Carlos Vieira Teixeira

Ataques e Malwares: conheça os perigos digitais mais comuns

A Internet está cheia de perigos e golpistas que tentam enganar pessoas com diversas técnicas e práticas ilícitas. Conhecer os principais tipos de ataques ajuda a proteger seus dados e dispositivos pessoais. Cada ataque abaixo é explicado de forma simples, com exemplos práticos, casos reais e dicas de prevenção fáceis de entender.

1. Phishing (simulação de identidade)

O que é: O *phishing* é um golpe no qual criminosos fingem ser pessoas ou empresas confiáveis para "pescar" suas informações pessoais. Eles enviam e-mails, SMS ou mensagens falsas com links ou anexos maliciosos. O nome *phishing* vem da ideia de "pescar" vítimas com uma isca atraente, do mesmo modo que pescadores usam iscas para fisgar peixes .

Exemplo/analogia: Imagine receber um e-mail que parece ser do seu banco pedindo para atualizar a sua senha. O link leva a um site falso que rouba seus dados – isso é *phishing*.

Caso real: Em 2016, hackers russos criaram um e-mail falso de redefinição de senha (um *phishing*) e enganaram a equipe da campanha da candidata a presidência dos Estados Unidos, Hillary Clinton. Com isso, roubaram milhares de e-mails confidenciais .

Como se proteger: Não clique em links ou abra anexos de e-mails suspeitos. Verifique sempre o remetente e desconfie de mensagens urgentes demais. Use filtros anti-spam e esteja atento: empresas sérias não pedem senha por e-mail. Não forneça informações pessoais. Use os protocolos de segurança para e-mails. Métodos de autenticação de e-mail, como registros SPF, DKIM e DMARC, ajudam a confirmar a origem da mensagem. Os proprietários de domínio podem configurar esses registros para dificultar que os invasores imitem seus domínios em um ataque de falsificação de domínio.

2. Malware

O que é: *Malware* é todo software feito para “infectar” seu computador, celular ou uma rede sem que você saiba. Ele pode danificar dispositivos, roubar dados ou assumir o controle do aparelho. Em suma, é como um vírus no mundo digital: entra no sistema e causa problemas .

Exemplo/analogia: Pense no *malware* como um germes ou parasita: entra sorrateiramente no seu corpo (computador) e se multiplica, causando doença (lentidão, travamentos) e passando informações para o atacante. Trojan, vírus e worm são tipos de malware com jeitos diferentes de agir.

Caso real: Um famoso exemplo é o verme *WannaCry* (2017), que infectou milhões de computadores no mundo todo, bloqueando seus arquivos até que vítimas pagassem resgate. Empresas e hospitais ficaram sem acesso a dados importantes, mostrando o dano que um *malware* pode causar.

Como se proteger: Instale antivírus e mantenha o sistema operacional atualizado. Não baixe arquivos ou aplicativos de fontes desconhecidas. Faça backups regulares dos seus dados para restaurá-los caso sejam criptografados ou apagados por *malware*. Evite usar dispositivos USB de procedência duvidosa. Manter programas sempre na versão mais recente reduz riscos de infecção.

3. Ransomware

O que é: O *ransomware* é um tipo de *malware* que “sequestra” seus arquivos e/ou dados, criptografando-os e exigindo pagamento (resgate) para liberá-los. Funciona como se alguém trancasse todos os seus pertences em um cofre e só devolvesse quando você pagasse. O pagamento geralmente é em criptomoedas (como Bitcoin) para dificultar rastrear o criminoso.

Exemplo/analogia: Imagine invadirem sua casa e prenderem todos os documentos importantes em cofres trancados, exigindo dinheiro para entregar a chave. No computador, o efeito é o mesmo: fotos, documentos e arquivos ficam inacessíveis até você pagar o resgate.

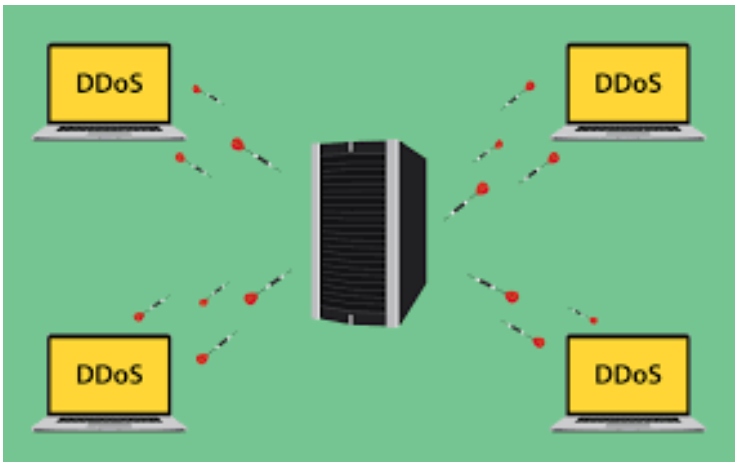
Caso real: Em setembro de 2020, um hospital em Düsseldorf (Alemanha) foi vítima de *ransomware*. O ataque paralisou os sistemas de emergência, forçando transferir um paciente grave para outro hospital. Infelizmente, devido ao atraso no atendimento causado pelo ataque, o paciente morreu . Esse foi o primeiro caso documentado de morte ligada a um ciberataque.

Como se proteger: Tenha backups sempre atualizados e fora da máquina principal (por exemplo, em disco externo desconectado ou nuvem segura). Não abra anexos ou links de remetentes desconhecidos, pois esse é o método mais comum de infecção. Mantenha programas e sistema operacional atualizados e use boas soluções de segurança (antivírus, *firewall*). Se receber mensagem suspeita (por exemplo, falsos pedidos de pagamento ou atualizações), confirme diretamente no site oficial ou por telefone.

4. DdoS (Ataque de Negação de Serviço)

O que é: Em um ataque (DdoS - *Distributed Denial of Service*), no qual os criminosos sobrecarregam um site ou servidor com inúmeras de requisições falsas, tornando-o lento ou totalmente fora do ar . É como um congestionamento provocado de propósito: muita gente tenta acessar um site ao mesmo tempo, e o site não consegue responder a todos.

Exemplo/analogia: Imagine uma loja com apenas uma porta atendendo clientes. Se mil pessoas tentam entrar de uma vez, a porta fica travada e ninguém entra direito. No ciberespaço, milhares de computadores (geralmente parte de uma *botnet*) enviam requisições ao alvo para deixá-lo inacessível.



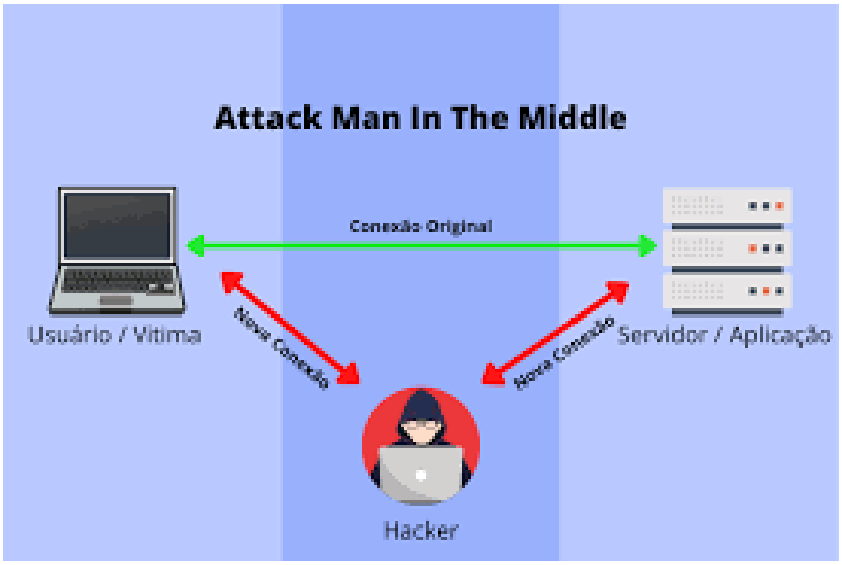
Caso real: Em 2016, um grande ataque DDoS atingiu o serviço DNS da Dyn, derrubando sites populares como Twitter, Netflix e Spotify por horas. Ninguém invadiu as contas, mas os serviços ficaram inacessíveis para milhões de usuários.

Como se proteger: Empresas utilizam redes distribuídas (CDNs), firewalls e servidores em nuvem que absorvem picos de tráfego. Para usuários, não há muito o que fazer diretamente além de entender que, se um site está fora do ar por conta de DDoS, é por notivos de ataques. Em geral, usar provedores confiáveis ajuda a reduzir a chance de ataque.

5. Main in the Middle (Homem no Meio)

O que é: Nesse ataque, o invasor se insere secretamente na comunicação entre você e um serviço online ou uma rede Wi-Fi, “escutando” ou modificando o que vocês fazem sem perceber. O criminoso fica no meio da conexão, daí o nome “homem no meio”.

Exemplo/analogia: É como se alguém estivesse interceptando suas cartas antes de entregá-las e lendo o conteúdo sem seu conhecimento. Outro exemplo, você acessa seu banco pelo Wi-Fi do café, mas um hacker criou um ponto de Wi-Fi falso. Ele intercepta seus dados de *login* enquanto aparenta passar tudo para o site do banco.



Caso real: A Equifax, uma das maiores empresas de crédito dos EUA, sofreu uma violação de dados que expôs informações pessoais de mais de 147 milhões de pessoas. Embora o ataque tenha envolvido múltiplas falhas de segurança, uma das técnicas utilizadas foi a interceptação de tráfego entre usuários e servidores, característica de um ataque de *Main in the Middle*.

Prevenção: Sempre confira se o site usa HTTPS (cadeado na barra do navegador). Evite redes Wi-Fi públicas abertas sem senha; prefira usar VPN. Manter seu antivírus e *firewall* ativos também ajuda a bloquear esses ataques.

6. Injeção de SQL

O que é: Um ataque de injeção SQL explora falhas em sites ou sistemas que usam banco de dados. O invasor insere código malicioso em campos de entrada (como formulários) para que o banco execute comandos indesejados. Basicamente, o criminoso “injeta” código SQL na aplicação para ler ou alterar dados privados no banco de dados.

Exemplo/analogia: Imagine um questionário onde, além de responder normalmente, você consegue escrever instruções secretas que o sistema executa. É como pedir informação em uma biblioteca (site), mas alguém consegue colocar um pedido oculto no livro que rouba mais dados.

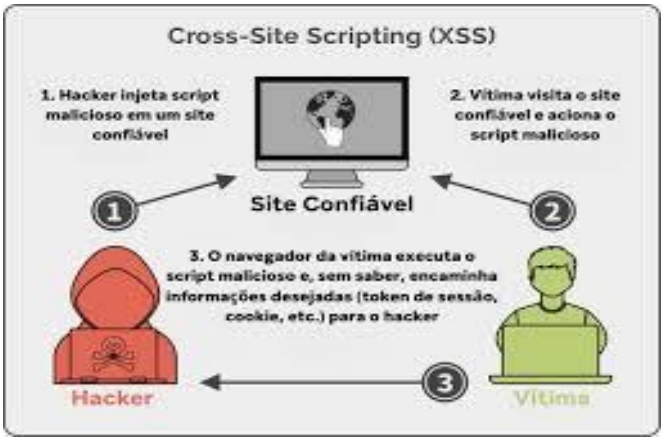
Caso real: Em 2015, a operadora britânica TalkTalk sofreu um ataque de injeção SQL. Hackers conseguiram acessar o banco de dados e roubaram dados de muitos clientes. A empresa acabou pagando multa grande pelo vazamento.

Como se proteger: Quem desenvolve sites deve sempre filtrar e validar todas as entradas de usuários para remover códigos (especialmente algo parecido com código SQL). Técnicas como consultas parametrizadas (*prepared statements*) ou uso de *firewall* de aplicações web podem bloquear injeções. Para usuários finais, não há ação específica, mas o ideal é navegar em sites confiáveis e ter senhas fortes, pois ataques assim visam falhas do site, não do usuário.

7. Cross-Site Scripting (XSS)

O que é: No XSS, o invasor insere *scripts* (código) malicioso em sites legítimos. Quando você visita uma página comprometida, esse código é executado no seu navegador como se fosse parte do site, permitindo roubar dados (como *cookies* de sessão) ou tomar controle do que aparece na tela.

Exemplo/analogia: É como alguém desenhar uma armadilha em um mapa de cidade. O site é o mapa confiável, mas o hacker desenha um atalho secreto que te leva para outro lugar (site malicioso). Por exemplo, em um site de compras, um criminoso pode injetar um código no campo de comentários, toda vez que alguém abre aquela página, o código envia os dados de *login* do visitante para o hacker .



Caso real: Imagine clicar num link compartilhado nas redes sociais que leva a um site de notícias. Você vê o site normalmente, mas um *script* oculto no site captura seus *cookies* de *login* e os envia ao invasor. A vítima nem percebe nada errado. Muito comum esse tipo de ataque.

Como se proteger: Sites devem filtrar e remover *scripts* de entradas de usuários. Manter todo o software do site atualizado fecha várias brechas. Como usuário, desconfie de links estranhos em e-mails e em redes sociais. Use navegadores modernos atualizados e extensões que bloqueiam *scripts* de fontes desconhecidas.

8. Ataque de força bruta (quebra de senha)

O que é: No ataque de força bruta, o criminoso tenta todas as combinações possíveis de senha até achar a certa. É um método antigo, mas ainda eficaz quando as senhas são fracas. É como um ladrão tentando arrombar um cadeado testando chave após chave até encontrar a certa.

Exemplo/analogia: Pense em um cadeado de 6 dígitos: o hacker usa um programa que experimenta "000000, 000001, 000002, …" sem parar até acertar. Com computadores poderosos, até muitas combinações podem ser testadas rapidamente.

Caso Real: Houve um caso no Brasil envolvendo senhas fracas no sistema do Conselho Nacional de Justiça (CNJ), revelado em 2023 durante a CPI dos Atos Golpistas. Quem revelou foi o hacker Walter Delgatti Neto, conhecido como o "hacker de Araraquara". Em depoimento à CPI, Delgatti afirmou que conseguiu acessar sistemas do CNJ usando senhas extremamente simples, como: **`123mudar`, `CNJ123`,`123452`,** entre outras. Segundo Delgatti, após analisar o código dos sistemas por cerca de três meses, encontrou credenciais que permitiram acesso à intranet do CNJ. O objetivo era criar um falso mandado de prisão contra o ministro Alexandre de Moraes, como parte de um plano político para desacreditar o sistema judiciário e tentar anular o resultado das eleições. O caso expôs a fragilidade da segurança cibernética em órgãos públicos e gerou forte repercussão política e institucional. Esse episódio é um exemplo claro de como senhas fracas podem ser exploradas por meio de ataques de força bruta ou simples tentativa e erro, sem necessidade de técnicas sofisticadas.

Como se proteger: Use senhas longas e complexas (letras maiúsculas, minúsculas, números e símbolos). Não use palavras óbvias como "senha123". Sempre ative a autenticação em dois fatores (2FA) quando possível, assim, mesmo que invadam sua senha, ainda precisarão de outro código extra. Sistemas podem limitar tentativas de *login*, bloqueando contas após algumas tentativas falhas. Nunca reutilize senhas em vários sites.

9. Engenharia Social

O que é: Engenharia social não é um ataque técnico, mas sim uma forma de manipular pessoas. Aqui, o inimigo explora a confiança, curiosidade ou medo da vítima para obter dados confidenciais ou acesso a sistemas. Os exemplos mais comuns são golpes por telefone, e-mail ou mesmo pessoalmente com a vítima, momento que o hacker finge ser alguém confiável e amigável buscando obter informações valiosas da vítima.

Exemplo/analogia: Já ouviu falar do golpe do "parente no hospital"? Alguém liga fingindo ser seu parente e pedindo dinheiro para remédio urgentemente? Essa pessoa desconhecida conseguiu informações suas como nome de familiares pelas redes sociais e usou a engenharia social para encontrá-las. Da mesma forma, um hacker pode fingir ser do suporte técnico pedindo sua senha ou acesso e tantas outras situações análogas que são comuns por parte dos atacantes contra vítimas.

Caso Real: Um exemplo real e marcante de ataque de engenharia social aconteceu com a empresária Barbara Corcoran, jurada do programa *Shark Tank*, em 2020. Um cibercriminoso se passou por uma assistente de Barbara e enviou um e-mail ao contador dela solicitando o pagamento de uma fatura de quase US$ 400.000. O golpista usou um endereço de e-mail quase idêntico ao da assistente real e incluiu detalhes plausíveis sobre investimentos imobiliários. O golpe só foi descoberto depois que o contador respondeu ao e-mail verdadeiro da assistente perguntando sobre a transação

Como se proteger: Desconfie de contatos inesperados. Não forneça senhas ou códigos a ninguém que você não conheça bem. Confirme pedidos urgentes por outro meio (por ex., ligue diretamente para quem supostamente pediu ajuda). Não clique em anúncios chamativos de ofertas imperdíveis. Ative autenticação multifator (2FA) sempre que possível para proteger contas.

10. Dia Zero (Zero-Day)

O que é: Um ataque “Dia Zero” explora uma falha de segurança desconhecida pelo fabricante do software ou equipamento. No caso do software, os desenvolvedores têm “zero dias” para corrigir, pois os hackers descobriram a falha antes da atualização existir . É o tipo de ataque mais difícil de detectar e prevenir, já que não há *patch* ou solução oficial no momento do ataque.

Exemplo/analogia: Imagine que a fechadura da sua casa tem um ponto fraco secreto que só os ladrões conhecem. Até o fabricante da fechadura descobrir e fazer um novo modelo, qualquer um com a informação certa pode entrar.

Caso Real: O Stuxnet foi um *malware* altamente avançado descoberto em 2010, projetado especificamente para sabotar as centrífugas de enriquecimento de urânio do Irã. Ele visava sistemas industriais controlados por controladores lógicos programáveis (PLCs) da Siemens, usados em instalações nucleares. O Stuxnet explorou quatro vulnerabilidades zero-day no Windows e uma no software da Siemens. Essas falhas permitiram que o *malware* se espalhasse nos sistemas.

Como se proteger: Mantenha o sistema operacional e aplicativos sempre atualizados assim que houver correções. Embora o *patch* não exista antes do ataque de dia zero, os desenvolvedores costumam lançar atualizações logo em seguida. Habilitar atualizações automáticas é a melhor forma de fechar as brechas rapidamente. Ferramentas de segurança modernas (que usam inteligência artificial) podem identificar

comportamentos suspeitos mesmo sem um *patch* específico. Em suma, quanto mais vigilante (atento a atualizações e a notícias de segurança) você for, menor é o tempo em que fica vulnerável.

Conclusão

A Internet é cheia de riscos, mas você pode ficar muito mais seguro seguindo boas práticas simples. Use senhas fortes e únicas para cada site e prefira senhas geradas automaticamente. Ative a autenticação em dois fatores sempre que disponível. Mantenha o sistema e programas do computador/ celular sempre atualizados. Tenha antivírus confiável ativado e faça backups regulares dos seus arquivos importantes. Desconfie de ofertas ou mensagens milagrosas: se parecer mentira, provavelmente é cilada. Educar-se e ensinar aos outros (escola, família, amigos) sobre esses perigos é fundamental. Com cuidado, prudência e conhecimento, é possível navegar na rede com tranquilidade. Cada ataque tem seus truques, mas as defesas básicas (atenção, atualização e backups) ajudam contra quase todos. Estar informado é a melhor arma contra cibercriminosos. Tenha bons hábitos digitais no dia a dia e incentive outros a fazer o mesmo para uma um uso da Internet mais segura!

Tipo de Ataque	Risco Principal	Como se Proteger
Phishing	Roubo de dados e senhas	Verificar remetente, não clicar em links duvidosos
Malware (vírus, trojans)	Danos ao sistema, roubo de informações	Usar antivírus, atualizações em dia, não baixar arquivos suspeitos
Ransomware	Criptografia de arquivos e extorsão financeira	Ter backups offline, evitar anexos desconhecidos
DDoS (Negação de Serviço)	Serviço/site fica indisponível	Usar firewalls, serviços em nuvem/CDN que absorvem tráfego

Tipo de Ataque	Risco Principal	Como se Proteger
Man-in-the-Middle	Interceptação de dados confidenciais	Usar HTTPS/VPN, evitar Wi-Fi público, manter antivírus
SQL Injection	Vazamento de base de dados (clientes, senhas etc.)	Desenvolver sites com consultas parametrizadas, filtrar entradas
XSS (Cross-Site Scripting)	Roubo de sessão/cookies e dados do usuário	Não clicar em links suspeitos, usar sites atualizados
Força Bruta (senha)	Conta invadida	Senhas fortes e únicas, bloqueio após várias tentativas
Engenharia Social	Informação pessoal entregue ao invasor	Desconfiar de pedidos urgentes, confirmar via outro canal, usar 2FA
Dia Zero	Exploração de vulnerabilidade desconhecida	Atualizar sistemas automaticamente, usar soluções de segurança avançadas

O que é phishing? |

IBM https://www.ibm.com/br-pt/think/topics/phishing

O que é malware? Definição, Tipos, & Exemplos

https://www.veeam.com/pt/glossary/what-is-malware.html

Um paciente morreu após ataques hackers de ransomware a um hospital da Alemanha - MIT Technology Review

https://mittechreview.com.br/um-paciente-morreu-apos-ataques-hackers-de-ransomware-a-um-hospital-da-alemanha/

Como se proteger de ransomware

https://www.kaspersky.com.br/resource-center/threats/how-to-prevent-ransomware

O que são ataques DDoS e como evitá-los?

https://support.hostinger.com/pt/articles/5634639-o-que-sao-ataques-ddos-e-como-evita-los

O que é ataque man in the middle (MITM)? | IBM

https://www.ibm.com/br-pt/think/topics/man-in-the-middle

Man-in-the-middle: O que é e 3 dicas para se proteger | Blockbit

https://www.blockbit.com/pt/blog/ataque-man-in-the-middle-o-que-e-e-3-dicas-para-se-proteger/

Injeção de SQL e como evitá-la

https://www.kaspersky.com.br/resource-center/definitions/sql-injection

O que é injeção de SQL?Riscos, exemplos e como evitá-los

https://www.datacamp.com/pt/tutorial/sql-injection

O que é um ataque Cross-Site Scripting? Definição e Exemplos

https://www.kaspersky.com.br/resource-center/definitions/what-is-a-cross-site-scripting-attack

Ataque de força bruta: definição e exemplos

https://www.kaspersky.com.br/resource-center/definitions/brute-force-attack

Engenharia social: o que é e como se proteger

https://www.claranet.com/br/blog/engenharia-social-o-que-e-e-como-se-proteger

Explorações e ataques de dia zero

https://www.kaspersky.com.br/resource-center/definitions/zero-day-exploit

O que é Ataque de Dia Zero?

https://www.checkpoint.com/pt/cyber-hub/threat-prevention/what-is-zero-day-attack/

Hacker afirma à CPI que uma das senhas do sistema do CNJ era '12345'; deputada diz que era 'senha simples'

https://g1.globo.com/politica/noticia/2023/08/17/hacker-afirma-a-cpi-que-uma-das-senhas-do-sistema-do-cnj-era-12345-deputada-diz-que-era-senha-simples.ghtml