CIBER GUIA

Sinta-se protegido na internet.

Tipos de Ameaças Cibernéticas: Introdução aos riscos e dicas de proteção.

Malware

São programas maliciosos como vírus, worms, cavalos de Tróia, ransomware e spyware podem ser instalados em dispositivos através de diversos meios, como links maliciosos, anexos de email contaminados ou downloads não confiáveis.

Comportamento: O malware pode roubar dados, danificar arquivos, comprometer a privacidade e até mesmo controlar o dispositivo da vítima.

Prevenção Malware

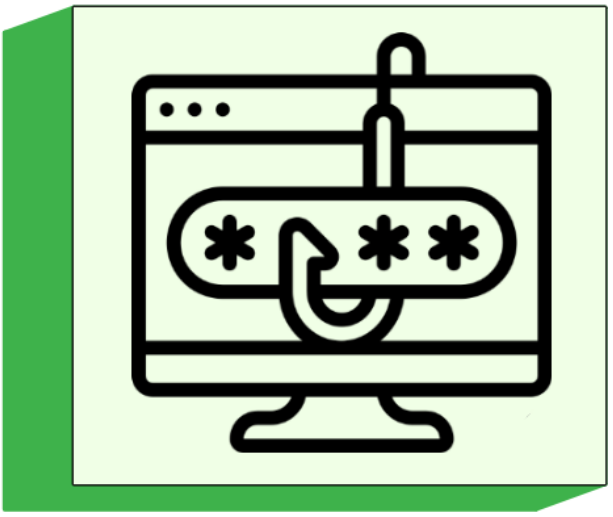
Antivírus e Antispyware: Instale e mantenha atualizado um software antivírus e anti spyware confiável em todos os seus dispositivos. confiável em todos os seus dispositivos.

Evite downloads não confiáveis: Baixe aplicativos e arquivos apenas de fontes oficiais e confiáveis.

Cuidado com links e anexos: Tenha cuidado ao clicar em links em emails ou mensagens de fontes desconhecidas. Evite abrir anexos suspeitos.

Mantenha o software atualizado: Mantenha o sistema operacional e todos os softwares instalados atualizados com as últimas correções de segurança.

Phishing



Essa técnica envolve a criação de sites falsos ou o envio de emails fraudulentos que imitam páginas legítimas, como bancos, lojas online ou redes sociais. O objetivo é induzir a vítima a fornecer informações confidenciais, como senhas, dados bancários ou números de cartão de crédito.

Comportamento: Podem se manifestar como links ou anexos maliciosos, solicitar informações pessoais ou financeiras, ou redirecionar para sites falsos.

Prevenção Phishing

Desconfie de emails e sites suspeitos: Esteja atento a e-mails com erros gramaticais ou ortográficos que podem indicar um e-mail falso, solicitações urgentes de informações confidenciais ou ofertas que parecem boas demais para ser verdade.

Verifique o remetente: Verifique o endereço de email do remetente antes de abrir qualquer email. Se o endereço for suspeito, não abra o email e exclua-o imediatamente.

Passe o mouse sobre links: Antes de clicar em qualquer link, passe o mouse sobre ele para ver o URL real. Se o URL parecer suspeito, não clique no link.

Utilize filtros de spam: Use filtros para bloquear e-mails de phishing conhecidos.

Engenharia Social

Essa manipulação psicológica visa explorar o comportamento humano para obter informações confidenciais ou acesso a sistemas. Através de técnicas

como persuasão, intimidação ou ofertas atraentes, os criminosos podem induzir a vítima a revelar dados sensíveis ou realizar ações que comprometam a segurança.

Comportamento: Enviam comunicações fraudulentas que parecem ser de fontes confiáveis. Fingem ser uma autoridade ou pessoa de confiança para coletar informações sensíveis.

Prevenção Engenharia Social

Esteja atento a golpes: Tenha cuidado com ofertas que parecem boas demais para ser verdade, solicitações urgentes de ajuda ou ameaças de consequências graves.

Nunca forneça informações confidenciais por telefone ou email: Bancos, empresas e órgãos governamentais nunca solicitarão senhas, dados bancários ou outras informações confidenciais por telefone ou email.

Verifique a fonte: Antes de fornecer qualquer informação pessoal, verifique a fonte da solicitação. Ligue para a empresa ou órgão em questão para confirmar a autenticidade da solicitação.

Instale um firewall: Um firewall pode ajudar a proteger seu computador contra acessos não autorizados.

Furto de Celular

Além do risco de perda de dados pessoais, o celular roubado pode ser utilizado para realizar compras online, acessar contas bancárias ou enviar mensagens fraudulentas em nome da vítima.

Comportamento: Roubam contatos, fotos, mensagens, e outras informações sensíveis para fins maliciosos. Abrem contas fraudulentas, realizam transações financeiras ou se comunicam com contatos fingindo ser o proprietário.

Prevenção Furto de Celular

Senha forte e bloqueio de tela: Utilize uma senha forte exclusiva para bloquear a tela do seu celular e configure o bloqueio automático após um período de inatividade.

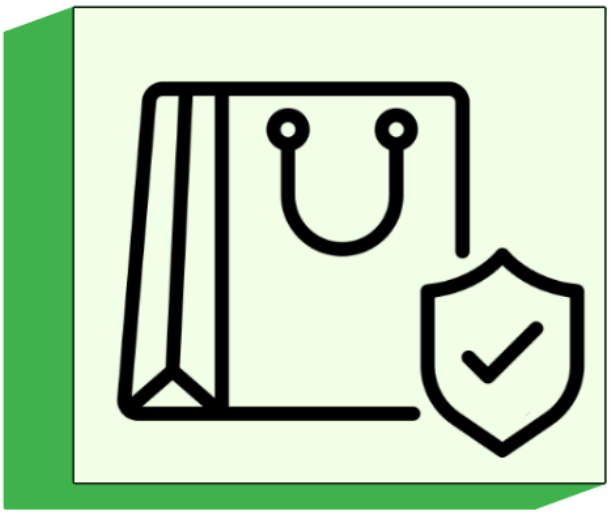
Localização e rastreamento: Ative os recursos de localização e rastreamento do seu celular para que você possa localizá-lo em caso de perda ou roubo.

Aplicativo antirroubo: Instale um aplicativo antirroubo que permita bloquear o celular remotamente, apagar dados e tirar fotos do ladrão.

Backup de dados: Faça backups regulares dos seus dados no seu computador ou na nuvem para evitar a perda de informações importantes.

Evite expor seu celular em locais públicos: Mantenha seu dispositivo guardado em locais seguros, especialmente em áreas movimentadas.

Comércio via Internet



Sites falsos, anúncios enganosos e golpes de venda online são algumas das ameaças presentes no comércio eletrônico. É importante pesquisar a reputação da loja

antes de realizar qualquer compra online e utilizar apenas meios de pagamento seguros.

Comportamento: Enviam e-mails ou mensagens falsas que parecem ser de lojas legítimas, pedindo dados de login ou informações de cartão de crédito. Roubam informações confidenciais transmitidas durante a compra, como dados de pagamento e endereços.

Prevenção Comércio Via Internet

Compre em sites confiáveis: Verifique a reputação do site antes de fazer uma compra. Prefira sites conhecidos e com boas avaliações.

Evite salvar dados do cartão em sites: Evite salvar os dados do seu cartão de crédito em sites de lojas online, mesmo que sejam confiáveis. Essa prática facilita o acesso indevido aos dados do cartão caso o site seja hackeado.

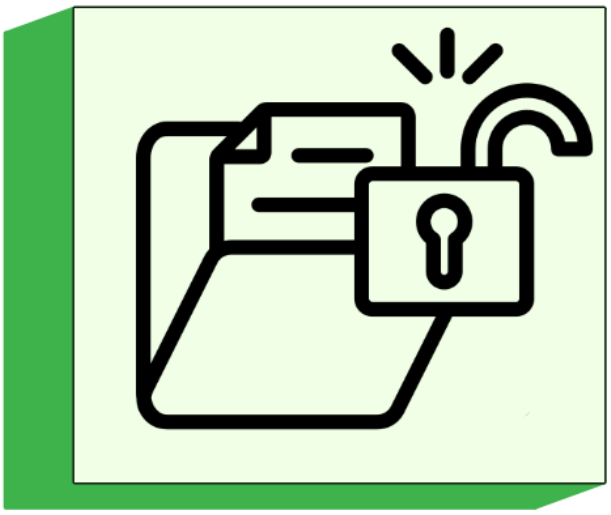
Use métodos de pagamento seguros: Utilize cartões de crédito virtuais ou serviços de pagamento seguros como PayPal, Mercado Pago, PagSeguro, Stone.

Verifique a segurança do site: Certifique-se de que o site utiliza HTTPS (cadeado na barra de endereço) para proteger suas informações.

Monitore suas transações: Verifique regularmente o extrato do seu cartão de crédito e relatórios bancários para detectar transações suspeitas.

Evite redes públicas ao fazer compras: Prefira redes privadas e seguras para realizar transações financeiras.

Vazamento de dados



Empresas e órgãos públicos podem sofrer ataques cibernéticos que resultam no vazamento de dados confidenciais de seus clientes ou usuários. Isso pode levar à perda de identidade, fraude financeira e outros danos.

Comportamento: Enviam e-mails ou mensagens fraudulentas que parecem ser de fontes confiáveis, levando as vítimas a fornecerem suas credenciais. Utilizam técnicas como força bruta, exploração de vulnerabilidades e engenharia social para acessar informações sensíveis. Dados podem ser vazados por negligência ou pela venda de informações.

Prevenção Vazamento de dados

Use senhas fortes e únicas: Utilize senhas complexas e diferentes para cada conta, e considere usar um gerenciador de senhas.

Habilite a autenticação de dois fatores (2FA): Adicione uma camada extra de segurança às suas contas online. A 2FA proporciona um gerenciamento de segurança mais robusto, exigindo duas formas de verificação para acessar uma conta ou realizar transações. Isso ajuda a proteger sua identidade e informações pessoais contra acessos não autorizados.

Seja cauteloso ao compartilhar informações: Limite a quantidade de informações pessoais que você compartilha online e com empresas. Se achar necessário questione a necessidade de fornecer informações e forneça apenas o mínimo necessário.

Monitore suas contas regularmente: Verifique suas contas e transações para identificar atividades suspeitas.

Acompanhe Seu Crédito e Identidade: Inscreva-se em serviços de monitoramento de crédito e identidade que alertam sobre atividades suspeitas.

Fique atento a emails e mensagens suspeitas: Tenha cuidado com emails e mensagens que solicitam seus dados pessoais ou que direcionam para sites falsos.

Redes Públicas

Redes Wi-Fi públicas não protegidas podem ser facilmente interceptadas por cibercriminosos, colocando em risco os dados trafegados pelos dispositivos conectados. É importante evitar o uso de redes públicas para realizar transações bancárias ou acessar sites confidenciais.

Comportamento: Capturam dados sensíveis como senhas, números de cartão de crédito e mensagens privadas. Enganam os usuários para se conectarem, permitindo que os hackers capturem todo o tráfego de rede.

Prevenção Redes Públicas

Evite usar redes públicas para atividades confidenciais: Não realize transações financeiras ou acesse contas importantes em redes públicas.

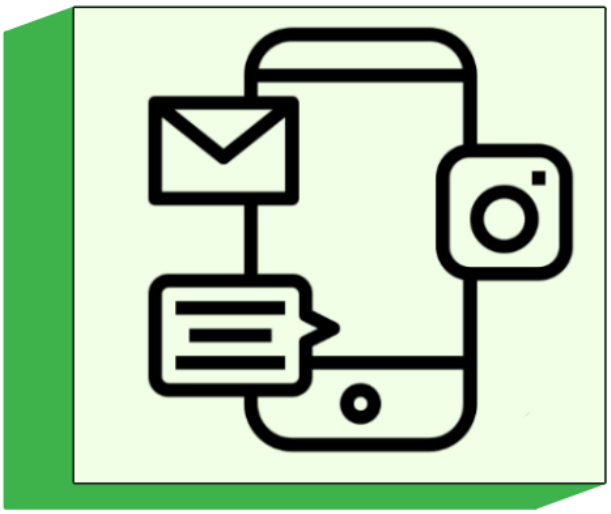
Use uma VPN: Uma Rede Virtual Privada (VPN) criptografa sua conexão, protegendo seus dados em redes públicas.

Desabilite conexões automáticas: Configure seu dispositivo para não se conectar automaticamente a redes Wi-Fi públicas.

Verifique a segurança da rede: Prefira redes públicas que requerem uma senha e que são oferecidas por fontes confiáveis.

Use HTTPS sempre que possível: Certifique-se de que os sites que você visita utilizam HTTPS para proteger sua comunicação.

Redes Sociais



As redes sociais são um terreno fértil para a disseminação de informações falsas, golpes e ataques de phishing. É importante ter cuidado com as informações que você compartilha online e configurar as configurações de privacidade para proteger seus dados.

Comportamento: Enviam mensagens ou publicações falsas que parecem ser de amigos ou empresas confiáveis, levando as vítimas a fornecerem suas credenciais ou informações sensíveis. Redirecionam os usuários para páginas que instalam software malicioso em seus dispositivos ou coletam dados sem consentimento.

Prevenção Redes Sociais

Ajuste suas configurações de privacidade: Ajuste as configurações de privacidade para controlar quem pode ver suas informações e postagens.

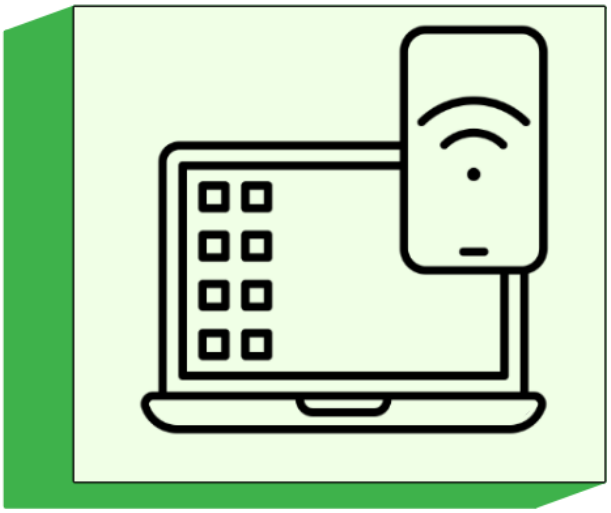
Seja seletivo ao aceitar solicitações de amizade: Aceite apenas solicitações de pessoas que você conhece e confia.

Evite compartilhar informações pessoais sensíveis: Não divulgue dados como endereço, número de telefone, ou informações financeiras.

Tenha cuidado com links e aplicativos: Não clique em links suspeitos e evite instalar aplicativos desconhecidos.

Habilite a autenticação de dois fatores (2FA): Adicione uma camada extra de segurança às suas contas de redes sociais.

Atenção ao que instala em seus dispositivos



Se não houver atenção ao que se instala nos dispositivos, uma série de riscos pode comprometer a segurança e a privacidade do usuário. Por exemplo, o dispositivo pode ser infectado por malwares, o que coloca em risco a privacidade devido a aplicativos que solicitam permissões excessivas, ou o usuário pode ser vítima de algum aplicativo malicioso que coleta informações pessoais sem o seu conhecimento.

Comportamento: Infectam dispositivos para roubar dados, espiar atividades ou causar danos ao sistema. Enganam os usuários para que instalem malware, para roubar informações ou comprometer a segurança do dispositivo. Por meio de softwares exibem anúncios indesejados nos dispositivos. Redireciona o navegador para sites publicitários e coleta dados de navegação sem consentimento.

Prevenção Aos Dispositivos

Baixe aplicativos apenas de fontes oficiais: Use a Google Play Store (Android) ou App Store (iOS) para baixar aplicativos, entretanto deve-se ter bastante atenção também nas lojas de aplicativos, verifique a origem do App na loja e as avaliações.

Verifique permissões de aplicativos: Revise as permissões solicitadas por um aplicativo antes de instalá-lo e conceda apenas o necessário.

Leia avaliações e pesquisas: Verifique avaliações e faça uma pesquisa sobre o aplicativo antes de baixá-lo.

Mantenha seu software atualizado: Instale atualizações de segurança regularmente para proteger contra vulnerabilidades.

Use software de segurança: Instale antivírus e outros programas de segurança para proteger seu dispositivo contra malwares.

Banco via Internet

É importante se atentar aos riscos que podem comprometer sua segurança financeira e pessoal, esses crimes cibernéticos podem ocorrer por meio de técnicas de phishing, fazendo a vítima passar informações, e acessando aplicativos ou sites falsos.

Comportamento: Enviam e-mails ou mensagens falsas que parecem ser do banco, pedindo dados de login ou informações de cartão de crédito. Capturam informações de login e senhas quando o usuário acessa sua conta bancária online com Software malicioso que registra tudo o que é digitado no teclado (Keyloggers).

Prevenção Banco via Internet

Acesse o banco através de dispositivos seguros: Utilize seu próprio dispositivo e evite computadores públicos ou compartilhados.

Use autenticação de dois fatores (2FA): Adicione uma camada extra de segurança às suas contas bancárias online.

Verifique a segurança do site do banco: Certifique-se de que o site utiliza HTTPS e verifique a autenticidade do site antes de fazer login.

Monitore suas contas regularmente: Verifique frequentemente suas transações para identificar atividades suspeitas rapidamente.

Evite redes Wi-Fi públicas: Prefira redes privadas e seguras ao acessar suas contas bancárias online.

Conteúdo Extra.

Tipos de Ameaças Cibernéticas: Malwares e Técnicas de engenharia social.

Categorizando de maneira geral as ameaças:

Malwares.

Software malicioso projetado para causar danos, roubar informações ou realizar outras atividades maliciosas em dispositivos e redes.

Principais Tipos de Malware:

● Vírus: Programas que se replicam inserindo cópias de si mesmos em outros programas ou arquivos.

● Worms: Programas que se replicam por conta própria e se espalham através de redes.

● Trojans (Cavalos de Tróia): Programas que parecem legítimos, mas realizam atividades maliciosas quando executados.

● Ransomware: Programas que criptografam dados e exigem pagamento para sua liberação.

● Spyware: Programas que coletam informações sobre as atividades do usuário sem o seu conhecimento.

● Adware: Programas que exibem anúncios indesejados.

● Rootkits: Programas que permitem acesso não autorizado e ocultam a presença de outros malwares.

● Keyloggers: Programas que registram as teclas digitadas para roubar informações.

Técnicas de Engenharia Social.

Métodos de manipulação psicológica usados para enganar as pessoas e fazê-las divulgar informações confidenciais ou realizar ações que comprometem a segurança.

Principais Técnicas de Engenharia Social:

● Phishing: E-mails, mensagens de texto ou sites fraudulentos que solicitam informações pessoais.

● Spear Phishing: Phishing direcionado a indivíduos ou organizações específicas com informações personalizadas.

● Pharming: Redirecionamento de tráfego de um site legítimo para um site falso.

● Baiting: Oferecer algo atraente para induzir a vítima a executar o malware.

● Pretexting: Enganar uma vítima para que ela forneça informações sob falsos pretextos.

● Quid Pro Quo: Prometer um benefício em troca de informações ou execução de uma ação.

● Scareware: Utilizar mensagens de medo para enganar os usuários e fazê-los instalar software malicioso.

● Malvertising: Distribuição de malware através de anúncios online maliciosos.

Material desenvolvido para Atividade Extensionista Uninter.