ASSOCIAÇÃO DO MINISTÉRIO PÚBLICO DO RIO GRANDE DO SUL
ampfrs

Núcleo de Inovação e Tecnologia

PÍLULAS DE INOVAÇÃO E TECNOLOGIA

EDIÇÃO III - NOVEMBRO/DEZEMBRO 2024

SEGURANÇA DIGITAL

Entender os perigos do ambiente digital é fundamento básico para proteger informações sensíveis pessoais e do Ministério Público

A segurança digital tornou-se um tema central em um mundo cada vez mais conectado. A proteção de informações sensíveis, a integridade dos sistemas e a privacidade dos usuários são elementos cruciais em qualquer organização, especialmente em instituições públicas como a do Ministério Público.

Com o aumento das ameaças cibernéticas e a dependência crescente da tecnologia, compreender os fundamentos da segurança digital é essencial para mitigar riscos e evitar "dores de cabeça".

"Há um ditado popular que diz que um computador seguro é aquele que está desligado. Isso é inteligente, mas é falso: O hacker convencerá alguém a entrar no escritório e ligar aquele computador. Tudo é uma questão de tempo, paciência, personalidade e persistência."

Kevin Mitnick, um dos mais famosos hackers do mundo

Nessa época de fim de ano as ameaças se multiplicam: compras online, comemorações em excesso, décimo terceiro na conta e as férias expoêm os usuários a maiores probabilidades de serem vítimas.

Com a enormidade de contas a serem pagas e com o desejo de maximizar os ganhos, é desafiador segurar a empolgação voltada a se aproveitar "boas ofertas" e não sair clicando em qualquer link que mandam para a gente antes que termine a promoção ("ūltimas unidade").

Dessa forma, nessa edição, teremos contato com fundamentos básicos da segurança digital, procedimentos e cuidados na internet, os perigos da inteligência artificial nesse cenário e os principais golpes online praticados no Brasil em 2024. Venham conosco nessa jornada de aprendizado!

DESTAQUES DO MÊS

O BÁSICO DA SEGURANÇA DIGITAL

A segurança digital tem três pilares: a confidencialidade, a integridade e a disponibilidade. Elas são popularmente abreviadas como CID.

A **confidencialidade** assegura que apenas pessoas autorizadas tenham acesso a informações sensíveis, utilizando tecnologias como criptografia e controle de acessos. Um exemplo é o uso do WhatsApp para enviar mensagens. Ele utiliza criptografia ponta a ponta, o que significa que apenas você e o destinatário podem ler as mensagens; nem mesmo a empresa WhatsApp pode acessá-las.

A **integridade** protege os dados contra alterações não autorizadas, garantindo que as informações permaneçam precisas e confiáveis.
Por exemplo, durante a coleta das provas digitais, um perito calcula o hash de cada arquivo (uma espécie de "impressão digital" única do documento).

Esse hash é registrado junto com a prova. No momento de apresentar o relatório em juízo, o hash é recalculado. Se o novo hash for idêntico ao registrado no momento da coleta, a integridade da prova está confirmada. Caso contrário, indica que o arquivo foi alterado em algum momento, comprometendo sua validade no processo judicial.

Já a **disponibilidade** garante que os sistemas e dados estejam acessíveis aos usuários legítimos sempre que necessário, mesmo diante de ataques ou falhas técnicas.

Isso é feito por meio de backups, servidores redundantes e proteções contra ataques, como o uso de firewalls. Por exemplo, um banco digital garante que você possa acessar sua conta 24 horas por dia, 7 dias por semana, utilizando sistemas redundantes. Se um servidor falhar, outro assume a operação, evitando que o serviço fique fora do ar.

Os hackers e golpistas em geral sempre atingem um ou mais desses pilares quando realizam seus ataques e golpes. Em algumas situações dependem da colaboração do alvo para a execução da ação criminosa.

Outros conceitos fundamentais, como autenticidade e não-repúdio, também desempenham um papel importante na segurança digital.

A **autenticidade** assegura que os usuários ou sistemas são quem "dizem" ser, enquanto o **não-repúdio** impede que uma pessoa ou sistema negue uma ação realizada, como o envio de um e-mail ou a realização de uma transação.

As ameaças à segurança digital evoluem constantemente, destacando-se entre as mais preocupantes os **malwares** e os **ataques de engenharia social**, como o phishing.

Essas técnicas são utilizadas para comprometer dados, invadir sistemas e causar prejuízos financeiros ou institucionais.

O aumento da sofisticação desses métodos exige não apenas tecnologias avançadas, mas também maior conscientização e preparo por parte dos usuários.

O malware abrange uma ampla categoria de softwares maliciosos, incluindo ransomware, trojans e spyware.

Um ataque de ransomware, por exemplo, pode criptografar dados críticos de uma instituição, como documentos de investigações sigilosas, exigindo resgate para restaurar o acesso. Já os trojans podem ser disfarçados como aplicativos legítimos, mas, ao serem executados, abrem portas para invasores controlarem remotamente o sistema da vítima.

Por outro lado, os ataques de engenharia social, como o **phishing**, não dependem de falhas tecnológicas, mas sim de falhas humanas. Esses golpes utilizam mensagens fraudulentas, muitas vezes simulando comunicação oficial de bancos, empresas ou órgãos públicos, para enganar os destinatários.

Por meio de links ou anexos maliciosos, os atacantes conseguem acesso a informações confidenciais ou instalam malwares no sistema da vítima.

Um exemplo recente de phishing sofisticado envolveu mensagens direcionadas a servidores públicos oferecendo supostas atualizações de sistemas de trabalho. Ao clicar no link fornecido, as vítimas eram redirecionadas para sites falsos que coletavam credenciais de acesso. Esses ataques mostram como os criminosos têm se tornado cada vez mais estratégicos ao personalizar abordagens e explorar contextos reais.

A prevenção contra malwares passa pelo uso de **soluções tecnológicas robustas**, como antivírus atualizados, firewalls avançados e sistemas de detecção e prevenção de intrusões (IDS/IPS).

Essas ferramentas ajudam a bloquear ataques antes que possam causar danos significativos. Entretanto, a eficiência dessas tecnologias depende de sua implementação correta e do monitoramento contínuo por equipes especializadas.

Quando se trata de engenharia social, a principal defesa é a **educação do usuário.** Todos os usuários das redes e sistemas devem ser capacitados para reconhecer tentativas de phishing, como mensagens urgentes pedindo dados ou ofertas que parecem boas demais para ser verdade.

Treinamentos regulares com exemplos práticos e atuais de fraudes ajudam a fortalecer a capacidade de discernimento e a reduzir a probabilidade de erro humano.

Outra medida crucial é a adoção de autenticação multifator (MFA), que adiciona uma camada extra de segurança ao acesso a sistemas.

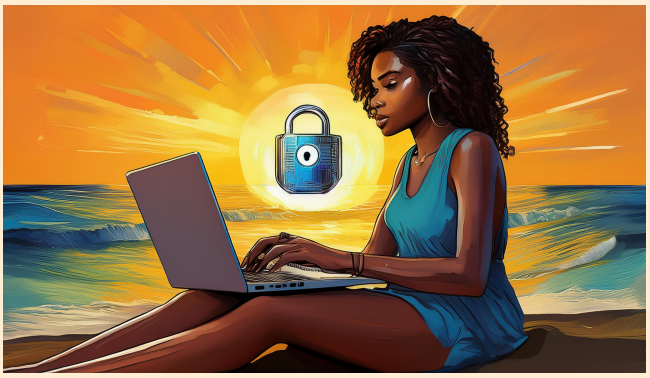
Mesmo que as credenciais sejam comprometidas por phishing, o atacante não conseguirá acessar a conta sem a segunda etapa de autenticação, como um código enviado ao celular do usuário. Essa prática é essencial para proteger sistemas que contêm informações sensíveis.

Diante do atual cenário em que as ameaças digitais estão em constante evolução, proteger-se contra malwares e engenharia social requer um esforço conjunto.

A PREVENÇÃO DO USUÁRIO

A crescente digitalização das atividades cotidianas trouxe inúmeras facilidades, mas também aumentou a exposição a cibercrimes, como fraudes eletrônicas, roubo de identidade e invasões de dispositivos.

Para se proteger é essencial que os usuários adotem boas práticas de segurança digital, garantindo não apenas a proteção de seus dados, mas também a de sistemas e redes aos quais estão conectados (IDEIA DE TIME).



Senhas Fortes

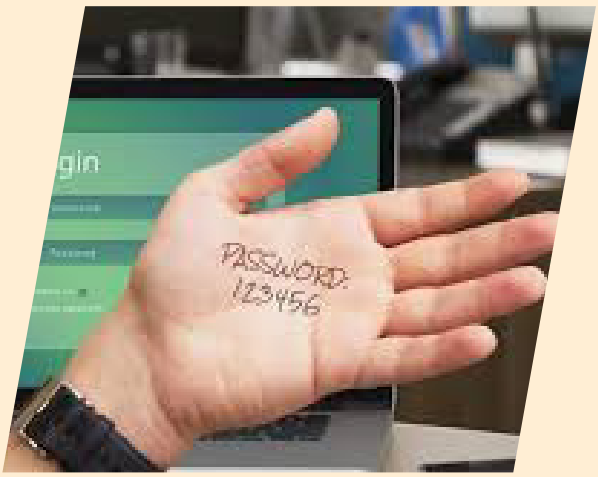
As senhas fortes são fundamentais para a segurança digital, servindo como uma barreira essencial contra acessos não autorizados a contas, dispositivos e informações sensíveis.

Em um mundo digitalizado, onde serviços bancários, redes sociais e até sistemas corporativos são acessados online, o uso de senhas robustas reduz significativamente os riscos de invasões e violações de privacidade.

Uma senha forte é composta por uma combinação de letras **maiúsculas** e **minúsculas**, **números** e **caracteres especiais**, além de ter no mínimo **12 caracteres**.

Diversas técnicas são usadas para quebrar senhas. Ataques de força bruta tentam todas as combinações possíveis até encontrar a correta, enquanto ataques de dicionário exploram senhas comuns ou padrões previsíveis, como “123456” ou “senha123”.

Outro método é a **engenharia social**, por meio do qual os atacantes enganam as vítimas para que elas revelem suas senhas - seja por meio de mensagens fraudulentas ou links maliciosos. Além disso, vazamentos de dados em plataformas conhecidas expõem senhas que podem ser reutilizadas em outros serviços, aumentando o alcance dos danos - verdadeiro efeito dominó.



Os usuários podem tomar medidas preventivas simples, mas eficazes, para fortalecer sua segurança digital. Evitar o uso de senhas previsíveis, como datas de nascimento ou nomes próprios, é crucial.

Cada conta deve ter uma senha única, de modo que a violação de uma não comprometa outras. Trocar senhas regularmente e nunca compartilhar credenciais com terceiros são práticas fundamentais.

Para gerenciar senhas de forma segura, diversos serviços e aplicativos podem ser utilizados. Gerenciadores de senhas como LastPass, Locker, 1Password e Bitwarden ajudam os usuários a criar, armazenar e proteger senhas complexas.

Essas ferramentas geram combinações únicas e difíceis de serem quebradas, além de alertarem para senhas comprometidas ou fracas. Sistemas operacionais modernos, como iOS e Android, também oferecem gerenciadores integrados, como o iCloud Keychain e o Google Password Manager, que armazenam credenciais de maneira criptografada e sincronizam entre dispositivos.

Tanto o iOS quanto o Android também implementam tecnologias adicionais de segurança, como autenticação biométrica (impressão digital e reconhecimento facial) e alertas sobre vazamentos conhecidos.

Essas plataformas recomendam automaticamente a atualização de senhas fracas ou reutilizadas. Manter o sistema operacional atualizado é outra medida importante, pois **patches de segurança** corrigem vulnerabilidades que poderiam ser exploradas por atacantes.

Autênticação Multifator (MFA)
É uma das ferramentas mais eficazes para fortalecer a segurança digital, protegendo contas e dispositivos contra acessos não autorizados.

Diferentemente da autenticação de um único fator, como o uso exclusivo de uma senha, a MFA **combina dois ou mais métodos de verificação de identidade**, geralmente divididos em três categorias: algo que você sabe (senha ou PIN), algo que você possui (smartphone, token físico) e algo que você é (impressão digital, reconhecimento facial ou de voz).

Essa abordagem reduz significativamente os riscos, pois mesmo que uma das camadas de segurança seja comprometida, as outras continuam protegendo a conta.

A importância da MFA é evidente no atual cenário de cibersegurança, onde ataques de phishing, vazamentos de dados e força bruta são comuns. Uma senha pode ser roubada, mas a exigência de um segundo fator, como um código gerado por um aplicativo ou enviado por SMS, dificulta o acesso indevido.

Para contas sensíveis, como e-mails, bancos e redes sociais, a MFA adiciona uma barreira extra, tornando as invasões muito mais complexas e menos atrativas para os criminosos.

Além disso, muitas plataformas já exigem ou recomendam o uso da MFA como prática padrão, especialmente em ambientes corporativos que lidam com **dados confidenciais.**

Há várias opções de MFA disponíveis no mercado adequadas a diferentes necessidades. Aplicativos como Google Authenticator, Authy e Microsoft Authenticator geram códigos temporários para validação.

Chaves de segurança físicas, como as oferecidas por Yubico e Feitian, oferecem uma camada adicional robusta, especialmente em ambientes corporativos.
Dispositivos móveis com autenticação biométrica também são amplamente utilizados, integrando impressões digitais ou reconhecimento facial como um fator de segurança. Além disso, plataformas como iOS e Android oferecem autenticação multifator integrada, como códigos automáticos e prompts de confirmação diretamente nos dispositivos, tornando o processo mais seguro e conveniente para os usuários.

Microsoft Authenticator

Não clicar em um link não verificado:
O usuário pode ser redirecionado para sites fraudulentos que capturam informações pessoais ou financeiros, instalarm malwares no dispositivo ou ativam ações indesejadas, como o sequestro de dados. O perigo está no fato de que esses links frequentemente se disfarçam de comunicações legítimas, como mensagens de bancos, empresas conhecidas ou contatos confiáveis, explorando a confiança e a desatenção do usuário.

Um dos principais riscos é o roubo de informações confidenciais por meio de páginas falsas que imitam sites oficiais. Por exemplo, em ataques de phishing, o usuário pode ser induzido a inserir credenciais bancárias ou dados pessoais em um site que parece legítimo, mas que está sob controle de criminosos.

Outro risco significativo é a instalação de malwares, como ransomwares, que criptografam os arquivos do dispositivo e exigem pagamento para restaurar o acesso - alguns links podem capturar automaticamente cookies ou dados armazenados no navegador, permitindo que os atacantes acessem contas ou informações sem o conhecimento do usuário.

Os impactos de clicar em links maliciosos podem ser graves e variados. Em casos financeiros, os dados roubados podem ser usados para compras fraudulentas, transferências bancárias ou até para criar contas falsas em nome da vítima.

Além disso, a instalação de softwares maliciosos pode comprometer a privacidade, permitindo que criminosos monitorem atividades, capturem senhas ou acessem informações sensíveis.

Manter sistemas e aplicativos atualizados

É uma das práticas mais importantes para garantir a segurança digital. Atualizações, conhecidas como patches de segurança, corrigem vulnerabilidades descobertas nos sistemas operacionais, softwares e aplicativos que usamos diariamente.

Essas falhas podem ser exploradas por atacantes para acessar dispositivos, roubar dados ou instalar malwares. Ignorar atualizações deixa os sistemas

expostos a ameaças que, muitas vezes, já são conhecidas e amplamente exploradas por criminosos digitais.

Os riscos de não atualizar incluem a exposição a ataques direcionados e genéricos, como exploração de vulnerabilidades "zero-day" (aquelas descobertas, mas ainda sem correção pública) ou falhas conhecidas que já foram corrigidas por desenvolvedores.

Por exemplo, um ransomware pode explorar uma brecha em um sistema desatualizado para criptografar os dados do dispositivo e exigir resgate.

Além disso, aplicativos desatualizados podem conter bugs que permitem acessos não autorizados ou uso indevido das funcionalidades, colocando em risco informações pessoais e corporativas.

Atualizar regularmente os sistemas reduz significativamente esses riscos e melhora a segurança geral do dispositivo. Sistemas operacionais modernos, como Windows, macOS, iOS e Android, oferecem configurações automáticas para baixar e aplicar atualizações de segurança, garantindo que dispositivos estejam sempre protegidos.

Evitar o uso de redes Wi-Fi públicas
É fundamental para garantir a segurança digital, pois essas conexões são frequentemente inseguras e vulneráveis a ataques cibernéticos.

Redes públicas, como as encontradas em cafeterias, aeroportos e hotéis, geralmente não possuem criptografia adequada, permitindo que dados transmitidos entre o dispositivo do usuário e a internet sejam interceptados por terceiros.

Um dos maiores riscos associados ao uso de Wi-Fi público é o ataque de **"man-in-the-middle"** (MITM), em que o atacante intercepta e monitora a comunicação entre o dispositivo do usuário e o servidor de destino.

Além disso, criminosos podem criar redes Wi-Fi falsas com nomes semelhantes aos de redes legítimas para enganar usuários e roubar informações.

Por exemplo, um golpista pode configurar uma rede chamada "Café_WiFi" em um local movimentado, atraindo vítimas que se conectam inadvertidamente. Outro risco é o uso de softwares para capturar informações transmitidas em redes abertas, permitindo acesso a contas bancárias ou e-mails.

Para mitigar esses riscos, a melhor prática é evitar o uso de redes Wi-Fi públicas para acessar informações sensíveis ou realizar transações financeiras.

Caso seja necessário utilizá-las, o **uso de uma VPN** (Virtual Private Network) é altamente recomendado, pois ela cria uma conexão criptografada que protege os dados transmitidos.

Além disso, certifique-se de acessar apenas sites que utilizam o **protocolo HTTPS**, que garante a criptografia entre o navegador e o site. Sempre que possível, prefira utilizar a rede móvel ou um ponto de acesso pessoal para garantir maior segurança na conexão. Essas práticas ajudam a minimizar os riscos associados ao uso de redes públicas e mantêm as informações dos usuários protegidas.

Evitar compartilhar informações pessoais sensíveis nas redes sociais
É essencial para proteger a privacidade e a segurança digital, tanto de adultos quanto de crianças e adolescentes. Dados como endereço, número de telefone, rotina diária ou localizações podem parecer inofensivos, mas podem ser utilizados por criminosos para fins como roubo de identidade, golpes ou até mesmo assédio.

No caso de **crianças e adolescentes**, a exposição nas redes sociais é ainda mais preocupante, pois pode atrair predadores online, facilitando crimes como aliciamento e exploração sexual.

A falta de controle sobre quem pode acessar essas informações torna as redes sociais um ambiente potencialmente perigoso.

Um dos principais riscos relacionados ao compartilhamento excessivo é a **engenharia social**, onde criminosos utilizam informações disponíveis nas redes para manipular vítimas ou aplicar golpes personalizados.

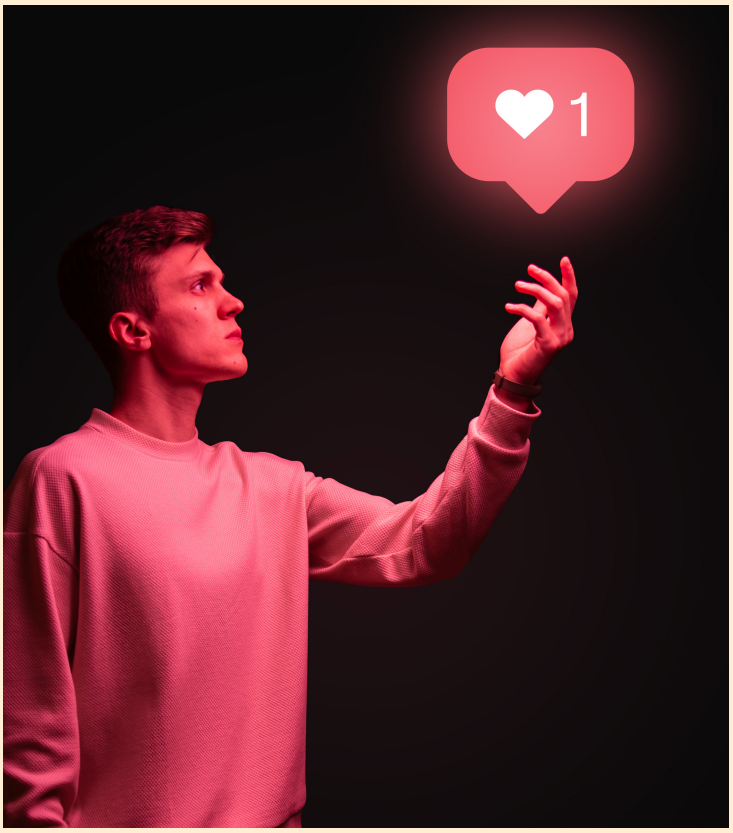
Por exemplo, dados sobre o local de trabalho ou os hábitos de uma pessoa podem ser usados para criar fraudes convincentes, como mensagens de phishing que parecem legítimas.

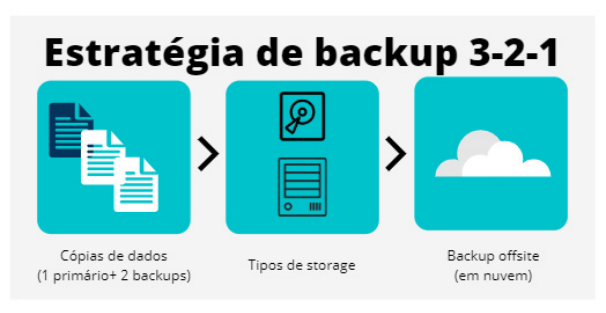
No caso de crianças, fotos e vídeos aparentemente inofensivos podem ser explorados por criminosos em **redes de pedofilia ou usados para bullying** e **humilhação digital,** causando danos psicológicos graves.

Para mitigar esses riscos, é essencial que adultos ajustem as **configurações de privacidade** de suas contas e das contas das crianças, limitando quem pode ver o conteúdo publicado.

É fundamental evitar a exposição de documentos, detalhes bancários, localizações em tempo real e imagens que identifiquem **uniformes escolares** ou locais de rotina das crianças.

Educar crianças e adolescentes sobre os perigos de interagir com desconhecidos ou compartilhar informações pessoais nas redes é igualmente importante.





Fazer Backups regularmente

Backups consistem em cópias de segurança de informações importantes, como documentos, fotos ou dados corporativos, armazenados em locais seguros e separados do sistema original.

Eles são fundamentais para mitigar os impactos de falhas técnicas, ataques cibernéticos, como ransomware, ou mesmo erros humanos, garantindo que os dados possam ser recuperados rapidamente e com integridade.

A regularidade dos backups é crucial para que os dados armazenados reflitam a versão mais recente possível, minimizando perdas. Soluções modernas, como backups automáticos em serviços de nuvem, aumentam a eficiência e reduzem o risco de esquecimentos.

É importante adotar uma estratégia diversificada, conhecida como **regra 3-2-1:** três cópias dos dados (original e duas de backup), armazenadas em dois formatos diferentes (como HD externo e nuvem), sendo uma mantida fora do local principal. Essa abordagem garante proteção em cenários como falhas físicas, ataques cibernéticos ou desastres naturais.

Usar Criptografia para proteger arquivos e mensagens sensíveis

A criptografia é uma ferramenta essencial para a segurança digital, garantindo que informações sejam transformadas em um formato codificado que só pode ser acessado por pessoas ou sistemas autorizados.

Ela protege dados em trânsito (enviados pela internet ou redes internas) e em repouso (armazenados em dispositivos ou servidores).

A criptografia assegura três pilares fundamentais da segurança da informação: **confidencialidade**, protegendo contra acessos não autorizados; **integridade**, impedindo alterações nos dados sem detecção; e **autenticidade**, garantindo que as informações venham de uma fonte legítima.

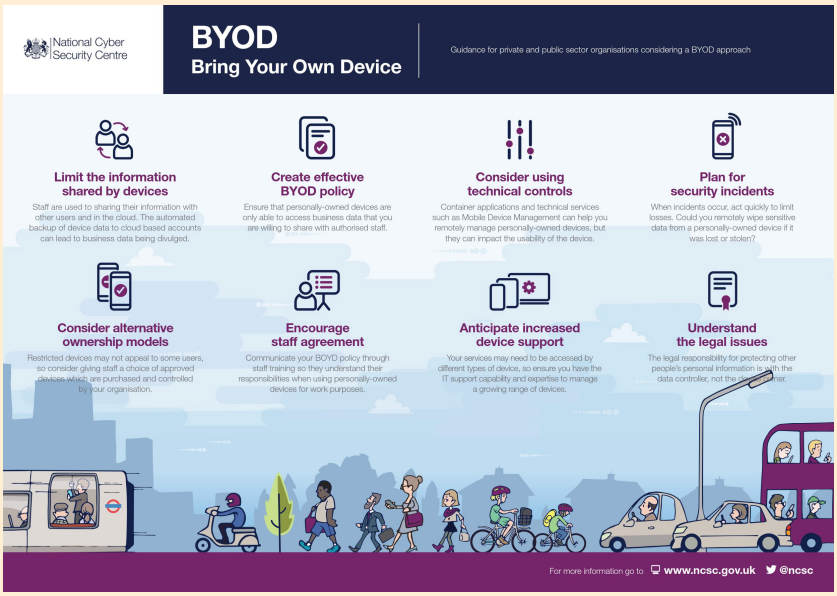
No contexto corporativo, a criptografia é amplamente utilizada em ferramentas de comunicação e colaboração, como o Microsoft Teams.

O Teams implementa criptografia ponta a ponta (E2EE) em chamadas, garantindo que o conteúdo das conversas permaneça acessível apenas aos participantes autorizados.

Ele também utiliza criptografia para proteger mensagens e arquivos armazenados no serviço, assegurando que mesmo em caso de interceptação, os dados permaneçam ilegíveis para terceiros.

No que diz respeito ao compartilhamento de arquivos, o Microsoft Teams reforça a segurança com a integração ao OneDrive e ao SharePoint, que também utilizam criptografia para proteger arquivos armazenados e em trânsito.

A plataforma também permite configurar permissões específicas, controlando quem pode visualizar, editar ou compartilhar um arquivo, proporcionando um nível adicional de proteção e controle sobre os dados.



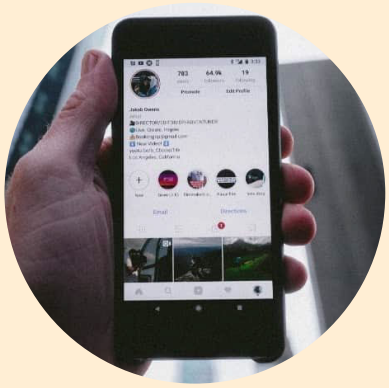
Ter cuidado com os equipamentos que conectam com as redes do MP ou que guardem arquivos do trabalho

A prática do BYOD (Bring Your Own Device), que permite que funcionários utilizem seus dispositivos pessoais para acessar sistemas corporativos, apresenta diversos **riscos de segurança,** especialmente quando o mesmo dispositivo é compartilhado com outros membros da família.

Situações como o uso do aparelho por crianças para jogos online, downloads de aplicativos desconhecidos ou navegação em sites de baixa reputação podem introduzir malwares ou comprometer a segurança do dispositivo.

O acesso a conteúdos inadequados, como pornografia, pode expor o aparelho a vírus ou tentativas de phishing, colocando em risco tanto os dados pessoais quanto as informações corporativas armazenadas ou acessadas no dispositivo.

OS GOLPES MAIS COMUNS



Conhecer os golpes mais comuns no ambiente permite fortalecer cuidados preventivos no dia a dia no ambiente digital. Na época de fim de ano, é preciso de estar de olhos abertos e com a atenção redobrada.

O Golpe do Phishing em Promoções no Instagram

No Instagram, os golpistas criam perfis falsos que imitam marcas ou lojas renomadas, oferecendo promoções exclusivas, sorteios ou brindes atrativos.

Ao clicar em um link enviado por esses perfis, as vítimas são redirecionadas para páginas que simulam o login oficial do Instagram.

Quando os alvos inserem suas credenciais, os dados são enviados diretamente aos criminosos.

Já no WhatsApp, mensagens com links falsos prometem prêmios ou promoções e, ao serem acessados, instalam malwares que permitem o sequestro da conta ou a captura de informações sensíveis. Com o controle da conta da vítima, os criminosos obtêm várias vantagens.

Primeiramente, utilizam o perfil sequestrado para espalhar o golpe, enviando mensagens para os contatos do usuário com pedidos de dinheiro ou oferecendo supostas promoções, amplificando o alcance da fraude.

Além disso, muitas contas sequestradas são revendidas no mercado negro digital, especialmente se tiverem muitos seguidores ou histórico de interação relevante.

Em outros casos, os golpistas pedem resgates financeiros para devolver o acesso à conta, gerando lucro direto com a extorsão.

Também há situações em que informações pessoais ou financeiras obtidas nesses golpes são usadas para fraudes maiores, como clonagem de cartões ou abertura de contas fraudulentas.

As dificuldades para combater esses golpes são significativas. As Big Techs, como a Meta (responsável por Instagram e WhatsApp), têm demonstrado lentidão no banimento de perfis falsos e na interrupção da propagação dos links maliciosos.

Isso ocorre porque os criminosos frequentemente criam múltiplos perfis e mudam suas estratégias rapidamente, dificultando a identificação automatizada.

Além disso, o processo de denúncia pelas vítimas pode ser confuso e demorado, o que agrava o problema. A recuperação de contas comprometidas também é burocrática e nem sempre eficaz, deixando os usuários vulneráveis e muitas vezes sem solução imediata.

Esses golpes expõem a necessidade urgente de plataformas digitais adotarem mecanismos mais robustos de detecção de fraude, como monitoramento automatizado de padrões de comportamento anômalos e validações mais rigorosas para a criação de contas.

Golpe das Lojas Online Falsas

É uma prática crescente que se aproveita da popularização do comércio eletrônico e da confiança dos consumidores em realizar compras pela internet.

Criminosos criam sites que imitam lojas legítimas, com layout profissional e ofertas extremamente atraentes, geralmente abaixo do preço de mercado. Esses sites fraudulentos são promovidos por meio de redes sociais, anúncios pagos e até mensagens diretas, atraindo consumidores que buscam produtos com descontos significativos.

Após a realização da compra, o consumidor não recebe o produto ou, em alguns casos, recebe itens de qualidade muito inferior ao prometido.

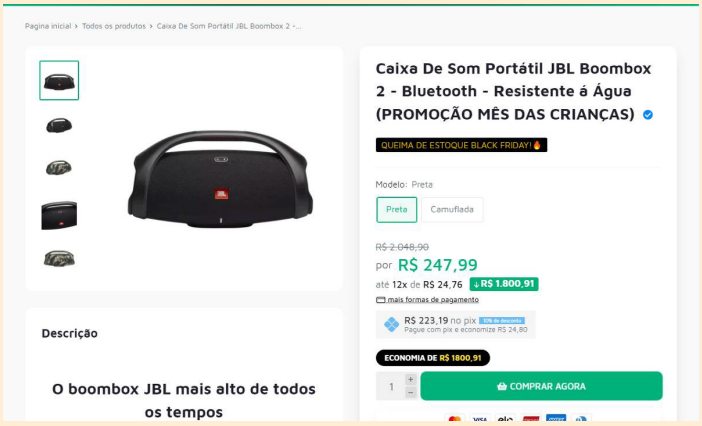
Além disso, as informações financeiras e pessoais fornecidas no momento da compra podem ser usadas em outros golpes, como clonagem de cartões e roubo de identidade.

Os criminosos geralmente utilizam formas de pagamento como Pix ou transferências bancárias, que são mais difíceis de rastrear e reverter.

No site oficial da Americanas você vai encontrar sempre "americanas.com.br"

Verifique se no início do link aparece a sigla "https" e/ou símbolo de cadeado. (🔒). Ambos indicam que a conexão é segura.

O combate a essas lojas online falsas é particularmente desafiador por conta da velocidade com que os sites são criados e desativados.



Muitos desses sites operam por períodos curtos, saindo do ar logo após acumularem um grande volume de vendas fraudulentas. Além disso, os criminosos frequentemente utilizam servidores em outros países, dificultando a atuação das autoridades brasileiras e a aplicação de sanções legais.

A disseminação dos links em redes sociais e a ausência de verificação rigorosa por parte das plataformas de anúncios também contribuem para a perpetuação do golpe.

Para prevenir esse tipo de golpe, é fundamental que consumidores adotem boas práticas de segurança ao realizar compras online.

Verificar a reputação da loja em sites de reclamação, conferir o domínio do site (evitando páginas com extensões suspeitas ou nomes semelhantes aos de marcas conhecidas) e optar por métodos de pagamento seguros, como cartões de crédito, são medidas essenciais.

Golpe do Aluguel de Temporada Falso

O golpe do aluguel de temporada falso é um esquema comum em períodos de alta procura por acomodações, como férias, feriados prolongados ou eventos especiais.

Os golpistas aproveitam a urgência e o desejo por boas ofertas para enganar vítimas, anunciando imóveis inexistentes ou indisponíveis em plataformas de aluguel, redes sociais e até em sites falsos que imitam empresas conhecidas.

A promessa de preços baixos e condições vantajosas é usada como isca para atrair os consumidores.
No golpe, os criminosos publicam anúncios com fotos atraentes de casas ou apartamentos, muitas vezes retiradas de sites legítimos.

A vítima é convencida a realizar um pagamento adiantado, como um sinal ou até o valor total do aluguel, sob o argumento de garantir a reserva.

Após o pagamento, o golpista desaparece, cortando contato com a vítima, que só descobre o golpe ao tentar ocupar o imóvel ou ao investigar a legitimidade do anúncio.

Sempre use plataformas confiáveis, que ofereçam sistemas de pagamento seguros e proteção contra fraudes. Verifique a reputação do anunciante, lendo avaliações de outros usuários e confirmando a existência do imóvel com informações externas, como mapas ou contatos diretos.

Nunca realize pagamentos via transferência bancária para contas desconhecidas ou pessoais.

Golpe da Viagem Falsa

Os golpes envolvendo vendas de passagens aéreas e pacotes de viagem falsos são uma prática recorrente, especialmente em períodos de alta demanda, como férias e feriados prolongados.

Criminosos se aproveitam do interesse por promoções e descontos atrativos para enganar consumidores, utilizando anúncios em redes sociais, e-mails e sites que simulam agências de turismo ou companhias aéreas legítimas. A promessa de preços muito abaixo do mercado é uma das principais iscas para atrair as vítimas.

O golpe funciona de diferentes maneiras. Em muitos casos, o consumidor é direcionado a um site fraudulento que imita o layout de empresas conhecidas, onde realiza a compra e faz o pagamento, geralmente via transferência bancária ou Pix.

Após a transação, o bilhete enviado não é válido ou sequer existe.

Em outra variação, golpistas utilizam anúncios em marketplaces e redes sociais, oferecendo pacotes de viagem por preços promocionais e, após o pagamento, cortam o contato com a vítima.

7 De Dezembro De 2023

PC-AM prende estelionatária por aplicar golpe do falso bilhete aéreo e lucrar mais de R$ 100 mil com a prática ilícita

A autora se passava por consultora de viagens e falsificava os bilhetes aéreos das vítimas

A Polícia Civil do Amazonas (PC-AM), por meio do 1° Distrito Integrado de Polícia (DIP), prendeu, na quarta-feira (06/12), Aline Nascimento Corrêa, 39, por aplicar o golpe do falso bilhete aéreo. Estima-se que a infratora lucrou mais de R$ 100 mil com a prática ilícita. A prisão ocorreu na residência dela no bairro Lírio do Vale, zona oeste da capital.

Conforme o delegado Cícero Túlio, titular da unidade policial, as investigações iniciaram após recebimento de diversas denúncias nos meses de setembro e outubro contra Aline.

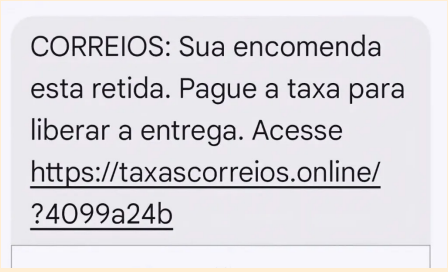
"Há aproximadamente um ano, Aline montou uma agência de viagens falsa na própria residência, e se passava por uma consultora de viagens. Com isso, ela ofertava promoções de passagens nas suas redes sociais, fazendo com que as vítimas tivessem interesse nesses pacotes promocionais e a procurassem para fechar negócio", explicou o delegado.

Segundo a autoridade policial, as vítimas cediam seus cartões de crédito para a infratora, acreditando que ela compraria suas passagens, no entanto, ela falsificava os bilhetes aéreos e utilizava o cartão para efetuar outras compras.

Golpe do rastreamento das encomendas

Um golpe sofisticado que tem ganhado destaque envolve o uso de malwares disfarçados como aplicativos de rastreamento de pacotes.

Com o aumento do comércio eletrônico, especialmente em épocas de maior movimentação, como Black Friday e Natal, muitos consumidores aguardam entregas e utilizam aplicativos ou links



para rastrear seus pedidos. Os golpistas aproveitam essa prática comum para induzir as vítimas a instalar aplicativos falsos, que na verdade são softwares maliciosos.

O golpe funciona da seguinte maneira: a vítima recebe um e-mail, SMS ou mensagem em aplicativos como WhatsApp, supostamente de uma empresa de logística, o Correios ou loja, informando sobre um problema na entrega ou solicitando o acompanhamento do pedido por meio de um link.

Ao clicar no link, a vítima é redirecionada para uma página que solicita o download de um "aplicativo de rastreamento". Ao instalar o software, o dispositivo da vítima é infectado com malware que pode roubar informações financeiras, credenciais bancárias ou até mesmo controlar o aparelho remotamente.

O perigo desse golpe está na aparência legítima dos aplicativos e na sofisticação dos malwares. Alguns desses programas conseguem capturar dados de aplicativos bancários, acessar

mensagens SMS para interceptar códigos de autenticação ou até ativar a câmera e o microfone do dispositivo sem que o usuário perceba. Em muitos casos, a vítima só percebe que foi enganada ao notar movimentações financeiras não autorizadas ou o comprometimento de contas pessoais.

O golpe do Marketplace

Ele ocorre principalmente em sites e aplicativos de comércio eletrônico onde usuários podem vender produtos diretamente a outros consumidores.

Os golpistas aproveitam a confiança e a informalidade dessas interações para enganar compradores e vendedores, causando prejuízos financeiros.

No caso de compradores, o golpe geralmente envolve anúncios de produtos atrativos, como eletrônicos ou móveis, a preços muito abaixo do mercado.

Após o contato inicial, o golpista solicita o pagamento antecipado via transferência bancária ou Pix, alegando urgência ou alta demanda pelo item. Depois de receber o dinheiro, o criminoso desaparece sem enviar o produto, deixando a vítima sem recursos ou formas fáceis de recuperar o valor.

Para os vendedores, o golpe pode envolver falsos comprovantes de pagamento. O golpista finge ter realizado a transferência do valor pelo produto e, em seguida, tenta apressar o envio antes que a vítima perceba que o pagamento não foi efetuado.

Em outra variação, os criminosos alegam problemas no pagamento e enviam links falsos para "resolver a questão", levando o vendedor a inserir dados bancários em sites fraudulentos.

A prevenção contra o golpe do marketplace envolve desconfiança de ofertas ou compradores que parecem bons demais para ser verdade. Nunca realize pagamentos ou envie produtos antes de confirmar a transação no ambiente seguro da plataforma, evitando transferências diretas.

Utilize métodos protegidos de pagamento, como intermediadores de crédito oferecidos pelo próprio marketplace, e verifique as avaliações de perfis antes de negociar.

COMPRA FRAUDULENTA

Marketplace não é responsável por golpe com pagamento fora da plataforma

Paulo Batistella — 30 de julho de 2024, 13h47

Consumidor

Plataformas de *marketplace* não podem ser responsabilizadas por eventuais pagamentos feitos pelo consumidor a golpistas em sistemas alheios ao delas na ocasião em que tiverem orientado, em seus termos e condições, que não deve ser feita qualquer transação por outro meio.

Golpes de Suporte Técnico Falso

Nesse golpe, os criminosos entram em contato com as vítimas, geralmente por telefone, e se passam por representantes de empresas conhecidas, como provedores de internet, fabricantes de software ou até instituições financeiras.

Eles afirmam que há um problema urgente no dispositivo ou conta da vítima e oferecem ajuda para resolvê-lo, induzindo a vítima a fornecer informações sensíveis ou a permitir acesso remoto ao computador ou celular.

O modus operandi do golpe envolve criar um senso de urgência e autoridade. Por exemplo, o golpista pode dizer que há uma falha grave de segurança no sistema ou que a conta da vítima foi comprometida e precisa de reparos imediatos.

Em muitos casos, eles solicitam que a vítima baixe um programa de acesso remoto, como TeamViewer ou AnyDesk, o que dá ao criminoso controle total sobre o dispositivo. Com esse acesso, eles podem roubar dados bancários, instalar malwares ou até transferir dinheiro diretamente de contas da vítima.

A vantagem dos criminosos nesse tipo de golpe é dupla. Primeiro, eles têm acesso a informações sensíveis que podem ser usadas para fraudes financeiras, como roubo de identidade ou compras não autorizadas.

Segundo, muitos criminosos utilizam esse acesso para instalar ransomware, sequestrando os dados da vítima e exigindo pagamento para restaurar o acesso. Além disso, em alguns casos, os golpistas cobram uma “taxa de serviço” sob o pretexto de que estão corrigindo o problema, gerando lucro direto durante a interação.

O combate ao golpe de suporte técnico falso é desafiador porque ele se baseia na engenharia social, explorando o medo e a confiança das vítimas. Para se proteger, é essencial nunca permitir acesso remoto ao dispositivo sem verificar a identidade do solicitante e desconfiar de ligações ou mensagens não solicitadas que afirmam ser de suporte técnico.

Empresas legítimas raramente entram em contato de forma proativa para resolver problemas, e qualquer solicitação desse tipo deve ser confirmada diretamente com a empresa por meio de canais oficiais. Além disso, manter sistemas atualizados e usar antivírus confiáveis reduz os riscos de vulnerabilidades exploradas nesses golpes.

Golpe da Novinha

O "golpe da novinha", também conhecido como "golpe da sextorsão", é uma prática criminosa que explora vulnerabilidades emocionais e o medo de exposição pública das vítimas.

O esquema começa com a criação de perfis falsos em redes sociais ou aplicativos de mensagens, geralmente se passando por jovens atraentes, muitas vezes menores de idade. Os golpistas iniciam conversas com o objetivo de estabelecer um vínculo emocional ou romântico, induzindo a vítima a compartilhar fotos ou vídeos íntimos.

Depois de obter o material comprometedor, os criminosos iniciam a chantagem, ameaçando expor o conteúdo às redes sociais, familiares ou colegas de trabalho da vítima. Em casos mais graves, os golpistas alegam falsamente que a vítima interagiu com uma pessoa menor de idade, aumentando a pressão psicológica.

Para evitar a exposição, as vítimas são coagidas a realizar transferências financeiras, muitas vezes via Pix ou outros métodos instantâneos.

Esse golpe é particularmente eficaz porque explora o medo e a vergonha da vítima, dificultando a denúncia às autoridades. Além disso, o uso de perfis falsos torna a identificação dos criminosos mais complexa. As consequências podem ser devastadoras, indo além do prejuízo financeiro: as vítimas frequentemente enfrentam estresse emocional, ansiedade e, em casos extremos, quadro de depressão.

Para se proteger, é essencial adotar boas práticas de segurança digital. Não compartilhe conteúdo íntimo online, especialmente com pessoas desconhecidas.

Além disso, desconfie de perfis que buscam criar vínculos rapidamente ou que pressionam por interações íntimas.

'Golpe da Novinha': casal é preso em RO suspeito de extorquir autoridades

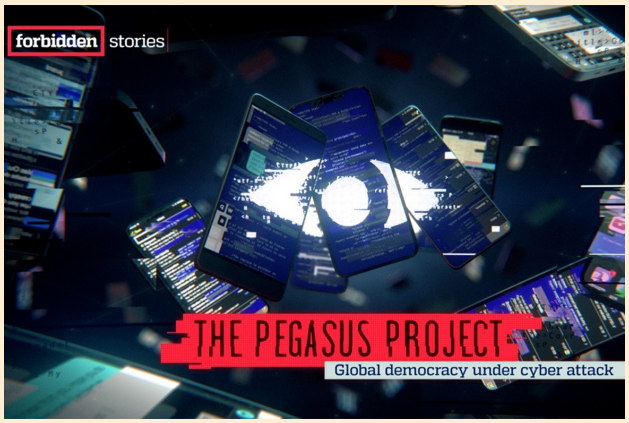
Vítimas denunciaram crime no final da última semana. Casal responsável por perfil falso em redes sociais foi preso em flagrante.

Por g1 RO

13/11/2023 18h28 · Atualizado há um ano

EXISTE 100% DE SEGURANÇA DIGITAL?

Não. As ações e as aplicações/dispositivos que empregamos para manter a segurança digital são como os muros, as câmeras, o alarme e as grades de uma casa: elas não impedem a invasão por um ladrão, apenas dificultam a ação, seja pelo tempo necessário para a obtenção do êxito, seja pela estrutura exigida para vencer os obstáculos. Existem no ambiente digital aplicações

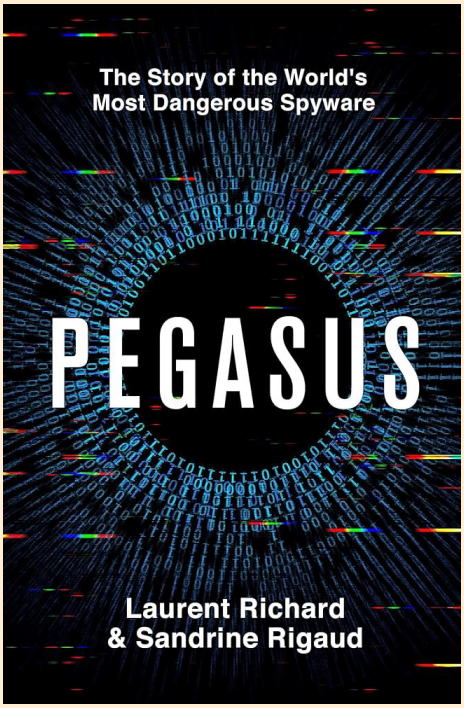


especiais capazes de superar barreiras tecnológicas significativas.

O termo **Meta 0**, ou **Zero Click Exploit**, refere-se a uma técnica avançada de ataque cibernético que permite comprometer dispositivos sem qualquer interação da vítima. Diferentemente de métodos tradicionais que dependem de cliques ou downloads, a Meta 0 explora vulnerabilidades desconhecidas (zero-day exploits) para invadir sistemas de forma silenciosa e direta, destacando-se como uma das maiores ameaças à segurança digital.

Essa abordagem ganhou destaque global devido à sua associação com o **Pegasus**, um software de espionagem desenvolvido pela empresa israelense NSO Group.

O Pegasus foi projetado para ajudar governos em investigações legítimas, como no combate ao terrorismo, mas denúncias apontaram seu uso para monitorar jornalistas, ativistas de direitos humanos e líderes políticos, frequentemente sem supervisão legal adequada.



A eficácia do Pegasus reside na sua capacidade de explorar falhas em aplicativos amplamente utilizados, como o WhatsApp e o iMessage.

Em 2019, por exemplo, ele explorou uma vulnerabilidade no WhatsApp que permitia a invasão de dispositivos apenas com uma chamada perdida, sem que a vítima precisasse atendê-la.

Essa sofisticação transformou o Pegasus em uma ferramenta de vigilância sem precedentes, capaz de acessar mensagens, chamadas, localização, câmera e microfone de forma totalmente invisível.

Os impactos são profundos: dispositivos comprometidos tornam-se instrumentos de espionagem, expondo não apenas a privacidade individual, mas também informações sensíveis de organizações e governos.

A dificuldade de detecção desses ataques, somada ao abuso documentado em diversos países, levanta preocupações éticas e jurídicas sobre o uso dessa tecnologia.

Do ponto de vista técnico, a Meta 0 representa um desafio constante para desenvolvedores de sistemas.

Como essas vulnerabilidades são desconhecidas, nem mesmo os dispositivos mais seguros, como os da Apple, estão completamente protegidos. Isso torna essencial a prática contínua de auditorias e atualizações para fechar brechas antes que sejam exploradas.

O uso do Pegasus também provoca debates sobre controle e responsabilidade. A ausência de supervisão adequada transforma uma ferramenta poderosa em uma ameaça à

liberdade e à privacidade.

A Meta 0 e o Pegasus são símbolos do potencial transformador da tecnologia – tanto para o bem quanto para o mal. Ao compreender seus riscos e possibilidades, a sociedade pode buscar um equilíbrio entre segurança e liberdade na era digital.

INTELIGÊNCIA ARTIFICIAL: O CRIME TAMBÉM AGRADECE

O avanço da inteligência artificial (IA) trouxe benefícios significativos em diversas áreas, mas também impôs desafios críticos à segurança digital.

Ferramentas baseadas em IA têm sido utilizadas por cibercriminosos para tornar ataques mais sofisticados, difíceis de detectar e mais eficazes. Este cenário exige esforços cada vez maiores para proteger sistemas e

usuários em um ambiente digital em constante evolução.

Um dos principais impactos da IA no cibercrime é a sua capacidade de personalizar ataques de engenharia social, como o phishing. Com algoritmos avançados, criminosos podem analisar grandes volumes de dados disponíveis publicamente, como perfis em redes sociais, para criar mensagens altamente direcionadas e convincentes. Isso aumenta significativamente a probabilidade de a vítima clicar em links maliciosos ou fornecer informações sensíveis, como senhas e dados bancários.

Além disso, a IA tem sido empregada para criar malwares inteligentes, que adaptam seu comportamento em tempo real para evitar a detecção por sistemas de segurança. Esses malwares podem reconhecer o ambiente em que estão operando, identificar medidas de segurança instaladas e ajustar suas ações para contorná-las. Isso torna a tarefa de defesa cibernética cada vez mais complexa, exigindo soluções igualmente sofisticadas.

Outro uso preocupante da IA no cibercrime é a criação de deepfakes, vídeos ou áudios falsificados que simulam com alta precisão a aparência ou a voz de uma pessoa. Deepfakes já foram usados em golpes de extorsão, disseminação de desinformação e até fraudes financeiras.

Por exemplo, casos em que criminosos simularam a voz de executivos para solicitar transferências bancárias urgentes demonstram como essa tecnologia pode ser usada para comprometer empresas e indivíduos.

A IA também facilita ataques automatizados em larga escala. Ferramentas alimentadas por aprendizado de máquina podem identificar vulnerabilidades em sistemas ou redes mais rapidamente do que os métodos tradicionais.

Isso permite que os criminosos lancem ataques coordenados contra múltiplos alvos em curto espaço de tempo, explorando brechas antes que possam ser corrigidas.

Além disso, a capacidade da IA de escalar operações fraudulentas representa um desafio. Bots alimentados por IA podem interagir com vítimas em tempo real, simulando diálogos humanos para enganar usuários em plataformas de suporte, comércio eletrônico ou até mesmo aplicativos bancários.

Por outro lado, a IA também está sendo usada para explorar vulnerabilidades em criptografia e autenticação. Com o poder de processamento avançado, algoritmos baseados em aprendizado de máquina podem quebrar senhas ou sistemas de autenticação, como CAPTCHAs, em questão de minutos. Isso coloca em risco até mesmo sistemas que anteriormente eram considerados seguros.

Os chamados ataques adversariais, que manipulam sistemas de IA para produzir resultados incorretos, também são uma preocupação crescente.

Cibercriminosos podem enganar sistemas baseados em IA, como filtros de conteúdo ou ferramentas de detecção de fraudes, utilizando dados projetados para induzir erros deliberados.

Diante desse cenário, a luta contra o cibercrime está se tornando uma corrida tecnológica, onde a segurança digital precisa evoluir rapidamente para acompanhar os avanços da IA.

Estratégias como o uso de IA defensiva, que aplica os mesmos princípios de aprendizado de máquina para prever e neutralizar ataques, são cada vez mais essenciais.

Além de medidas tecnológicas, é crucial investir na educação dos usuários para reconhecer ataques sofisticados facilitados pela IA, como deepfakes ou mensagens personalizadas de phishing. Apenas com uma combinação de soluções técnicas robustas e conscientização humana será possível mitigar os riscos que o avanço da IA representa para a segurança digital.

May 8, 2024

FBI Warns of Increasing Threat of Cyber Criminals Utilizing Artificial Intelligence

SAN FRANCISCO—The FBI San Francisco division is warning individuals and businesses to be aware of the escalating threat posed by cyber criminals utilizing artificial intelligence (AI) tools to conduct sophisticated phishing/social engineering attacks and voice/video cloning scams. The announcement, made today from the RSA cybersecurity conference at the Moscone Center in San Francisco, coincides with the division's outreach efforts to include an FBI booth at the conference and participation in multiple conference panel sessions during the week of May 6, 2024.

QUERO APROFUNDAR!

CLIQUE NOS LIKS PARA SABER MAIS!

Perdi o controle do meu perfil no Instagram. O que Fazer?

Como proteger o celular para ir a shows ou grandes aglomerações

Como identificar uma loja online falsa?

Curso Básico de Segurança Digital

Saiba mais sobre o Pegasus

Principais Golpes Digitais de 2024

PÍLULAS AO VIVO - PROVAS DIGITAIS (PEDRO MOURÃO)

PÍLULAS AO VIVO - POLICEWARE (SAUVEI LAI)

PÍLULAS AO VIVO - INOVAÇÃO E PROTEÇÃO DE DADOS (NEWTON MORAES)

PÍLULAS DE CULTURA

Hackers - Piratas de Computador (1995)

Hackers é um clássico cult dos anos 90 que mistura estilo, tecnologia e aventura para contar a história de um grupo de jovens hackers envolvidos em uma conspiração cibernética.

O filme segue Dade Murphy, um prodígio da computação, e seus amigos enquanto são injustamente acusados de um crime cibernético de proporções globais.

Eles descobrem que foram incriminados por um hacker mais experiente que está tentando ocultar suas próprias atividades ilegais. Com visual vibrante, trilha sonora eletrônica marcante e uma visão fantasiosa sobre o mundo digital, o filme oferece um retrato estilizado do que era percebido como hacking na década de 1990.

Ele também aborda temas que continuam relevantes, como privacidade digital, o poder da informação e as implicações éticas do uso da tecnologia.

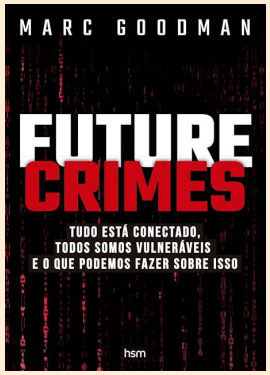
O filme é uma janela para a era inicial do ciberespaço, onde a internet ainda era um território misterioso. Seu charme e a forma como influenciou a percepção cultural sobre hackers garantem seu lugar como uma obra emblemática.

Snowden (2016)

Snowden, dirigido por Oliver Stone, é um drama biográfico que narra a trajetória de Edward Snowden, o ex-analista da NSA que expôs programas de vigilância em massa conduzidos pelo governo dos Estados Unidos.

O filme explora como Snowden, interpretado por Joseph Gordon-Levitt, passou de um patriota confiante no sistema para um denunciante perseguido, após descobrir a extensão do monitoramento realizado sobre cidadãos comuns e líderes globais. O longa equilibra cenas de suspense com momentos emocionais, apresentando o dilema moral enfrentado pelo protagonista e o impacto de suas ações em sua vida pessoal.

Snowden convida o público a refletir sobre os limites entre segurança e liberdade, levantando questões sobre o papel da tecnologia e a ética do monitoramento governamental. Embora tenha sido acusado de ser parcial em sua abordagem, o filme oferece uma perspectiva poderosa e acessível sobre um tema complexo.



Future Crimes, de Marc Goodman

O livro oferece uma análise envolvente e alarmante sobre como a tecnologia moderna está sendo explorada por criminosos para cometer novos tipos de crimes digitais.

Goodman, especialista em cibersegurança, apresenta exemplos reais e impactantes, desde fraudes online e hacks em dispositivos conectados até o uso de drones para atividades ilícitas e a criação de armas por impressão 3D.

O autor também alerta para os riscos futuros associados à Internet das Coisas, inteligência artificial e biotecnologia, destacando como essas inovações, se não reguladas, podem gerar consequências catastróficas.

Com uma abordagem acessível, o livro combina histórias reais com reflexões sobre as implicações sociais e éticas desses avanços tecnológicos. Goodman propõe soluções práticas, como maior controle sobre dados pessoais, educação digital e a implementação de políticas regulatórias para mitigar os riscos.

Future Crimes é uma leitura essencial para quem busca entender os desafios da segurança digital e a importância de antecipar ameaças em um mundo cada vez mais conectado.

Neuromancer, de William Gibson

É um marco da ficção científica que lançou as bases do gênero cyberpunk. Publicado em 1984, o livro narra a história de Case, um hacker decadente contratado por uma inteligência artificial para realizar um ousado ataque cibernético.

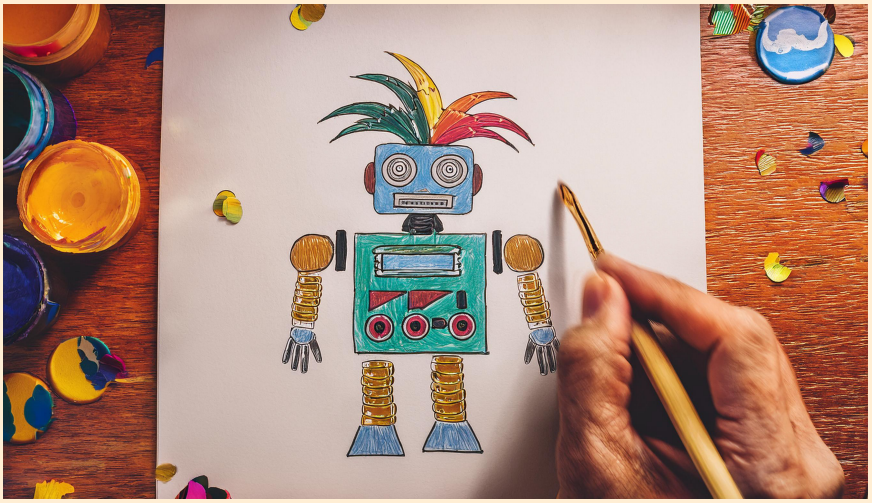
Ambientado em um futuro distópico, o romance apresenta um mundo repleto de corporações poderosas, realidades virtuais e avanços tecnológicos que moldam a sociedade. Com sua narrativa visceral e visualmente rica, Gibson introduziu conceitos como o ciberespaço e explorou temas como o impacto da tecnologia na identidade e na ética humana.

A obra é notável pela forma como combina um enredo acelerado com uma visão sombria e detalhada de um futuro hiperconectado.

Neuromancer não apenas antecipou debates sobre inteligência artificial e segurança digital, mas também influenciou profundamente a cultura pop e o imaginário tecnológico, inspirando obras como Matrix e redefinindo a relação entre humanos e máquinas.

Com sua prosa densa e inovadora, o livro é uma leitura essencial para fãs de ficção científica e para aqueles que desejam explorar as interseções entre tecnologia e sociedade.

OS INQUIETOS TAMBÉM DESCANSAM...



2024 foi um ano desafiador!

Embora tenha nascido o Núcleo de Inovação e Tecnologia, enfrentamos a maior tragédia climática do nosso estado.

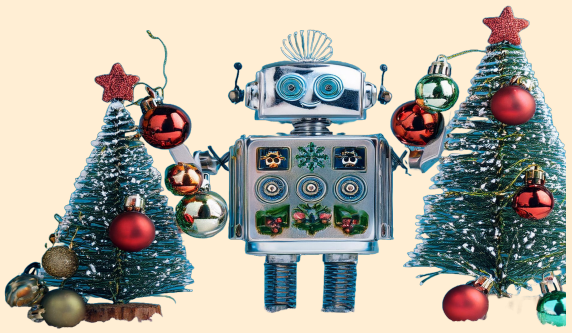
Foi preciso passar por um hiato na nossa programação até setembro, quando lançamos o Projeto Pílulas. Estamos muito felizes com a adesão dos associados ao nosso trabalho e prometemos que ano vem teremos ainda mais novidades.

Pretendemos ser ainda mais criativos nos canais de comunicação para a implantação efetiva da nossa trilha educacional de literacia digital. Acreditamos num Ministério Público do Século XXI, pronto a responder os anseios da Sociedade Digital!

Até Março!

FELIZ NATAL!

UM 2025 CHEIO DE SUCESSO E DE ALEGRIAS!



Curadoria da Edição

JÚLIA FLORES SCHUTT

MARCIO ABREU FERREIRA DA CUNHA

ROBERTO CARMAI DUARTE ALVIM JÚNIOR

osinquietosmp@gmail.com

@osinquietosmp