar atividades maliciosas nas redes que administram. No entanto, também pode ser utilizada de forma maliciosa por atacantes para capturar informações

sensíveis, como senhas, números de cartão de crédito e conteúdo de arquivos confidenciais que trafegam por conexões inseguras, ou seja, sem criptografia. As informações capturadas são armazenadas na forma em que trafegam, portanto, dados criptografados só serão úteis ao atacante se ele conseguir decodificá-los.

3.5 forças bruta (*brute force*)

Um ataque de força bruta, ou brute force, é uma técnica que envolve adivinhar, por tentativa e erro, um nome de usuário e senha para acessar sites, computadores e serviços com os mesmos privilégios do usuário. Qualquer dispositivo acessível via Internet, protegido por nome de usuário e senha, pode ser alvo desse tipo de ataque, incluindo dispositivos móveis, especialmente se o atacante tiver acesso físico a eles.

Se um atacante obtiver seu nome de usuário e senha, ele pode realizar ações maliciosas em seu nome, como trocar sua senha, dificultando seu acesso ao site ou computador invadido; invadir seu serviço de e-mail, acessando suas mensagens e lista de contatos, e enviando mensagens em seu nome; acessar suas redes sociais, enviando mensagens maliciosas aos seus seguidores ou alterando suas configurações de privacidade; e invadir seu computador, executando ações como apagar arquivos, obter informações confidenciais e instalar códigos maliciosos.

Mesmo que o atacante não consiga descobrir sua senha, você pode ter problemas para acessar sua conta se ela sofrer um ataque de força bruta, pois muitos sistemas bloqueiam contas após várias tentativas de acesso sem sucesso. Embora esses ataques possam ser realizados manualmente, geralmente são feitos com ferramentas automatizadas facilmente obtidas na Internet, tornando o ataque mais eficaz.

As tentativas de adivinhação geralmente se baseiam em dicionários de diferentes

idiomas, listas de palavras comuns, substituições óbvias de caracteres, sequências numéricas e de teclado, e informações pessoais conhecidas ou coletadas na Internet. Dependendo de como é realizado, um ataque de força bruta pode resultar em um ataque de negação de serviço devido à sobrecarga de tentativas em um curto período.

3.6 desfigurações da pagina *(defacement)*

A desfiguração de página, também conhecida como defacement ou pichação, é uma técnica que envolve a alteração do conteúdo de uma página web de um site. Os atacantes, chamados de defacers, podem utilizar várias formas para desfigurar uma página web, incluindo a exploração de erros na aplicação web, vulnerabilidades no servidor de aplicação web, vulnerabilidades na linguagem de programação ou nos pacotes utilizados no desenvolvimento da aplicação web, invasão do servidor onde a aplicação web está hospedada para alterar diretamente os arquivos do site, e furto de senhas de acesso à interface web usada para administração remota.

3.6 negações de serviço *(DoS ou DDoS)*

A negação de serviço, ou DoS (Denial of Service), é uma técnica onde um atacante utiliza um computador para tirar de operação um serviço, um computador ou uma rede conectada à Internet. Quando realizada de forma coordenada e distribuída, utilizando vários computadores, é chamada de negação de serviço distribuída, ou DDoS (Distributed Denial of Service). O objetivo desses ataques não é invadir ou coletar informações, mas exaurir recursos e causar indisponibilidade ao alvo, prejudicando todos que dependem dos recursos afetados.

Em ataques registrados, os alvos ficaram impedidos de oferecer serviços durante o período do ataque, mas voltaram a operar normalmente depois, sem vazamento de informações ou comprometimento de sistemas. Algumas pessoas podem voluntariamente usar ferramentas para participar de ataques, mas a maioria dos computadores envolvidos está infectada e faz parte de botnets sem o conhecimento de seus donos.

Ataques de negação de serviço podem ser realizados de várias maneiras, como enviando uma grande quantidade de requisições para um serviço, consumindo seus recursos e impedindo que outras requisições sejam atendidas; gerando grande tráfego de dados para uma rede, ocupando toda a banda disponível e tornando indisponível o acesso a computadores ou serviços dessa rede; ou explorando vulnerabilidades em programas, tornando um serviço inacessível.

Em situações de saturação de recursos, um serviço pode ficar inoperante ao tentar atender suas próprias solicitações legítimas. Por exemplo, um site de transmissão de jogos da Copa do Mundo pode não suportar uma grande quantidade de usuários assistindo aos jogos finais e parar de funcionar.

3.6 Prevenções

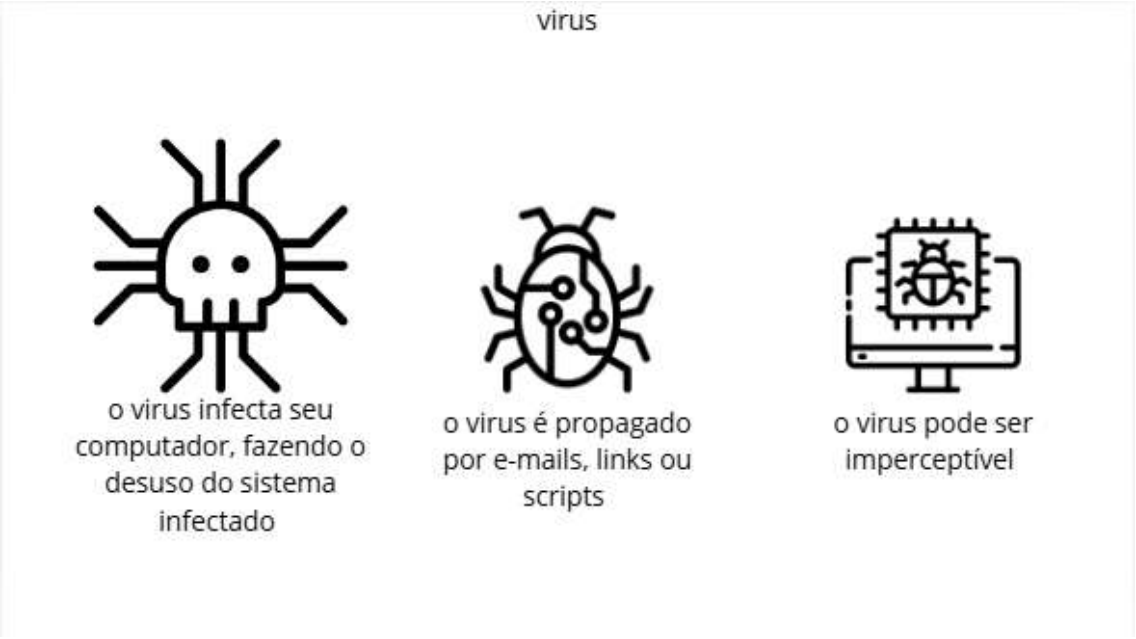
As chances de um ataque na Internet ser bem-sucedido dependem das medidas preventivas adotadas por usuários, desenvolvedores de aplicações e administradores de computadores, serviços e equipamentos. Se cada um fizer sua parte, muitos ataques podem ser evitados ou minimizados. Como usuário da Internet, é importante proteger seus dados, usar mecanismos de proteção disponíveis e manter seu computador atualizado e livre de códigos maliciosos. Isso contribui para a segurança geral da Internet, pois reduz a quantidade de computadores vulneráveis e infectados, diminui a eficácia das botnets e dos ataques de negação de serviço, aumenta a conscientização sobre mecanismos de segurança, melhora a qualidade das senhas, e promove o uso de criptografia para proteger dados. Além disso, a redução de vulnerabilidades em seu computador diminui as chances de invasão ou infecção.

4. Códigos maliciosos (*Malwares*)

Códigos maliciosos, ou malware, são programas desenvolvidos para realizar ações danosas e atividades maliciosas em um computador. Eles podem infectar ou comprometer um computador de várias maneiras, como explorando vulnerabilidades nos programas instalados, auto executando-se a partir de mídias removíveis infectadas, acessando páginas web maliciosas com navegadores vulneráveis, através da ação direta de atacantes que invadem o computador e incluem arquivos maliciosos, ou pela execução de arquivos infectados obtidos de anexos de e-mails, mídias removíveis, páginas web ou compartilhamento de recursos.

Uma vez instalados, os códigos maliciosos têm acesso aos dados armazenados no computador e podem executar ações em nome dos usuários, conforme suas permissões. Os principais motivos para o desenvolvimento e propagação de malware incluem a obtenção de vantagens financeiras, a coleta de informações confidenciais, o desejo de autopromoção e o vandalismo. Além disso, os códigos maliciosos são frequentemente usados como intermediários para golpes, ataques e disseminação de spam.

4.1 Vírus



Um vírus é um programa ou parte de um programa de computador, geralmente malicioso, que se propaga inserindo cópias de si mesmo e se tornando parte de outros programas e arquivos. Para se tornar ativo e continuar o processo de infecção, o vírus depende da execução do programa ou arquivo hospedeiro. Ou seja, para que seu computador seja infectado, é necessário que um programa já infectado seja executado.

Os disquetes costumavam ser o principal meio de propagação de vírus, mas com o tempo, novas formas surgiram, como o envio de e-mails. Atualmente, mídias removíveis, especialmente pen-drives, são o principal meio de propagação.

Existem diferentes tipos de vírus. Alguns permanecem ocultos, infectando arquivos do disco e executando atividades sem o conhecimento do usuário, enquanto outros ficam inativos por certos períodos, entrando em atividade apenas em datas específicas. Entre os tipos mais comuns estão:

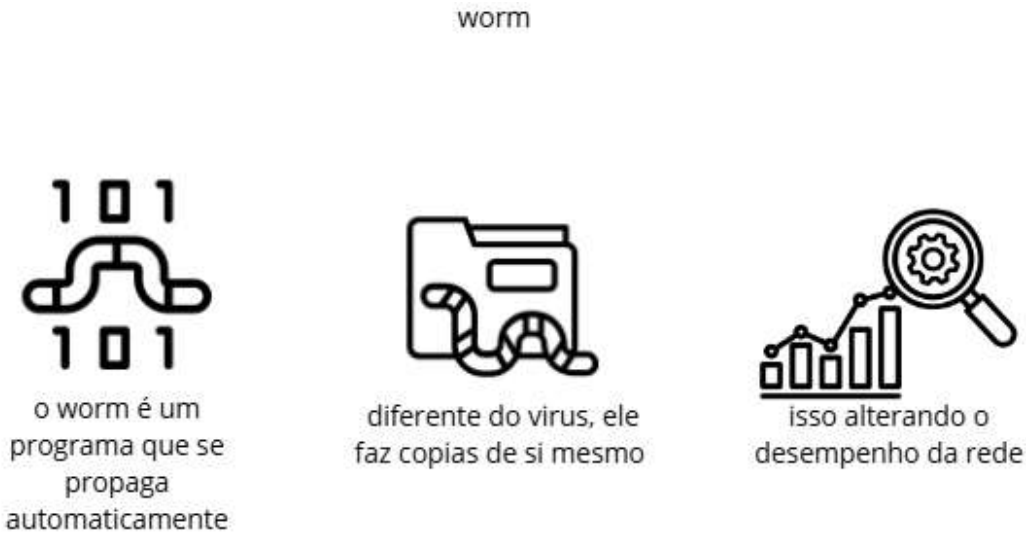
- **Vírus propagado por e-mail**: Recebido como um anexo de e-mail que tenta induzir o usuário a clicar e executar o arquivo, infectando outros arquivos e enviando cópias de si mesmo para contatos do usuário.

- **Vírus de script**: Escrito em linguagens como VBScript e JavaScript, pode ser recebido ao acessar uma página web ou por e-mail, e pode ser executado automaticamente dependendo das configurações do navegador e do leitor de e-mails.

- **Vírus de macro**: Escrito em linguagem de macro, tenta infectar arquivos manipulados por aplicativos como os do Microsoft Office.

- **Vírus de telefone celular**: Propaga-se de celular para celular via Bluetooth ou mensagens MMS. A infecção ocorre quando o usuário permite o recebimento e execução de um arquivo infectado, podendo destruir arquivos, transmitir contatos, fazer ligações e drenar a bateria, além de tentar se propagar para outros celulares.

- **4.2 *worm***



Um worm é um programa que se propaga automaticamente pelas redes, enviando cópias de si mesmo de computador para computador. Diferente de um vírus, ele não se propaga inserindo cópias de si mesmo em outros programas ou arquivos, mas sim pela execução direta de suas cópias ou pela exploração automática de vulnerabilidades em programas instalados nos computadores.

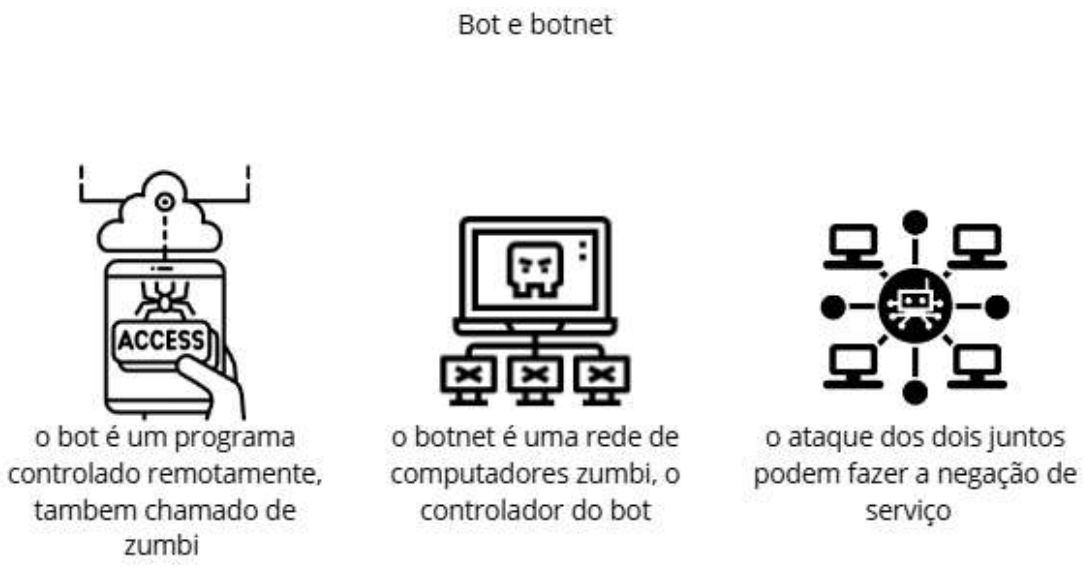
Worms são conhecidos por consumir muitos recursos devido à grande quantidade de cópias que propagam, o que pode afetar o desempenho de redes e a utilização de computadores. O processo de propagação e infecção dos worms ocorre em várias etapas: identificação dos computadores alvos, envio das cópias, ativação das cópias e reinício do processo.

Primeiro, o worm identifica os computadores alvos através de varredura na rede, aguardando contato de outros computadores, utilizando listas predefinidas ou informações contidas no computador infectado. Em seguida, ele envia cópias de si mesmo para esses alvos explorando vulnerabilidades, anexando-se a e-mails, via canais de IRC, programas de mensagens instantâneas ou pastas compartilhadas.

Para que a infecção ocorra, o worm precisa ser executado, o que pode acontecer imediatamente após a transmissão, diretamente pelo usuário ou através de uma ação específica do usuário, como a inserção de uma mídia removível. Após a infecção do alvo, o processo de propagação e infecção recomeça, com o

computador infectado tornando-se um novo originador dos ataques.

4.3 *Bot e botnet*

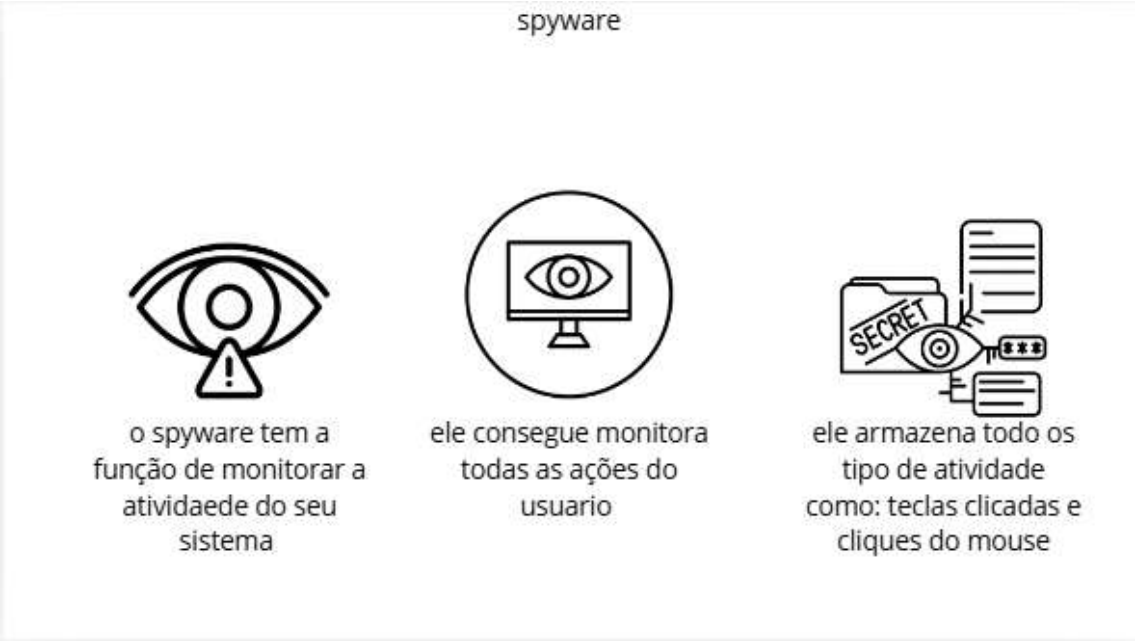


Um bot é um programa que pode ser controlado remotamente por um invasor, utilizando mecanismos de comunicação como canais de IRC, servidores web e redes P2P. Ele possui um processo de infecção e propagação similar ao de um worm, explorando vulnerabilidades em programas instalados nos computadores. Um computador infectado por um bot é chamado de zumbi, pois pode ser controlado sem o conhecimento do seu dono, e pode ser usado para enviar spam, realizar ataques e furtar dados.

Uma botnet é uma rede de computadores zumbis que permite potencializar as ações dos bots. Quanto mais zumbis na botnet, mais potente ela é. O controlador da botnet pode usá-la para seus próprios ataques ou alugá-la para outros. As ações maliciosas comuns realizadas por botnets incluem ataques de negação de serviço, propagação de códigos maliciosos, coleta de informações, envio de spam e camuflagem da identidade do atacante.

O funcionamento básico de uma botnet envolve a propagação de bots para infectar computadores, que então ficam à disposição do controlador. Quando o controlador deseja realizar uma ação, ele envia comandos aos zumbis, que executam as instruções e depois aguardam novos comandos.

4.4 *Spyware*

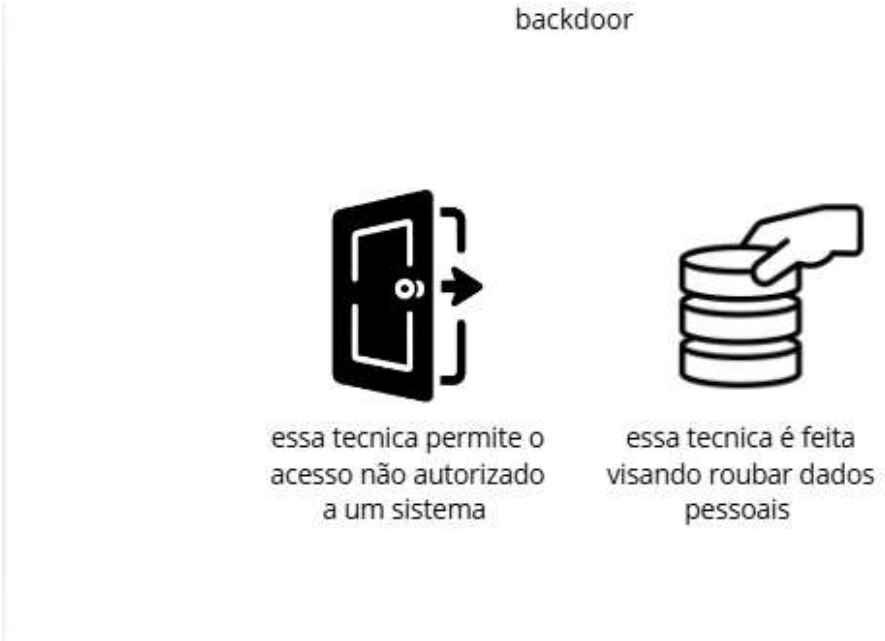


Spyware é um programa projetado para monitorar as atividades de um sistema e enviar as informações coletadas para terceiros. Seu uso pode ser legítimo ou malicioso, dependendo de como é instalado, das ações realizadas, do tipo de informação monitorada e do uso que é feito das informações coletadas.

Quando usado de forma legítima, o spyware é instalado pelo próprio dono do computador ou com seu consentimento, com o objetivo de verificar se outras pessoas estão utilizando o sistema de modo abusivo ou não autorizado. No entanto, quando usado de forma maliciosa, o spyware pode comprometer a privacidade do usuário e a segurança do computador, monitorando e capturando informações como navegação na web, contas de usuário e senhas.

Existem tipos específicos de spyware, como keyloggers, que capturam e armazenam as teclas digitadas pelo usuário; screenloggers, que armazenam a posição do cursor e a tela apresentada no monitor; e adware, que apresenta propagandas e pode ser usado para fins legítimos ou maliciosos. Keyloggers são frequentemente ativados por ações específicas do usuário, como acessar sites de comércio eletrônico ou internet banking. Screenloggers são usados para capturar teclas digitadas em teclados virtuais, enquanto adware pode apresentar propagandas direcionadas de acordo com a navegação do usuário, muitas vezes sem seu conhecimento.

4.5 *backdoor*



Um backdoor é um programa que permite a um invasor retornar a um computador comprometido, criando ou modificando serviços para esse fim. Ele pode ser incluído por outros códigos maliciosos que já infectaram o computador ou por atacantes que exploram vulnerabilidades nos programas instalados. Uma vez instalado, o backdoor assegura o acesso futuro ao computador, permitindo que ele seja acessado remotamente sem a necessidade de repetir os métodos de invasão ou infecção, geralmente sem ser notado.

A inclusão de um backdoor geralmente envolve a disponibilização de um novo serviço ou a substituição de um serviço existente por uma versão alterada com recursos de acesso remoto. Programas de administração remota, como BackOrifice, NetBus, SubSeven, VNC e Radmin, se mal configurados ou usados sem consentimento, também podem ser classificados como backdoors.

Há casos em que fabricantes de programas incluem backdoors propositalmente para necessidades administrativas, o que representa uma séria ameaça à segurança do computador, comprometendo a privacidade do usuário e podendo ser usados por invasores para acesso remoto.

4.6 Cavalo de troia (*Trojan*)

Um cavalo de troia, ou trojan, é um programa que, além de executar as funções para as quais foi aparentemente projetado, também realiza outras ações maliciosas sem o conhecimento do usuário. Exemplos de trojans incluem programas que parecem ser cartões virtuais, álbuns de fotos, jogos ou protetores de tela, mas que, ao serem executados, instalam códigos maliciosos no computador. Trojans também podem ser instalados por atacantes que alteram programas existentes para que executem ações maliciosas além de suas funções originais.

Existem diferentes tipos de trojans, classificados de acordo com as ações maliciosas que executam. Alguns exemplos são:

- **Trojan Downloader**: Instala outros códigos maliciosos obtidos da Internet.
- **Trojan Dropper**: Instala outros códigos maliciosos embutidos no próprio código do trojan.
- **Trojan Backdoor:** Inclui backdoors, permitindo o acesso remoto do atacante ao computador.
- **Trojan DoS**: Instala ferramentas de negação de serviço para realizar ataques.
- **Trojan Destrutivo**: Altera ou apaga arquivos e diretórios, podendo deixar o computador fora de operação.
- **Trojan Clicker:** Redireciona a navegação do usuário para sites específicos, aumentando acessos ou apresentando propagandas.

- **Trojan Proxy**: Instala um servidor de proxy, permitindo navegação anônima e envio de spam.

- **Trojan Spy:** Instala programas spyware para coletar informações sensíveis, como senhas e números de cartão de crédito.

- **Trojan Banker:** Coleta dados bancários do usuário, ativando-se quando sites de Internet Banking são acessados.

4.7 Rootkit

Um rootkit é um conjunto de programas e técnicas que permite esconder e assegurar a presença de um invasor ou de outro código malicioso em um computador comprometido. Esses programas podem remover evidências em arquivos de logs, instalar outros códigos maliciosos como backdoors, esconder atividades e informações, mapear vulnerabilidades em outros computadores e capturar informações da rede onde o computador comprometido está localizado.

O termo rootkit vem da junção das palavras “root” (conta de superusuário ou administrador em sistemas Unix) e “kit” (conjunto de programas usados para manter os privilégios de acesso dessa conta). É importante notar que rootkits não são usados para obter acesso privilegiado, mas para mantê-lo.

Inicialmente, rootkits eram usados por atacantes para manter o acesso privilegiado após invadir um computador e esconder suas atividades. Hoje, eles também são incorporados por outros códigos maliciosos para ficarem ocultos e não serem detectados. Há casos de rootkits instalados propositalmente por empresas de CDs de música para proteger direitos autorais, mas isso compromete a segurança do computador, pois podem ser usados por invasores para esconder sua presença e arquivos maliciosos.

4.8 Prevenção

Para manter seu computador protegido contra códigos maliciosos, é essencial adotar algumas medidas preventivas. Manter os programas atualizados com as versões mais recentes e aplicar todas as atualizações disponíveis é fundamental. Além disso, utilizar mecanismos de segurança como antimalware e firewall pessoal ajuda a proteger seu sistema.

É importante também tomar cuidados ao manipular arquivos, pois novos códigos maliciosos podem surgir rapidamente, muitas vezes mais rápido do que a capacidade dos mecanismos de segurança de se atualizarem. Informações detalhadas sobre os principais mecanismos de segurança e outros cuidados necessários para manter seu computador seguro podem ser encontradas nos capítulos específicos sobre Mecanismos de Segurança e Segurança de Computadores.

6. Outros Riscos

Com o aumento na quantidade de serviços *web* disponíveis hoje, o número de usuários que utilizam estes serviços aumentou, uso de *softwares* como navegadores, *Gmail*, entre outros.

Para conseguir atender este público, diversos serviços e funções foram adicionadas para melhorar experiência. Entretanto, estes serviços ainda têm vulnerabilidades e muitos criminoso exploram para invadir e roubar informações, como senhas de contas bancárias e outras.

Nos tópicos abaixo, haverá explicações de como esses ataques ocorrem e cuidados que os usuários devem tomar enquanto navegam pela *internet*, pois as redes tornaram mais fácil a comunicação e o envio de informações entre pessoas, entretanto, também facilitou para que mal-intencionados possam cometer delitos no meio digital.

6.1 *Cookies*

Cookies são pequenos arquivos que são gravados no computador quando você realiza algo no site, seja clicar em uma sessão ou em um anúncio. Estes arquivos são reenviados aos donos do site e com isso eles podem descobrir coisas como produtos que pesquisamos, nosso carrinho, nossa lista de desejos.

Estes *cookies* podem ser temporários, que são apagados automaticamente que o navegador é fechado, ou podem ser permanentes, que ficam gravados na máquina até expirar ou serem apagados. Também podem ser primários(*first-party*), os quais são reenviados para o domínio do site ou terceiros(*third-party*), os quais vão para outros domínios (são mais relacionados aos anúncios).

Perigos relacionados a *cookies* são:

Compartilhamento de informações: As informações que são coletadas podem ser enviadas a terceiros, e isto pode impactar na privacidade do usuário. Um exemplo, quando você entre e um *site* que não foi acessado antes, mas ao abri-lo, ele recomenda produtos que foram pesquisados em outros *sites*.

Informações pessoais: Formulários também podem gravar dados em *cookies*, isso permite que *crackers* podem acessar as informações caso não tenha uma criptografia adequada.

Vulnerabilidades: Quando utilizamos um navegador, ele disponibiliza algumas informações sobre o nosso computador, como *softwares* instalados ou *hardware* que utilizamos. Os *cookies* têm acesso à essas informações, deixando uma brecha na segurança para um possível ataque.

Autentificação: Em alguns *sites*, podemos deixar senhas e contas salvas para que possamos acessar elas com facilidade na próxima vez. Entretanto, estes dados são salvos em *cookies*, que caso sejam acessados por terceiros, podem *logar* em sua conta se passando por você.

Hábitos de navegação: Com base em cookies de terceiros, as empresas podem descobrir os hábitos de navegação do usuário, comprometendo a privacidade.

Prevenção: Bloquear os serviços que são fornecidos por *cookies* não é recomendado, pois isto pode causar um mal funcionamento do site. Entretanto, é possível bloquear alguns serviços.

Usar navegadores com níveis de acesso médio, para que não coletem tantas informações do seu computador.

Não deixar que os *cookies* sejam definidos automaticamente, sempre definindo quais será o tipo de acesso.

Configurar para que os *cookies* sejam apagados toda vez que navegador fechar. (como usar a guia anônima)

Não permitir que seus dados sejam enviados à terceiros.

Navegar anonimamente caso utilize computadores de outros locais (como LAN House).

6.2 Código Móveis

6.2 Códigos movéis

Os códigos móveis são muito utilizados para fazer sites, eles podem apresentar diversas vulnerabilidades se caso for mal implementado. Abaixo, alguns dos riscos que podem ser causados por código móvel:

Programas em *Java*: Normalmente, estes programas já possuem alguma forma de segurança, entretanto, ainda possuem vulnerabilidades, o que pode pode fazer que um programa *Java* malicioso seja executado.

JavaScript: Apesar de ser usado muito na *web*, um código de *Javascript* ainda pode ser usado para prejudicar outras máquinas. Ele é muito usado para a criação de sites falsos, tornando-o bastante perigoso.

Componente *activeX:* O *activeX* é um pequeno grupo de programas que nos permite instalar coisas da *internet.* entretanto, ele possui acesso ao *hardware* e *software* de todo computador, e não possui nenhum recurso de segurança para impedir a instalação de algo malicioso.

Prevenção:

Bloquear todos os códigos móveis vai resultar em mal funcionamento de *sites*, portanto, o que deve ser feito é:

Permitir a execução de Java e JavaScript, mas utilizar algum outro complemento que libere gradualmente o que será executado.

Permitir que o *ActiveX* instale e execute arquivos somente se vierem de sites confiáveis.

Tomar cuidado com o que for instalar na *internet*.

6.3 Janelas pop-up

As janelas de pop-up são automáticas e são presente muitas vezes em *sites não confiáveis.* Geralemte apresentam conteúdos impróprios ou anúncios. Apresenta diversas falhas, pois podem redirecionar para outro *site* ou instalar algum arquivo.

Prevenção:

Configurar o navegador para bloquear pop-up por padrão

Deixar um lista de sites confiáveis se for necessário.

6.4 *plug-ins,* complementos e extensões

São programas que podem ser instalados em navegador e outros para adicionar novas funcionalidades. Muitos desses programas são disponibilizados em repósitoios, que podem ou não realizar uma avaliação antes de de deixá-los no repostório. Apesar de possuir muitos fornecedores confiáveis, não podemos nos descuidar.

Prevenção:

Tenha programas de segurança (como um ant-vírus) instalado antes de baixar algo de terceiros.

Atualizar todos os *softwares* regularmente.

Verificar se o fornecedor é confiável.

Sempre dê uma olhada nas avaliações dos usuários.

Verificar as permissões que são requisitadas para realizar a instalação.

6.5 *links* com patrocínio

São anúncios que são pagos para que possam ser exibidos no *site,* geralmente, eles aparecem quando um usuário busca algo e o *site* redireciona para um *link* relacionado a pesquisa. Como o anunciante pode realizar algumas funções no site, como transferência de dinheiro, atacantes buscam brechas para redirecionar para um link falso, e roubar dados.

Prevenção

Não use *sites* de buscas desconhecido para realizar pesquisas de informações que você já saiba.

6.6 Banners de anúncio

Eles funcionam como um *outdoor,* é alugado um espaço no *site* que será exibido o anúncio proposto. E quanto mais cliques tiver em um banner, maior será a remuneração. Entretanto, pessoas viram aqui uma oportunidade de aplicar golpes. Conhecido por *malvertising*, que é a prática de criar um anúncio falso e publicá-lo como se fosse real.

Prevenção:

Não clicar em *banners* de sites desconhecidos.

Sempre verificar se o *firewall* está ativo.

Manter atualizados programas de segurança.

6.7 programas P2P

São softwares que são responsáveis que pelo compartilhamento de pastas. Por conta disso, muitos desses programas podem acessar diversos arquivos dentro do computador, e muitos não tem medida de verificação de arquivos maliciosos, o que pode causar problemas.

Prevenção:

sempre manter estes softwares atualizados e com configurações que não permitam acesso total ao computador.

Ter um antmalware instalado e atualizado constantemente.

Verificar os arquivos compartilhados.

6.8 Compartilhamento de recursos computacionais

O compartilhamento de recursos é permitir que outros usuários possam ter acesso a arquivos na máquina. Apesar de útil, isso deixa uma vulnerabilidade, pois este usuário pode acessar informações confidenciais e outros.

Prevenção

Não permitir que qualquer usuário possa alterar coisas.

Criar senhas para acessar ou compartilhar arquivos

Monitoramento dos *logs* dos usuários

7 - Título 1 - Mecanismos de defesa: Os mecanismos de segurança são ferramentas e práticas que ajudam a proteger os dados e a privacidade dos usuários na internet, sendo usado a favor da empresa. As políticas de segurança definem claramente as regras e responsabilidades dos funcionários e administradores, garantindo o uso seguro e eficiente dos recursos computacionais.

1

Os mecanismos de segurança incluem ferramentas essenciais como programas **antimalware**, que detectam e removem softwares maliciosos, **firewalls** que monitoram e controlam o tráfego de rede para prevenir acessos não autorizados e **filtros antispam**, que bloqueiam e-mails indesejados e potencialmente perigosos. Essas ferramentas são fundamentais para proteger os dados e a privacidade dos usuários. Além das ferramentas de defesa, o **monitoramento contínuo das**

atividades de rede é crucial. Isso permite identificar e responder rapidamente a atividades suspeitas, garantindo que as ameaças sejam neutralizadas antes de causar danos significativos na empresa.

2

As políticas de segurança definem claramente as regras e responsabilidades dos funcionários e administradores. Isso inclui diretrizes sobre o **uso seguro dos recursos computacionais**, garantindo que **todos saibam como proteger os dados da empresa**. Políticas específicas, como a de senhas, estabelecem regras sobre o **uso de senhas fortes e a periodicidade de troca**. A política de backup define **como as cópias de segurança devem ser realizadas**, incluindo o **tipo de mídia utilizada**, **período de retenção** e **frequência de execução**, assegurando que os dados possam ser recuperados em caso de perda.

3

A autorização determina as ações que cada entidade da empresa pode executar. O controle de acesso gerencia **quem pode acessar quais recursos**, garantindo que **apenas usuários autorizados tenham acesso a informações críticas**. A autenticação é crucial para a segurança, garantindo que apenas pessoas autorizadas tenham acesso a informações sensíveis. Isso pode ser feito por meio de **senhas fortes**, **tokens de segurança** ou **biometria**, como **impressões digitais** e **reconhecimento facial**. Implementar autenticação multifator adiciona uma camada extra de proteção, tornando difícil para invasores obterem acesso não autorizado aos sistemas da empresa.

A integridade dos dados **é protegida contra alterações não autorizadas, garantindo que as informações permaneçam precisas** e **confiáveis**. Isso é feito através de controles rigorosos e criptografia. A confidencialidade assegura que informações sensíveis sejam acessadas **apenas por pessoas autorizadas**. Utilizar criptografia para **codificar dados e realizar auditorias regulares** ajuda a manter a **confidencialidade** e a **segurança das informações**.

Título 2 - Utensílios - A definição clara de regras e responsabilidades, aliada a um plano bem elaborado da resposta a incidentes, assegura que a empresa esteja preparada para enfrentar e mitigar qualquer violação de segurança. Ao manter-se em conformidade com as regulamentações e investir na educação dos colaboradores, não só protege seus ativos digitais, mas também fortalece a confiança de seus clientes e parceiros, garantindo um ambiente seguro e eficiente para todos.

8.1 senhas e contas

Para utilizar computadores, antes, precisamos criar contas e senhas para poder acessa-los com mais segurança e tranquilidade. Para isso, devemos considerar:

Criar uma senha forte, com caracteres e muitos dígitos

Não colocar nada pessoal na senha.

Trocar de senha regularmente.

Se não tomar cuidado, sua senha pode ser descoberta das formas abaixo:

Se logar em um computador infectado sua senha pode ser roubada

Digitar a senha em um site falso

Pelo cliques no teclado.

8.2 elaborar senhas seguras

A elaboração de senhas fortes é fundamental para poder utilizar os computadores, pois só isso já diminui os riscos de uma possível invasão ou roubo de conta. Para fazer uma senha forte, é necessário:

Evitar uso de informações pessoais, como nome do gato, próprio nome, etc

Evitar sequencias de teclado ou numéricas.

Evitar palavras que estejam públicas, como nomes de música, séries e outros.

Usar palavras grandes

Usar caracteres especiais.

Números de forma aleatória

Letras de forma aleatória.

8.3 alterações de senha

Caso tenha a dúvida ou algum motivo para acreditar que descobriram sua senha, ela deve ser alterada imediatamente. Algumas situações são:

Usou uma máquina que pode estar infectada

Acessou um link em um site suspeito

Utiliza a mesma senha em contas indiferentes

Mesmo fora destes casos, é sempre recomendado trocar as senha de tempo em tempo.

8.4 gerenciamento de senhas

Geralmente, é muito comum usuários que querem facilitar a vida e deixá-la mais fácil usar ferramentas como me lembre para salvar suas senhas. Alguns até repetem a mesma senha em outras contas para facilitar, entretanto, isso também abre brechas para que possam invadir nossa conta. Portanto:

Não reutilize senhas em outras contas

Evitar usar “continuar conectado", usar somente em sites confiáveis.

Para evitar percas, sempre anote as senhas no papel.

8.5 recuperação de senhas

Mesmo que tenha muito cuidado ou que tenha uma boa memória, não é incomum a perca de senhas, por isso, há soluções para este tipo de problema como está listado abaixo:

Permitir que tenha uma pergunta para você se perder a senha

Ter um e-mail de recuperação de conta

Confirmar informações de cadastro, como número de celular.

Enviar um código via SMS.

9.1 criptografia

Criptografia é de forma simplificada, codificar mensagens de maneira que só quem enviou e quem recebeu saiba o que está escrito nela. É bastante utilizado no mundo digital. Com a criptografia é possível proteger seus dados, sejam comuns ou backups.

9.2 Criptografia de chaves

Umas das técnicas de criptografia é a chave simétrica e assimétrica.

Criptografia de chave simétrica: Para codificar e decodificar a mensagem, é preciso somente uma chave, que pode ser um único usuário que saiba qual é, mas também é possível mais de um saber.

Criptografia de chave assimétrica: Neste caso, há duas chaves, uma pública e uma privada. A pública qualquer um pode saber, já a privada é restrita ao dono e não pode ser revelada, pois é ela que vai decodificar a mensagem.

A chave mais recomendada é a chave simétrica, já que possui uma maior confidencialidade.

9.3 Função de resumo

A função de resumo ou hash, é utilizado para verificar a integridade de um arquivo, pois independente do tamanho do arquivo, o valor gerado pelo hash é fixo. Ele é usado para:

Verificar a integridade de arquivos

Verificar se houve alteração

9.4 Assinatura digital

É um comprovante de que quem alterou e entregou o documento realmente é o dono. É feito através da chave pública, pois para decodificar o documento é necessário da chave privada, a qual somente o dono possui.

9.5 certificados digital

O certificado digital é usado como comprovante sobre o dono da chave privada, pois a chave pública pode estar nas mãos de cada um, mas se caso outra pessoa tiver a chave privada, ela pode se passar por um impostor e receber a mensagem, por isso, um certificado que deixa claro o dono da chave deve ser feito.

9.6 Programas de criptografia

Para garantir que tenha um ambiente seguro e que seus dados não sejam roubados ou tenham a integridade ferida, é necessário utilizar softwares de criptografia,. Alguns já vem instalados, pois fazem parte do sistema operacional.

9.7 Cuidados para tomar

Sempre usar criptografia para enviar mensagens

Usar criptografia nas conexões do seu e-mail com o provedor

Apenas envie dados importantes caso tenha certeza de que é a pessoas certa a receber

Usar o hash em arquivos para garantir integridade

11. Privacidade

Para navegar na internet, é necessário que o usuário possua sua privacidade, coisa que mudou com a criação da internet. Um meio onde a privacidade é ameaçada o tempo todo. Portanto, devemos sempre ficar alerta com isso

11.1 redes sociais

As redes sociais permitem que hoje, vejamos o que ocorre do outro lado do mundo, ver o que nossos amigos entretanto, apesar da comunicação ser mais fácil, as redes ainda são um perigosas, pois pode ocorrer:

Furto de identidade

Roube de perfil

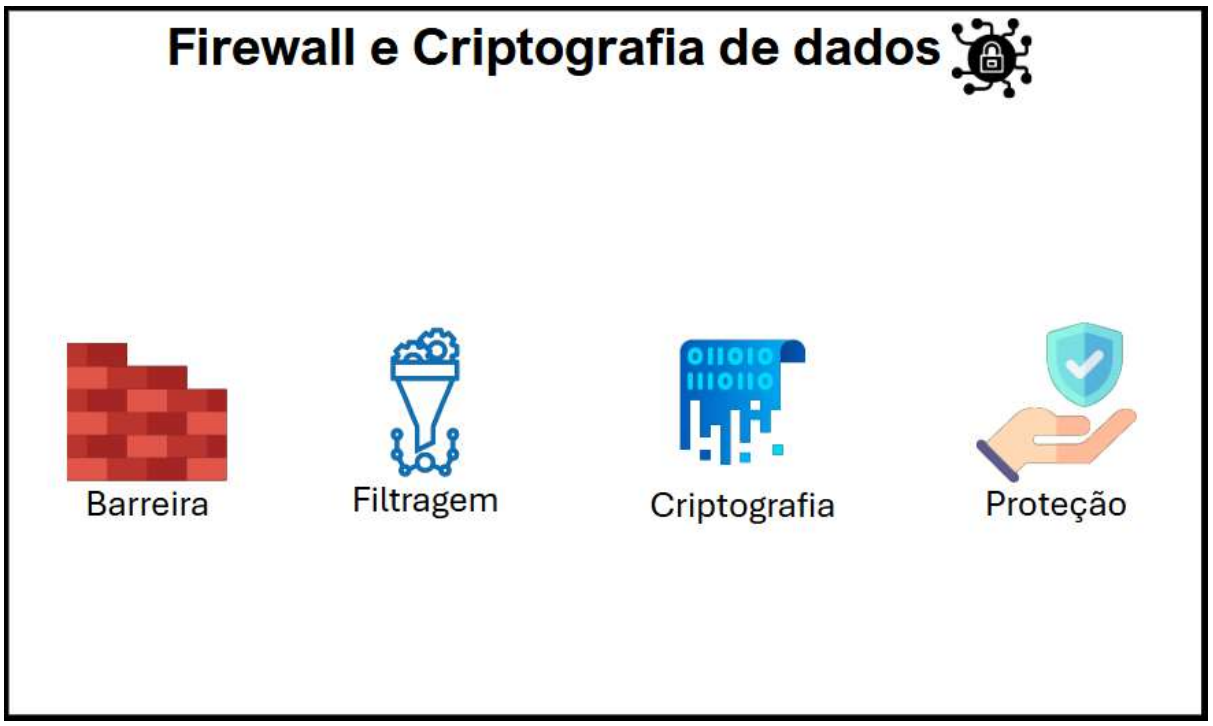
Dano a imagem

Invasão de privacidade

Sequestro

Portanto, para evitar este tipo de situação, devemos sempre manter monitoramento e não clicar em links desconhecidos por ai.

13 - Título 1 - Segurança de Redes: A segurança de redes é essencial para proteger as operações e os dados da empresa contra ameaças digitais. Adotar ferramentas como firewalls para monitorar o tráfego e evitar acessos indesejados, e usa criptografia para proteger as informações durante a transmissão, impedindo que dados confidenciais sejam interceptados.

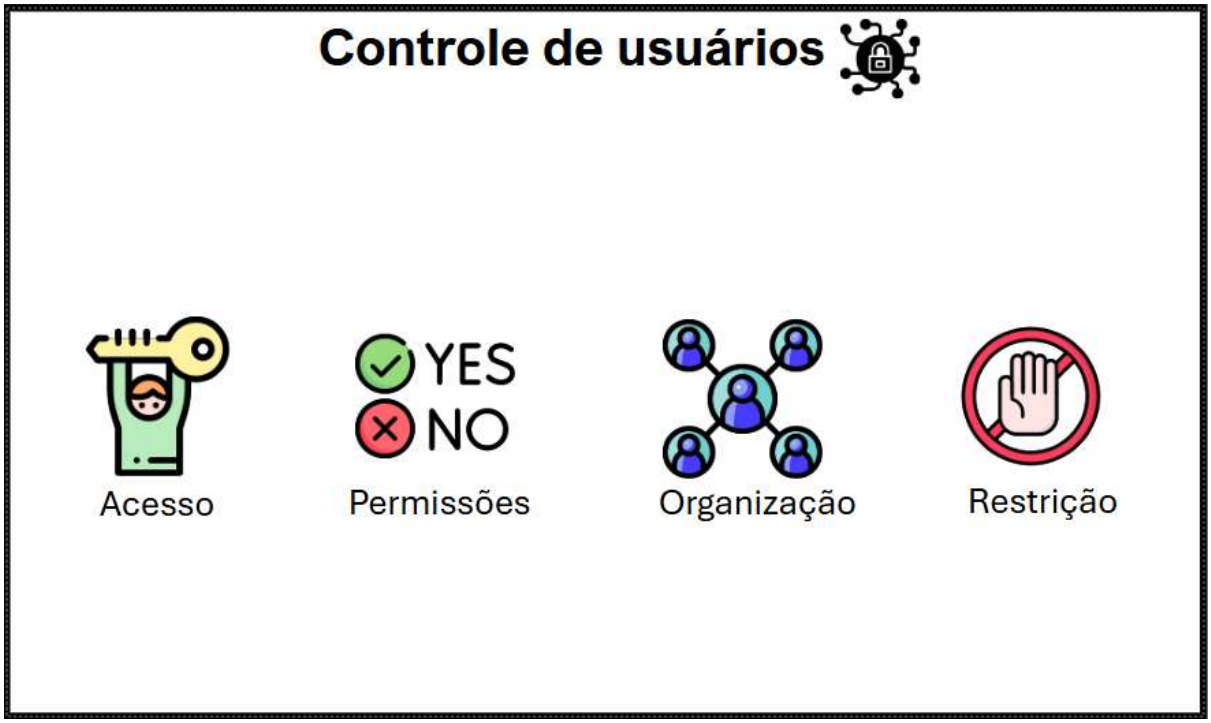


Utilizar **firewalls** como barreira essencial contra acessos indesejados, **monitorando o tráfego de rede** para impedir que invasores acessem dados sensíveis. Essa ferramenta permite que a empresa **filtre** e **controle as conexões**, garantindo que apenas o tráfego autorizado alcance seus servidores e dispositivos.

2

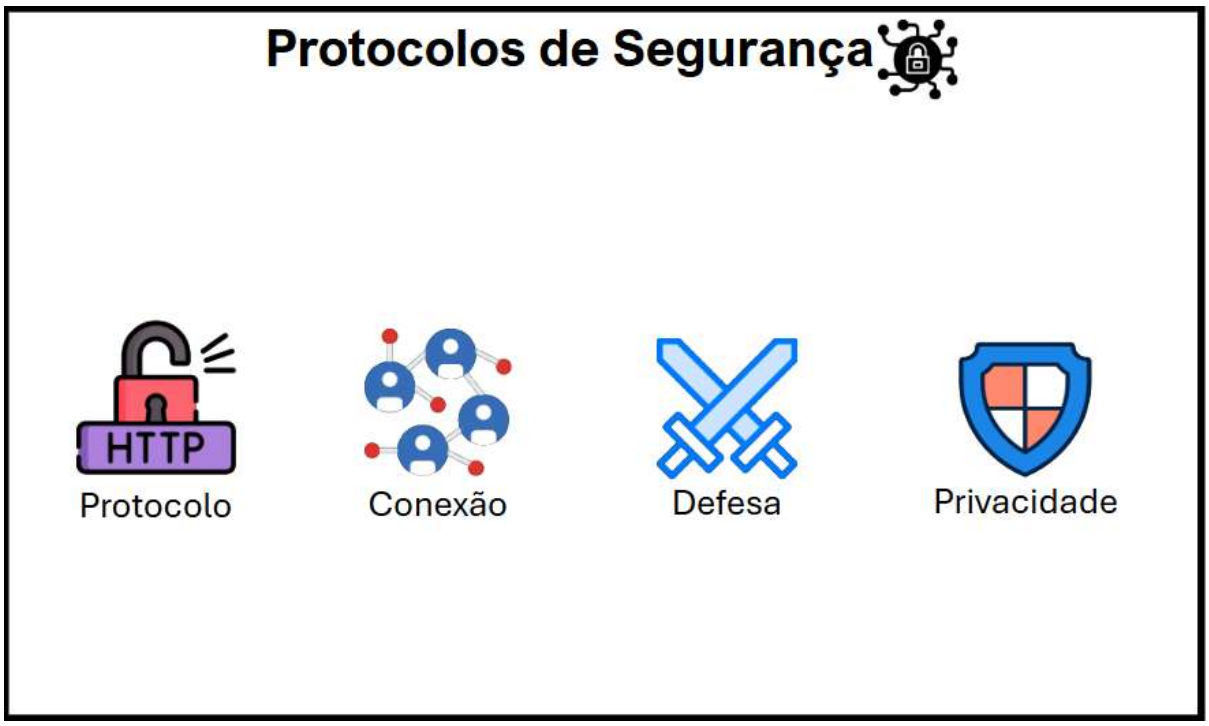
A segurança na transferência de dados é fundamental para a proteção das informações corporativas. A empresa utiliza **protocolos** que garantem a integridade e a confidencialidade dos dados durante o tráfego. Além disso, são implementadas **técnicas de monitoramento** para detectar e prevenir tentativas de interceptação. Essas práticas ajudam a **evitar vazamentos** e asseguram que informações sensíveis permaneçam protegidas, fortalecendo assim a confiança dos clientes nas operações da empresa.

3



Adote políticas rigorosas de acesso restrito, garantindo que apenas funcionários autorizados possam acessar informações e sistemas críticos. Com **autenticações multifatoriais** e **senhas fortes**, a empresa protege **dados sensíveis** contra acessos não autorizados. Além disso, o monitoramento contínuo das atividades dos usuários permite identificar comportamentos suspeitos rapidamente.

4



Os protocolos de segurança são fundamentais para proteger as informações que transitam pela rede da empresa. Eles garantem a **integridade** e a **confidencialidade dos dados**, utilizando técnicas de **criptografia** e **autenticação**. Entre os principais protocolos implementados estão o HTTPS, que assegura a comunicação segura na web, e o TLS, que protege as transmissões de dados em tempo real. Essas tecnologias são essenciais para prevenir ataques e garantir que apenas usuários autorizados tenham acesso às informações sensíveis. Com a adoção de protocolos de segurança eficazes, a TRES LISS reforça a proteção de seus sistemas e a confiança de seus clientes.

Título 2 - Segurança: Em suma, implementar restrições de acesso para assegurar que apenas funcionários autorizados possam visualizar ou modificar informações sensíveis. Além disso, utilizar protocolos avançados de Wi-Fi para proteger o ambiente virtual, garantindo a segurança da rede, mesmo durante acessos remotos. Essas medidas são essenciais para prevenir invasões e roubos de dados, garantindo a continuidade dos serviços, ao mesmo tempo em que preservam a confiança dos clientes e a integridade dos sistemas empresariais.

14 - Título 1 - Segurança em Dispositivos Móveis: A segurança em dispositivos móveis é inevitável devido ao uso crescente de smartphones e tablets. As principais ameaças incluem malware, roubo de dispositivos e acesso não autorizado a dados. O malware pode roubar informações pessoais, enquanto o furto de dispositivos

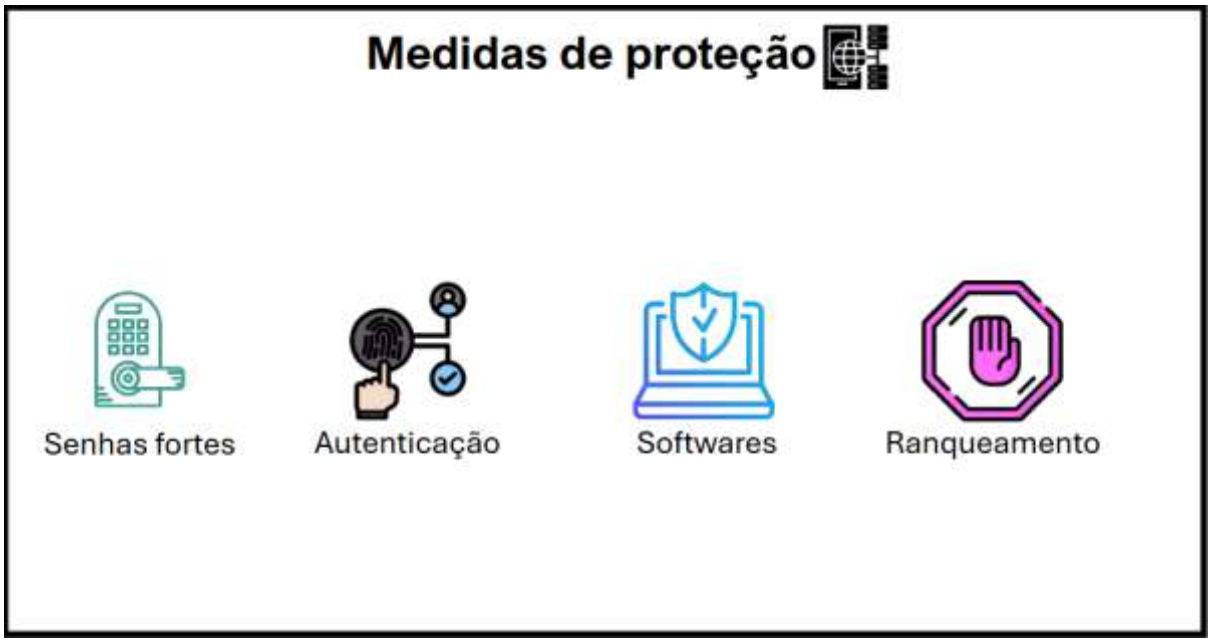
resulta na perda de dados sensíveis. A resiliência dos dispositivos é a capacidade de se recuperar rapidamente de ataques, garantindo a proteção dos dados.

1

Os dispositivos móveis enfrentam várias vulnerabilidades que podem comprometer a segurança dos dados dos usuários. As principais incluem malware, roubo de dispositivos, acesso não autorizado e exposição de dados pessoais. O **malware** pode ser instalado por meio de aplicativos maliciosos, roubando informações sensíveis. O **roubo** pode resultar na perda de dados importantes. O **acesso não autorizado** acontece quando as configurações de segurança não são adequadas,

permitindo que terceiros acessem informações. E a **exposição de dados pessoais** ocorre quando informações são coletadas e exploradas por cibercriminosos.

2



Para garantir a segurança dos dispositivos móveis da empresa, é essencial adotar medidas eficazes. Primeiramente, os colaboradores devem fazer uso de senhas fortes, **dificultando o acesso não autorizado. Implementar a dupla verificação** é outra prática importante, pois adiciona uma camada extra de proteção ao acessar contas corporativas. A instalação de **softwares de proteção**, como antivírus e firewalls, também é crucial para proteger os dispositivos contra malware e ameaças cibernéticas.

3

Manter o sistema operacional e os aplicativos atualizados é essencial para corrigir vulnerabilidades. Use **senhas fortes** e **ative a autenticação em duas etapas** para reforçar a segurança. Aplicativos de segurança, como **antivírus** e **ferramentas de localização**, ajudam a proteger os dados em caso de perda ou roubo. Práticas de segurança consistentes aumentam a confiabilidade dos dispositivos móveis.

4

A **recuperação** é fundamental para a proteção dos dispositivos móveis. Manter **backups** regulares é crucial para garantir que dados importantes não sejam perdidos durante falhas ou ataques, facilitando a **recuperação** rápida das informações. É importante ter um plano de **resposta a incidentes** para agir de maneira eficaz em situações imprevistas, minimizando potenciais danos. A **segurança** dos dados deve ser uma prioridade, utilizando técnicas como **backup**, **criptografia** e **autenticação** para proteger informações sensíveis. Essas práticas ajudam a garantir a integridade dos dados e permitem que a organização se recupere rapidamente de desafios.

Título 2 - Conclusão: Sabemos que a segurança em dispositivos móveis é necessária no mundo de hoje. Tomando medidas como a utilização de senhas fortes, a implementação de autenticação em duas etapas e a manutenção de aplicativos atualizados, as empresas podem proteger informações sensíveis. Realizar backups regulares e ter um plano de resposta a incidentes são práticas essenciais para garantir a rápida recuperação de dados. Assim, adotar essas estratégias é fundamental para mitigar riscos e assegurar a integridade dos dados em um ambiente digital cada vez mais desafiador.