De Antivírus a Exploração de dia zero:

20 termos de cibersegurança que você precisa conhecer

NordVPN®

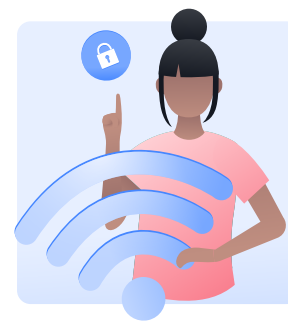
“

A cibersegurança afeta tudo o que fazemos online e agora, mais do que nunca, a vida online se tornou a vida normal. Por extensão, as ameaças à segurança cibernética são ameaças aos nossos meios de subsistência e nos educar é essencial para proteger o nosso bem-estar. Todo mundo se beneficia com a compreensão dos princípios básicos, e é por isso que é importante que todos nós entendamos os termos de segurança cibernética de A a Z.

Troy Hunt

Troy Hunt – Membro do Conselho Consultivo da NordVPN, diretor regional da Microsoft e ganhador do prêmio Microsoft Most Valuable Professional como Desenvolvedor em Segurança, blogueiro no site troyhunt.com, palestrante internacional sobre segurança da web e autor de muitos cursos de segurança de primeira linha para desenvolvedores da web na Pluralsight.

Table of contents:



Prefácio

Se você está dando seus primeiros passos no reino da cibersegurança, este é o lugar para se começar. Para explicar o motivo disso, vamos ver como as coisas realmente funcionam.

Suponha que você se depare com a palavra spyware e deseje saber o que ela significa. No momento em que você começar a pesquisar, você será atacado por termos que nunca ouviu antes. Você poderá encontrar uma definição assim:

> Spyware é um tipo de malware que monitora o dispositivo da vítima para extrair dados sensíveis sem o conhecimento dela. Exemplos de spyware: adware, keyloggers e trojans.

Essa é uma definição precisa, mas não muito útil. Agora você tem mais perguntas. Como um spyware funciona? O que são considerados dados sensíveis e quão preocupado você deveria estar sobre a segurança deles? O que é um keylogger? Isso é uma palavra de verdade?

Vamos adotar uma abordagem diferente.

Em vez de dar definições técnicas, vamos mostrar como a cibersegurança afeta sua vida e fornece comparações realistas. Este não é um glossário completo, e isso é intencional. Ele foi feito para estimular seu apetite por mais aprendizagem.

Se você estiver procurando explicações técnicas mais detalhadas sobre todas as coisas relativas à segurança online, visite nosso blog em nordvpn.com/pt-br/blog, no qual você encontra conteúdos populares e aprofundados.

Antivírus

Você recebeu um novo e-mail. Assunto: **Eu te amo.**

Nele, você encontra uma bela confissão de amor de um admirador anônimo. E há uma foto também. Curioso, você clica no anexo — e baixa um vírus.

Seu antivírus o coloca em quarentena imediatamente. Você teve sorte — era um vírus antigo, o registro dele já estava no banco de dados.

Se o vírus for novo e não estiver registrado no banco de dados, o antivírus pode usar outras ferramentas para detectá-lo. Ele monitora seu computador em busca de atividades suspeitas. Se um programa tentar burlar o antivírus e for executado na inicialização sem permissão ou baixar outro malware, o antivírus reage.

E não existem apenas vírus. Há todo tipo de software malicioso — trojans, ransomware, keyloggers, etc. — que tentam comprometer ou abusar dos seus dispositivos.

Hoje, a palavra “antivírus” representa todos os tipos de ferramentas antimalware que protegem os dispositivos contra malwares.

Termos relacionados: vírus, malware, software antimalware, trojan, worm, adware.

B

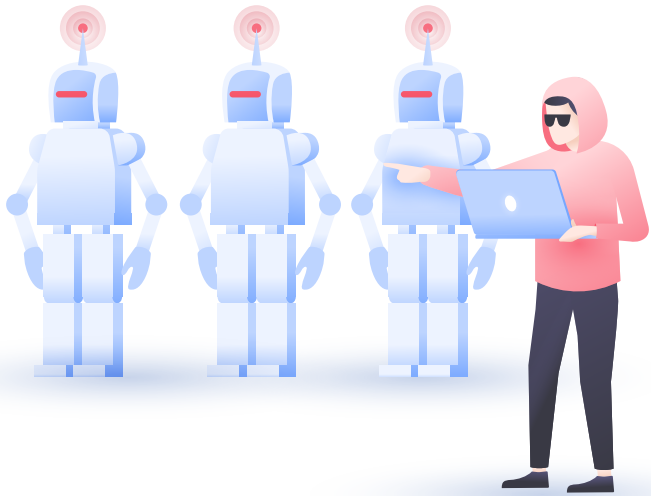
Botnet

Você abre o navegador e digita o endereço do seu site de meme favorito. Ugh, ele caiu. E você nunca vai adivinhar a causa.
São zumbis.

Bots, para ser mais exato. Um enxame de dispositivos irracionais e infectados enviou centenas de milhares de solicitações ao site e o sobrecarregou.

Esse ataque é chamado de DDoS, que se traduz como “negação de serviço distribuída”. As pessoas usam botnets para esse e outros fins nefastos, como envio de spam por e-mail ou criação de tráfego de Internet falso.

Seus dispositivos também podem fazer parte de um botnet, respondendo secretamente aos comandos do cibercriminoso. É difícil saber se o seu computador é um bot — o único sinal pode ser um desempenho um pouco inferior ou a ocorrência de superaquecimento.



Termos relacionados: bot, zumbi, ataque DDoS.

C

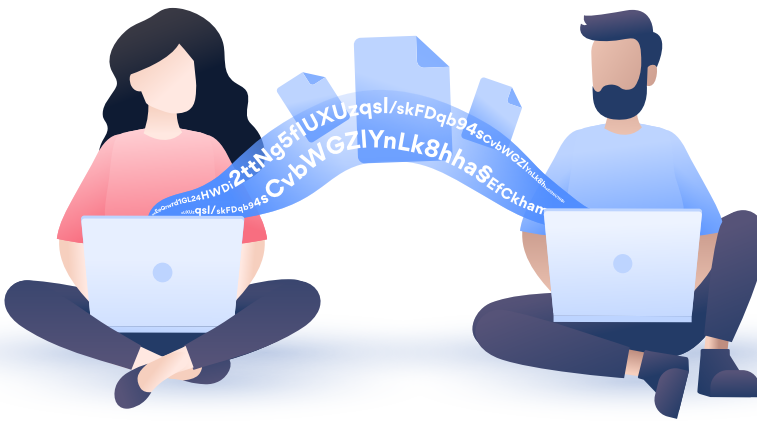
Texto Cifrado (Ciphertext)

Você abre um aplicativo de mensagens e envia uma mensagem de texto: "DESCULPE, PESSOAL, não posso ir esta noite. Provavelmente peguei uma infecção estomacal".

Isso é o que chamamos de um texto simples. É um texto não criptografado que pode ser interceptado e lido por um espião online. Ele é também o que chamamos de mentira — afinal, você se sente bem, mas prefere assistir a um filme. Pelo menos você está usando um aplicativo de mensagens seguro. Ele aplica um algoritmo para transformar sua desculpa em um texto cifrado:

> "ueEeQrwrd1GL24HWDi2ttNg5fIUXUzqsIFqb94^Ef2NU1NBrD
> rPb84wbReVnclTP2AgnMCkhaHC3UrfR8VWxh3jWWh+0WE"

Isso é a criptografia em ação. O texto simples é transformado em texto cifrado por meio de uma chave segura (uma cifra). Os aplicativos de mensagens que seus amigos usam têm a chave que decifra suas mensagens. Espiões online não têm a chave e, portanto, não podem ler suas conversas.



Termos relacionados: criptografia, cifra, texto simples, decifrar

D

Violação de dados

Você tem uma conversa em grupo com vários dos seus amigos mais próximos. Um dia, você percebe capturas de tela da conversa circulando por todas as redes sociais. Você acaba de vivenciar uma violação de dados.

Uma violação de dados acontece quando dados sensíveis caem nas mãos de alguém que não tinha o direito de lidar com eles.

Como isso aconteceu? Um hacker interceptou suas comunicações? Ou foi um trabalho interno? Talvez o colega de quarto de Marcos acessou a conversa enquanto Marcos estava longe do laptop. Ele sempre pareceu estranho. Mas você provavelmente nunca descobrirá a causa.

É isso o que também acontece nas principais violações de dados corporativos.

As empresas coletam grandes quantidades de dados, às vezes dados de usuários como você e algumas dessas empresas são violadas, os dados vazam e você vê seus logins e senhas flutuando pela web.

Verifique periodicamente se suas contas foram comprometidas em uma violação de dados no site haveibeenpwned.com.

Termos relacionados: divulgação não intencional de informações, vazamento de dados, roubo de dados.

E

Criptografia de ponta a ponta

Você já deve ter ouvido as companhias falarem em um tom alegre: “Vamos implementar criptografia de ponta a ponta!”. O que há de tão inovador nisso? A criptografia de ponta a ponta elimina a necessidade de um intermediário. Somente você e a pessoa para quem a mensagem está endereçada podem ver seu conteúdo.

Pense em seus dados como uma nota de papel. Antes de enviá-la, você a coloca em um envelope, que protege seu conteúdo de bisbilhoteiros. Isso é criptografia.

Em algum lugar ao longo do caminho, um terceiro (por exemplo, o serviço de mensagem instantânea que você está usando) abre o envelope, retira seus dados e os envia para o destino final.

É assim que a internet funciona, existem intermediários em todo o caminho.

A criptografia de ponta a ponta elimina a necessidade de um intermediário. Somente você e a pessoa para quem a mensagem está endereçada podem ver seu conteúdo.

Termos relacionados: texto cifrado, texto simples.

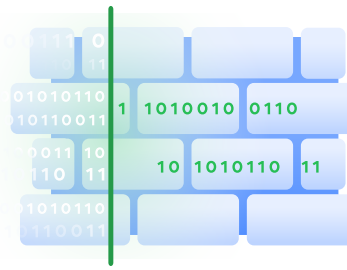
F

Firewall

Você está em uma fila. Quando você alcança o segurança, ele diz: “Você não pode entrar”. Você dá meia volta e retorna para casa, nada de balada hoje.

O segurança impõe as regras sobre quem entra ou não na boate. Essas regras são arbitrárias, elas dependem das políticas da boate e das circunstâncias externas. Por exemplo, a boate estar lotada ou estar organizando uma festa particular.

Na mesma linha, um firewall fica entre sua rede local e a Internet. Como um segurança digital, ele impõe as regras a respeito de qual tráfego é bom o suficiente para entrar na rede.
Um firewall permite o tráfego vindo de fontes ou endereços IP confiáveis. Não está na lista? Desculpe, tráfego, dê meia volta e vá para casa. É assim que um firewall protege sua rede de tráfegos maliciosos da Internet que podem comprometer seu sistema.



H

Hacker

Você os conheceu em filmes. Misteriosos, perigosos, até antissociais. Eles são criminosos digitais que vivem fora da rede. Eles invadem o Pentágono em menos de 5 minutos.

Isso é claramente ficção. Hackers são pessoas e cada pessoa tem seus motivos. Alguns gostam do desafio intelectual de entrar em redes. Outros, os chamados black hat hackers, agem com malícia. Eles comprometem os sistemas para ganho pessoal, roubam dados valiosos ou dinheiro, interrompem redes e podem causar todos os tipos de danos.

Muitas empresas e governos empregam white hat hackers, que testam a segurança de seus sistemas de computador ao tentar invadi-los. Isso é chamado de teste de intrusão, que pode assumir várias formas, até mesmo físicas.

Por exemplo, um white hat hacker pode entrar no prédio da empresa seguindo um funcionário. As pessoas são educadas, geralmente mantêm as portas abertas para as outras, até mesmo para estranhos. Uma vez lá dentro, o hacker pode roubar discos rígidos com dados confidenciais, acessar computadores não supervisionados ou comprometê-los (com keyloggers, por exemplo).

Você pode ser hackeado?

Depende das suas medidas de segurança. No entanto, hackers extremamente habilidosos costumam encontrar uma forma de entrar até mesmo nas redes mais seguras. A boa notícia é que eles provavelmente têm alvos mais interessantes em mente do que sua conta na Steam.

Normalmente, você sofre com os hackers indiretamente, veja: violação de dados.

Você deve ter cuidado com os golpistas que criam sites falsos e enviam links maliciosos, veja: phishing. Digite sua senha em um site de golpes e você estará fornecendo-a diretamente para o golpista.

Termos relacionados: grey hat hacker, black hat hacker, white hat hacker, intrusão, teste de intrusão.

1

Endereço

Seu telefone possui um endereço IP (abreviação de endereço de protocolo de internet) atribuído pela sua rede. O mesmo acontece com seu laptop, smart TV e todos os outros aparelhos que se conectam à Internet. Nenhum dispositivo poderia funcionar online sem um.

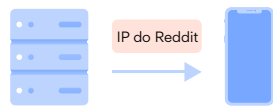
Por quê?

Digamos que você precise matar algum tempo. Você pega o telefone e digita “Reddit.com” na barra de endereço.

Mas seu telefone não sabe o que “Reddit.com” significa. O idioma nativo dele é composto por números, não palavras. Para acessar o Reddit, seu telefone envia uma pergunta:

Qual é o endereço IP do Reddit.com?

A questão é dirigida a um servidor especial, um banco de dados de endereços IP. O servidor encontra o IP do Reddit e o envia de volta para o seu telefone.



Solicitação

Seu telefone então envia a solicitação para o endereço IP do Reddit. O Reddit envia de volta as informações para o IP do seu telefone.

Dado de IP do Reddit

Um segundo se passa. O Reddit é carregado na tela. Nada desperta seu interesse, você aperta o botão Fechar.

J

Cryptojacking

Seu computador está quente e zumbindo, o ventilador está girando como um louco. E ele está lento, você tem que esperar alguns instantes antes que qualquer coisa carregue.

O motivo? Um hacker sequestrou seu computador para extrair criptomoedas.

Você provavelmente já ouviu falar de criptomineração (criptomining). Para simplificar, trata-se de quando você recebe criptomoedas como recompensa por executar cálculos complexos em seu computador. Mas esses cálculos consomem muito poder do computador, geralmente uma quantidade de poder enorme para que a criptomineração seja lucrativa.

Para resolver esse problema, os hackers sequestram dispositivos para extrair criptomoedas para eles. Eles realizam esse ataque chamado de cryptojacking usando um malware ou um código malicioso em páginas da web. As vítimas desavisadas ficam se perguntando por que seu computador está em brasa com superaquecimento.

P.S. Sim, nós sabemos que colocar cryptoJacking sob a letra J no índice é trapacear. Mas a letra J é um deserto vazio em termos de cibersegurança, então nós aproveitamos dela.

Termos relacionados: criptomineração, criptomineração maliciosa.

K

Keylogger

Você está na biblioteca, escrevendo um artigo para sua aula de economia. O prazo era ontem. A bateria do seu laptop acabou, e você deixou o cabo em casa.

Uma garota de aparência amigável está sentada ao seu lado. Então pede o laptop dela, você precisa de 5 minutos para terminar o pensamento enquanto ele ainda está borbulhando em sua cabeça. Ela fica feliz em ajudar. Você pega o laptop dela, conecta-se ao seu drive na nuvem e termina a crítica às políticas antitruste da Crise de 1929.

Ao voltar para casa, você descobre que seu e-mail e muitas de suas contas online foram hackeadas. Como?

A garota tinha um keylogger instalado em seu laptop. É uma ferramenta que registra as teclas digitadas. Ele gravou tudo o que você digitou, incluindo sua senha e login da unidade em nuvem.

Como você usa a mesma senha para o drive na nuvem e para o e-mail, o hacker obteve acesso à sua conta de e-mail principal (é por isso que você não deve reutilizar senhas). Com ele, o hacker redefiniu as senhas de suas outras contas.

Os keyloggers raramente vêm de garotas de aparência amigável. Normalmente, eles assumem a forma de dispositivos de hardware que os hackers anexam a computadores não supervisionados. Eles também podem ser ferramentas de software, usadas ilegal ou legalmente. Por exemplo, algumas empresas instalam keyloggers em seus computadores para monitorar seus funcionários.

Termos relacionados: spyware.

L

Bomba lógica

Você está no trabalho, cinco minutos depois de um prazo. Você está digitando furiosamente quando tudo cai. Você não consegue acessar a rede interna ou qualquer arquivo remoto. Não há mais trabalho hoje.

No dia seguinte, você ouve rumores. Foi um ex-funcionário, um cara de TI descontente, ele desligou a rede interna. Mas como pode ser isso? Ele foi demitido há meio ano e não tinha mais acesso aos sistemas da empresa.

Bem, em seu último dia de trabalho, ele deixou uma bomba lógica. É um código malicioso que é ativado quando certas condições são atendidas. Por exemplo, quando o CEO se conecta a um sistema confidencial. Uma bomba lógica pode ter efeito em uma data específica, como aconteceu em nossa história quando a bomba lógica explodiu meio ano depois de ser montada.

Termos relacionados: bomba-relógio, ameaça interna

Ataque man-in-the-middle

Você está em uma cafeteria, conectado ao Wi-Fi público. Você acabou de enviar um e-mail ao seu empreiteiro, solicitando o número da conta bancária dele. Você pega o número, paga a taxa e bebe seu café com creme.

Dois dias depois, o empreiteiro liga para você com uma pergunta: “Quando vou receber o pagamento?”

O quê?

Flashback para a cafeteria. Um hacker chegou ao café antes de você, configurou um ponto de acesso evil twin e o nomeou de “Wifi GRÁTIS da Cafeteria”. Acreditando que era uma rede legítima, você se conecta a ela. A partir desse momento, o hacker pode monitorar seu tráfego na internet.

Esse é um ataque man-in-the-middle em ação.

O hacker interceptou seu e-mail e enviou a você o número da conta bancária dele. Ele foi pago, enquanto o empreiteiro ainda espera pela taxa.

Tenha em mente que as redes Wi-Fi públicas não são seguras. Mesmo que não estejam configuradas por um hacker, você nunca sabe se elas estão bem configuradas. Alguém pode estar espreitando no meio de suas comunicações. Certifique-se de usar uma VPN antes de se conectar a uma rede pública.

Termos relacionados: ataque evil twin, honeypot Wi-Fi

N

Rede

Seus dispositivos são parte de uma rede, que é parte de uma rede maior, que pode ser parte de uma rede ainda maior, que pode ser — você já pegou a ideia. Essa é a internet, uma rede de redes de computadores, grandes e pequenas. E você está nela.

A rede mais próxima de você é chamada de LAN, rede de área local. Ela se refere a um grupo de dispositivos interconectados em um local físico. Então, quando você se conecta ao seu roteador doméstico, você se conecta à sua LAN.

Sua rede doméstica é provavelmente muito pequena, com até 10 dispositivos conectados (ou se você adora gadgets, muito mais, mas não estamos julgando, a tecnologia é incrível). Uma LAN também pode abranger toda uma empresa ou cobrir toda uma escola com milhares de dispositivos interconectados.

Termos relacionados: internet, LAN.

P

Phising

Você recebe um e-mail do seu banco. É um aviso, alguém tentou sacar dinheiro de sua conta. “Envie seu login e senha IMEDIATAMENTE para confirmar sua identidade”, informa o banco.

Parece assustador, mas você não deve agir por medo.

Verifique cuidadosamente o remetente e você provavelmente descobrirá que não é o seu banco, mas alguém se passando por ele. Não responda nem clique em nenhum link do e-mail. Ligue diretamente para o seu banco e pergunte sobre o e-mail.

O golpe é chamado de phishing e assume várias formas. Mensagens ou e-mails que usam medo e urgência para extrair detalhes confidenciais. Um site falso que se parece quase exatamente com o da sua universidade. Digite seu login e senha e você estará entregando-os a um golpista.

Defender-se é simples, seja cauteloso. Desconfie de mensagens duvidosas que afetem seus medos ou ainda pior, quando prometem algo bom demais para ser verdade. Especialmente se você precisar clicar num “clique aqui” para reivindicá-lo.

Pare, pense e verifique novamente. Não clique em um link se a URL não parecer legítima. Como regra geral, nunca insira ou divulgue sua senha a menos que você tenha certeza absoluta de que é seguro.

R

Ransomware

Você liga o computador e, espere aí, o que é isso? A tela não carrega. Mas há uma mensagem: “Seus arquivos foram criptografados pelo NarutoRun Hacker Group. Você tem uma semana para transferir 500 dólares em Bitcoin para nossa carteira ou seus arquivos serão perdidos para sempre. Rasengan!”

Parece o enredo de uma comédia mal escrita, mas não é para rir. Ransomware é um tipo de malware que criptografa à força os dados da vítima. Ninguém, exceto os hackers, pode desfazer a criptografia porque apenas eles detêm a chave. (Existem muitos protocolos de criptografia que são praticamente inquebráveis sem a chave de descriptografia. Veja: texto cifrado, criptografia de ponta a ponta.)

Você não deve pagar o resgate porque seus dólares (mais provavelmente, criptomoedas, geralmente solicitados por hackers) serviriam apenas para apoiar os criminosos. Em vez disso, aprenda como combater o ransomware:

- Não baixe nada de sites suspeitos. Não abra links, e-mails ou mensagens suspeitas. Veja: phishing.
- Faça backup dos seus arquivos mais sensíveis.
- Atualize seus aplicativos e software, especialmente seu software de segurança.
- Use senhas fortes.

S

Engenharia social

Você é acordado por seu telefone no início da manhã. A pessoa do outro lado explica educadamente que é um técnico da LiteNet, seu provedor de serviços de Internet. Eles tiveram uma falha de rede que pode ter resultado em uma pequena perda de dados.

Você poderia fornecer os quatro últimos dígitos do número do seu cartão de crédito para que eles possam compará-los com os registros em seus servidores?

Meio adormecido, você o faz e volta aos seus sonhos. Você acorda adequadamente duas horas depois, toma um bom café da manhã e descobre que foi hackeado.

A pessoa que ligou para você não era um técnico, mas sim um engenheiro social, um golpista que usa manipulação psicológica para induzir as pessoas a realizarem uma ação específica ou revelarem detalhes confidenciais.

Vamos dividir o golpe em partes. O golpista pegou você no início da manhã, se apresentou para afastar suas suspeitas (a LiteNet é o maior provedor de Internet na sua área, foi um palpite fácil) e soltou alguns jargões técnicos sem sentido para parecer legítimo.

Então ele ligou para a LiteNet fingindo ser você e disse que tinha esquecido a senha. Ele forneceu os últimos quatro dígitos do número do seu cartão de crédito para confirmar a identidade (ou seja, sua identidade) e redefinir sua senha LiteNet — incluindo a senha de sua conta de e-mail LiteNet.

LiteNet é um falso provedor de internet que criamos para essa história. Mas muitas empresas reais podem redefinir sua senha pelo telefone com base apenas nos quatro últimos dígitos do seu cartão de crédito. Você deve fornecer o mínimo de informações confidenciais possível ao se inscrever e declarar explicitamente que não divulga quaisquer detalhes por telefone.

Os engenheiros sociais empregam muitas técnicas para manipular os usuários, as quais são sofisticadas e contundentes. Um golpista pode enviar milhares de e-mails falsos na esperança de encontrar algumas vítimas que são crédulas o suficiente para responder com seus detalhes de cartão de crédito ou senhas. Veja também: phishing.

T

Autenticação de dois fatores

Você está fazendo login no Twitter no telefone do seu amigo porque deixou o seu em casa. Como esse é um novo dispositivo, você precisa confirmar o login em um aplicativo de autenticação especial. Que está no seu telefone. Que está em casa.

Argh, é um dilema de cibersegurança!

Sim, isso pode causar um pequeno incômodo, mas a autenticação de dois fatores (2FA) protege você com uma segunda camada de proteção. Se você tiver problemas para acessar sua conta sem o telefone, os hackers também terão.

Os dois fatores geralmente são:

Algo que você conhece (uma senha ou um código PIN). Algo que você tem (um telefone, um livro de códigos ou sua biometria).

Nenhum sistema é inviolável, mas a 2FA eleva a segurança de suas contas para um nível além do que a maioria dos usuários possui. Os cibercriminosos geralmente são oportunistas, então, em vez de tentar contornar a 2FA, eles escolherão outros alvos, de preferência alguém que use ABCDEFG como senha.

Você deve habilitar a 2FA em todos os serviços que a suportam. É uma maneira fácil de ficar muito mais seguro online com o mínimo de inconveniência.

Termos relacionados: autenticação multifator.

V

VPN

Você navega, você desliza, você surfa. E toda vez que você fica online, você deixa alguns dados sobre você. Seu provedor de serviços de Internet tem acesso ao seu tráfego online. Cada site que você visita pode ver seu endereço IP.

Não é apenas a privacidade, mas a sua segurança online que também está em jogo. Muitos sites ainda não usam um protocolo de comunicação seguro. A maioria dos aplicativos não divulga que tipo de práticas de segurança cibernética eles adotam. Você se vê obrigado a confiar neles sem motivos para tanto.

Uma VPN (rede privada virtual) é uma ferramenta que direciona todo o seu tráfego por meio de um servidor seguro, criptografa o processo e altera seu IP e localização virtual. Mesmo que possa parecer técnico, a VPN é uma ferramenta comum que é facilmente acessível para leigos.

Isso não significa que todas as VPNs são igualmente boas. Uma VPN roteia todo o seu tráfego através de seus servidores, então ela pode coletar seus dados e vendê-los pelo lance mais alto. A boa notícia é que a maioria das maiores VPNs é transparente sobre suas práticas, não mantém logs de usuários e, portanto, não tem nada para vender ou divulgar a terceiros.

Por exemplo, nós da NordVPN temos nossa política e serviço de não registro avaliados regularmente por uma empresa de Auditoria Big Four.

Termos relacionados: bomba-relógio, ameaça interna.

Wi-Fi

Você está em seu quarto de hotel, navegando no Wi-Fi gratuito. Alguns andares abaixo, um hacker está espionando sua atividade online. Como?

As redes Wi-Fi públicas são inerentemente inseguras, os cibercriminosos podem usar vários métodos para explorá-las ou comprometê-las.

Se o roteador estiver mal configurado, um hacker pode observar o tráfego da Internet de qualquer pessoa usando o hotspot público. Ou o hacker pode encontrar uma maneira de injetar um malware pela rede em seu dispositivo.

Um hacker pode configurar um ponto de acesso falso, o chamado evil twin e induzir você a se conectar a ele. Veja também: Ataque man-in-the-middle.
Seu nível de segurança depende de:

A configuração e as medidas de segurança no Wi-Fi do hotel. As práticas de segurança dos sites que você visita e dos aplicativos que usa. Suas práticas pessoais de cibersegurança.

Normalmente, você não sabe o nível de segurança de uma rede pública, então evite acessar dados sensíveis quando estiver conectado a ela. Por que não mudar para dados móveis? Ou ativar uma VPN?

P.S. Se você estiver organizando um evento, não conte com o Wi-Fi fornecido pelo local, porque isso raramente é seguro. Configurar corretamente um ponto de acesso Wi-Fi não é uma tarefa fácil e requer conhecimento técnico preciso, é melhor contratar profissionais se você não tiver as habilidades técnicas.

Mas seu trabalho é tão importante quanto você precisar se comunicar! Informe aos participantes do evento sobre os hotspots oficiais e os avise para não se conectar a nenhum outro hotspot, mesmo que ele pareça legítimo.

Termos relacionados: injeção de malware, detecção de Wi-Fi.

Z

Exploração de dia zero

Você atualizou seu software, instalou um antivírus, ativou seu firewall. Neste momento, nenhum hacker conseguiu invadir seu sistema, certo?

Se fosse assim tão simples...

Redes de computadores, software e hardware são criados por pessoas. As pessoas erram, não pensam em todos os cenários possíveis, deixam vulnerabilidades.

Os hackers exploram justamente esses erros e vulnerabilidades. Eles procuram o elo mais fraco do sistema e o quebram.
Assim que uma vulnerabilidade é descoberta, ela é corrigida. As atualizações que você instala nos seus aplicativos ou sistema operacional geralmente são apenas isso, patches para vulnerabilidades recém-descobertas.

(Claro, algumas vulnerabilidades nunca podem ser corrigidas. Humanos, e não máquinas, geralmente são o elo mais fraco quando se trata de segurança cibernética. Veja: engenharia social.)

Uma vulnerabilidade de dia zero é desconhecida do fornecedor e, portanto, não foi corrigida ainda. O nome se refere ao número de dias que um fornecedor teve para consertar a vulnerabilidade zero. Um ataque baseado nessa vulnerabilidade é chamado de exploração de dia zero ou ataque de dia zero.

Portanto, mesmo que você mantenha seu sistema protegido, corrigido e atualizado, uma exploração de dia zero pode comprometê-lo por meio de uma vulnerabilidade anteriormente desconhecida. A solução é a vigilância constante. Seja inteligente quando estiver online, use senhas fortes e não clique em links se você não tiver certeza de que eles são seguros.

Dessa forma, você minimiza seus riscos e forçará os cibercriminosos a procurar alvos mais fáceis.

Termos relacionados: vulnerabilidade de dia zero, ataque de dia zero.