

CIBERSEGURANÇA PARA LEIGOS

Como os sistemas são invadidos
e como são protegidos

Belisario Retto de Abreu

Sumário

Apresentação 1

Capítulo 1: Tudo pode ser invadido? 1

Capítulo 2: Engenharia social, o ataque que engana pessoas 3

Capítulo 3: Senhas, a chave que todo mundo copia 6

Capítulo 4: Malware, os programas que trabalham contra você 8

Capítulo 5: Ransomware, quando seus arquivos viram refém 10

Capítulo 6: Ataques à rede, ouvir, imitar e derrubar 12

Capítulo 7: Sites e aplicativos, quando o próprio programa tem a falha 14

Capítulo 8: Vulnerabilidades, zero-days e a corrida das atualizações 16

Capítulo 9: O fator humano, de dentro e de perto 18

Capítulo 10: Nuvem, celular e coisas conectadas, os novos alvos 21

Capítulo 11: Criptografia, o cadeado invisível da internet 23

Capítulo 12: Defesa em camadas, nenhuma porta sozinha basta 25

Capítulo 13: Quando acontece, resposta a incidentes e a lei 27

Capítulo 14: Inteligência artificial, deepfakes e o futuro da segurança 29

Capítulo 15: Guia por sistema, como se proteger no Windows, macOS, Lin… 32

Capítulo 16: Backups, a defesa que desfaz o estrago 42

Capítulo 17: Segurança no dia a dia, seu roteiro, o glossário e as fontes 47

Cibersegurança para Leigos: como os sistemas são invadidos e como são protegidos

Nov 18, 2026 · @Belisario Retto de Abreu

Apresentação

Quase tudo o que você faz hoje passa por um sistema que alguém, em algum lugar, está tentando invadir: o banco no celular, o e-mail, a câmera da sala, o hospital, a usina de energia. Este livro explica, sem exigir nenhum conhecimento técnico, como esses ataques funcionam e como cada um deles é barrado.

A ideia central é simples: ninguém consegue defender o que não entende. Por isso cada capítulo segue o mesmo desenho. Começa com uma cena, mostra a fragilidade que o atacante explora, explica o ataque passo a passo em linguagem comum, e fecha com a defesa e uma seção "Na prática", com algo que você pode fazer ainda hoje. Todo capítulo traz ao menos uma figura desenhada para tornar a ideia visível.

Um aviso importante. Este livro descreve os ataques no nível de ideia, o suficiente para reconhecer e se defender, e não é um manual de invasão. Invadir sistemas sem autorização é crime no Brasil e em quase todo o mundo. Se um dia quiser testar a segurança de algo, faça isso somente no que é seu ou com permissão por escrito de quem é o dono.

São dezessete capítulos. O primeiro mostra quem ataca e por quê. Os capítulos 2 a 10 percorrem os tipos de ataque, dos golpes que enganam pessoas às falhas escondidas em programas, redes, nuvem, celulares e aparelhos conectados. Os capítulos 11 a 14 explicam as defesas, o que fazer quando algo dá errado e o que a inteligência artificial muda nesse jogo. O capítulo 15 traz recomendações específicas para Windows, macOS, Linux, Android e iPhone, com roteiros à parte para a Internet, as redes sociais, o e-mail e as conexões físicas, como pendrives e Bluetooth. O capítulo 16 trata dos backups, e o último reúne tudo num roteiro de hábitos.

Capítulo 1: Tudo pode ser invadido?

Em novembro de 1988, um estudante de pós-graduação nos Estados Unidos soltou na internet um pequeno programa que se copiava de computador em computador. Ele não queria destruir nada. Queria, segundo contou depois, medir o tamanho da rede. Mas o programa tinha um erro: copiava-se com tanta frequência que sobrecarregava as

máquinas e as deixava inúteis. Em poucas horas, uma parte enorme da internet daquela época, que ainda era pequena, parou. Foi o primeiro grande ataque digital a ganhar as manchetes, e ficou conhecido como o verme de Morris.

A lição daquele dia continua valendo. Um programa escrito por uma pessoa só, sem dinheiro e sem má intenção declarada, derrubou milhares de computadores porque os sistemas tinham falhas que ninguém tinha olhado com cuidado. De lá para cá, a rede cresceu milhares de vezes, e as falhas também.

O que é "proteger" um sistema

Para falar de segurança com clareza, os especialistas usam três ideias, chamadas de pilares. A **confidencialidade** quer dizer que só quem deve ver uma informação consegue vê-la: seu extrato bancário, suas mensagens, seu prontuário. A **integridade** quer dizer que a informação não foi alterada sem permissão: o valor da transferência continua o mesmo, o resultado do exame não foi trocado. A **disponibilidade** quer dizer que o sistema funciona quando você precisa: o aplicativo abre, o hospital consegue acessar a ficha do paciente.

Todo ataque que você vai conhecer neste livro fere pelo menos um desses três pilares. Quem rouba senhas fere a confidencialidade. Quem altera um número de conta num boleto fere a integridade. Quem derruba um site com milhões de acessos falsos fere a disponibilidade. Quando você souber qual pilar está em risco, já terá metade do caminho para entender a defesa.

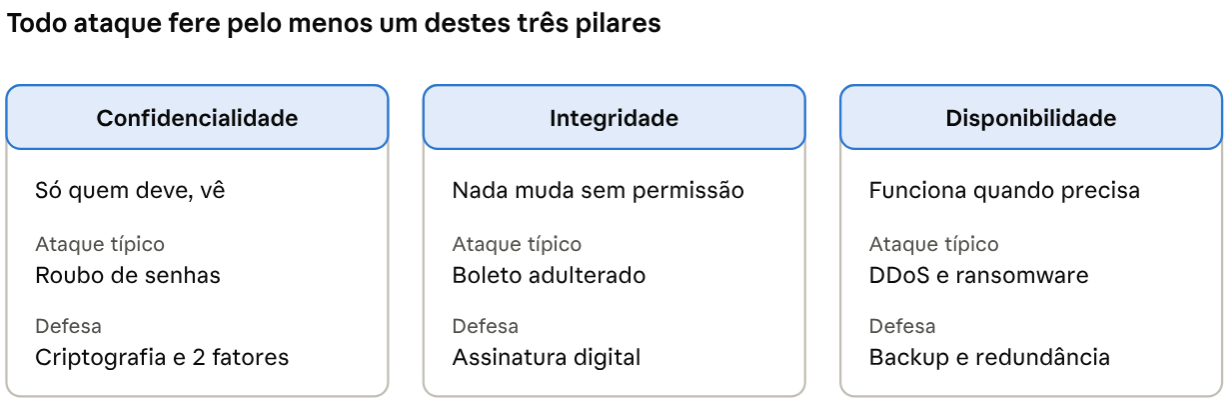


Figura 1.1 · os três pilares da segurança, com um ataque e uma defesa de cada

Quando souber qual pilar está em jogo, você saberá que tipo de defesa procurar.

Quem ataca, e por quê

O atacante de filme, o gênio de capuz sozinho num porão, existe, mas é minoria. A maior parte dos ataques vem de gente comum com um objetivo claro. Os **criminosos** querem dinheiro: roubam cartões, sequestram arquivos e pedem resgate, aplicam golpes por mensagem. Os **governos** querem informação ou poder: espionam outros países, sabotam

infraestrutura, interferem em eleições. Os **ativistas** querem chamar atenção para uma causa, muitas vezes derrubando ou pichando sites. Os **insiders**, funcionários ou ex-funcionários com acesso, agem por vingança, dinheiro ou descuido. E há os **curiosos e iniciantes**, que testam ferramentas prontas sem entender direito o que provocam.

Um detalhe que muda tudo: atacar ficou barato. Hoje existem serviços, vendidos como se fossem assinaturas, que alugam ferramentas de ataque a quem não sabe programar. Isso quer dizer que o número de atacantes não depende mais da quantidade de gênios, e sim da quantidade de pessoas dispostas a pagar um pouco.

Por que os sistemas têm falhas

Sistemas são feitos por gente, e gente erra, tem pressa e tem orçamento. Os programas de hoje têm milhões de linhas de código, e basta uma errada para abrir uma porta. Os aparelhos são vendidos com senhas de fábrica que ninguém troca. As empresas deixam uma atualização para a semana que vem, e a semana vira meses. E, sobretudo, os sistemas são usados por pessoas, que clicam, confiam, atendem o telefone e ajudam quem parece estar com problema. Boa parte dos ataques não quebra a tecnologia: engana quem a opera.

Isso leva a uma ideia que vai atravessar o livro. Não existe sistema 100% seguro. O objetivo da defesa nunca é "impedir tudo", e sim tornar o ataque caro, lento e arriscado o bastante para que o atacante desista ou seja descoberto, e garantir que, se algo der errado, o estrago seja pequeno e a recuperação seja rápida.

Na prática: o que você tem a proteger?

Pegue uma folha e liste cinco coisas digitais que seriam um problema se saíssem do seu controle: a conta do banco, o e-mail principal, as fotos da família, o WhatsApp, o celular em si. Ao lado de cada uma, escreva qual pilar mais importa: ninguém pode ver, ninguém pode alterar, ou não pode ficar fora do ar. Você acabou de fazer o primeiro passo de qualquer plano de segurança: saber o que vale proteger. Ao longo do livro, você vai voltar a essa lista e marcar que defesa cobre cada item.

Capítulo 2: Engenharia social, o ataque que engana pessoas

Dona Marta recebeu uma ligação numa tarde de terça. A voz, educada e calma, disse ser do setor de segurança do banco dela. Havia uma compra suspeita no cartão, de uma cidade que ela nunca visitou, e o atendente precisava confirmar que a titular estava bem. Para cancelar a compra, bastava ela ler o código que ia chegar por mensagem. O código chegou, ela leu, e dez minutos depois o dinheiro tinha saído da conta. Nenhuma tecnologia foi quebrada. Quem foi enganada foi a Marta.

Isso se chama **engenharia social**: usar a confiança, a pressa, o medo ou a vontade de ajudar das pessoas para fazer com que elas mesmas abram a porta. É o tipo de ataque mais comum do mundo, porque é o mais barato: não exige nenhuma falha técnica, só uma boa história.

Por que funciona

Os golpistas sabem como o cérebro decide em situações de estresse. Eles usam quase sempre os mesmos gatilhos. A **urgência**: "você tem uma hora". A **autoridade**: alguém do banco, da polícia, do chefe. O **medo**: sua conta será bloqueada. A **cobiça**: você ganhou um prêmio. E a **simpatia**: alguém gentil, que fala seu nome e parece conhecer sua vida. Quando mais de um gatilho aparece junto, a pessoa deixa de pensar e passa a reagir, que é exatamente o que o golpista quer.

As variedades do golpe

O **phishing** é a mensagem falsa enviada em massa, normalmente por e-mail, que imita um banco, uma loja ou um serviço conhecido e leva a um site falso para você digitar sua senha. O nome vem de "pescar": o golpista joga a isca para milhares de pessoas e espera alguma morder. O **smishing** é o mesmo golpe por SMS ou aplicativo de mensagens, e o **vishing** é o golpe por voz, como no caso da dona Marta. O **spear phishing** é a versão personalizada: o golpista estuda a vítima, usa o nome do chefe, do projeto em andamento, e a mensagem parece legítima de verdade. Quando o alvo é um executivo, o nome muda para **whaling**, à caça da baleia.

O **pretexting** é inventar um pretexto convincente: um falso técnico de internet, um falso entregador, um colega de outro departamento que precisa de uma senha "só dessa vez". O **quid pro quo** oferece algo em troca, como uma ajuda com o computador, para obter acesso. O **baiting**, ou isca, deixa um pendrive "esquecido" num estacionamento, esperando que a curiosidade de alguém o conecte à rede da empresa. E há a **fraude do falso chefe**, em que o golpista, fingindo ser o diretor, manda o financeiro pagar com urgência uma conta nova, e as empresas perdem milhões assim todos os anos.



Figura 2.1 · o roteiro de um golpe de engenharia social e o ponto em que ele se quebra

O golpista precisa que você vá da isca direto à ação; qualquer pausa para confirmar desfaz o plano.

O golpe do "parente em apuros" e do falso suporte

No Brasil, duas variantes são muito comuns. Na primeira, o golpista cria um perfil com a foto de um conhecido, escreve "troquei de número" e, em seguida, pede dinheiro por causa de uma emergência. Na segunda, finge ser o suporte do banco ou de uma loja e convence a vítima a instalar um aplicativo de acesso remoto, o que dá ao golpista controle total do celular ou do computador. Nos dois casos o roteiro é o mesmo: criar pressão e impedir que a vítima pare para checar.

Como se defender

A melhor defesa é um hábito, não uma ferramenta: **pare e confirme por outro canal**. Se o banco liga, desligue e ligue de volta para o número que está no verso do cartão. Se o chefe pede uma transferência por mensagem, telefone para ele. Se um amigo pede dinheiro com um número novo, ligue para o número antigo. Bancos e empresas sérias nunca pedem sua senha completa nem códigos enviados por mensagem. Desconfie sempre de urgência, de prêmios e de links encurtados, e olhe o endereço do site antes de digitar qualquer dado: sites falsos costumam ter letras trocadas ou terminar de forma estranha.

As empresas somam a isso treinamento, filtros de e-mail que isolam mensagens suspeitas e regras como "toda transferência nova exige duas pessoas". Uma regra assim não depende de ninguém ser esperto naquele dia.

Na prática: o teste dos dez segundos

Da próxima vez que uma mensagem pedir algo com pressa, conte até dez e responda três perguntas. Quem está pedindo? Por que o pedido chegou por esse canal? O que acontece se eu esperar uma hora? Se alguma resposta for estranha, confirme por outro caminho antes de clicar, pagar ou responder. Esse pequeno intervalo derruba a maior parte dos golpes.

Capítulo 3: Senhas, a chave que todo mundo copia

Rafael usava a mesma senha em quase tudo: o e-mail, a loja online, a conta de uma rede social que ele nem abria mais. Um dia, essa rede social sofreu um vazamento, e milhões de e-mails com senhas foram parar numa lista à venda. Duas semanas depois, Rafael recebeu um aviso de compra que não fez no cartão. O ladrão não "descobriu" a senha dele. Ele só tentou, em dezenas de lojas e bancos, a senha que já estava na lista, e numa delas deu certo.

A senha é a fechadura mais usada do mundo, e é também uma das mais frágeis, porque depende da memória humana. Pessoas escolhem senhas fáceis de lembrar, e o que é fácil de lembrar costuma ser fácil de adivinhar.

Como as senhas são atacadas

O ataque de **força bruta** tenta todas as combinações possíveis até acertar. Uma senha de quatro dígitos tem dez mil possibilidades, que um computador percorre num instante. Cada caractere a mais multiplica o trabalho, e por isso o tamanho importa mais do que a complicação: uma frase longa vale muito mais do que uma palavra curta cheia de símbolos. O ataque de **dicionário** é uma versão inteligente do mesmo: em vez de testar tudo, testa primeiro as senhas mais usadas do mundo, os nomes próprios, as datas de nascimento e as palavras com trocas previsíveis, como o "a" virando "@".

O **credential stuffing**, o caso do Rafael, aproveita a mesma senha usada em vários lugares. O atacante pega uma lista vazada e testa cada par de e-mail e senha em outros serviços, de forma automática. Funciona porque muita gente repete senhas. O **password spraying** faz o contrário: testa poucas senhas muito comuns, como "123456" ou "senha123", contra muitas contas, para não disparar o bloqueio que acontece depois de muitos erros numa conta só.

Há também o roubo direto. O **keylogger** registra o que você digita (voltaremos a ele no capítulo sobre malware). O phishing do capítulo anterior leva você a entregar a senha de mão beijada. E o **vazamento**, quando uma empresa é invadida e perde seus dados, joga senhas na rede mesmo que você tenha sido cuidadoso. Por isso, empresas decentes não guardam sua senha em texto aberto: guardam apenas uma espécie de impressão digital

dela, chamada **hash**, que não permite voltar à senha original, apenas conferir se a que você digitou é igual. Mesmo assim, hashes fracos podem ser quebrados por tentativa em massa quando vazam.

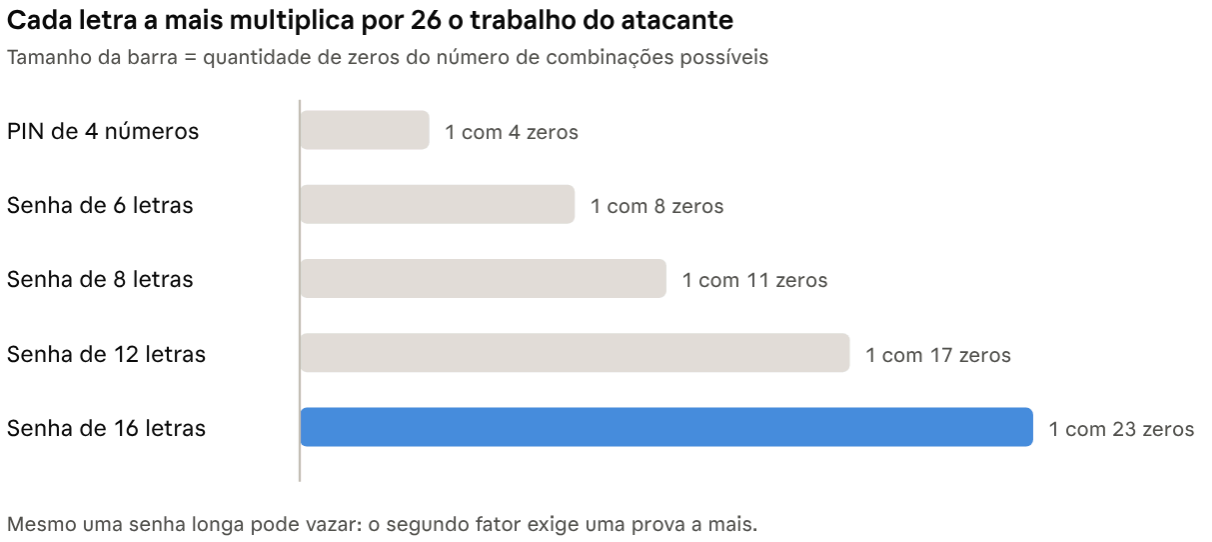


Figura 3.1 · combinações possíveis por tamanho de senha (calculado: 26 letras ou 10 números elevado ao tamanho)

O tamanho pesa mais do que a complicação: passar de 8 para 12 letras multiplica o número de combinações por mais de 400 mil.

Como se defender

A primeira regra é **uma senha diferente para cada serviço**. Parece impossível de lembrar, e é, por isso existe o **gerenciador de senhas**, um aplicativo que cria senhas longas e aleatórias, guarda todas num cofre trancado por uma senha mestra e as preenche por você. Você só precisa lembrar uma frase boa. A segunda regra é **escolher frases, e não palavras**: quatro ou cinco palavras sem relação, como "cavalo bateria lua tijolo", são mais fortes e mais fáceis de lembrar do que "P@ssw0rd!".

A terceira regra é a mais poderosa: a **autenticação em dois fatores**, ou MFA. Ela exige duas provas de que você é você: algo que você sabe (a senha) e algo que você tem (o celular com um código ou um aplicativo autenticador, ou uma chave física de segurança) ou algo que você é (a digital ou o rosto). Assim, mesmo que a senha vaze, o ladrão não entra sem o segundo fator. Códigos por SMS ajudam, mas podem ser interceptados por golpes de troca de chip, então aplicativos autenticadores e chaves físicas são mais seguros. As chamadas **passkeys**, cada vez mais comuns, vão além: trocam a senha por uma chave criptográfica guardada no seu aparelho, que não pode ser digitada em um site falso.

Na prática: duas contas, dez minutos

Escolha as duas contas mais importantes da sua vida, normalmente o e-mail principal e o banco. Troque a senha de cada uma por uma frase longa e única, e ative a verificação em dois passos. Depois, instale um gerenciador de senhas e comece a mudar as demais aos poucos, uma por semana. Em poucas semanas, o vazamento de qualquer site deixa de ser um problema para você.

Capítulo 4: Malware, os programas que trabalham contra você

Um pendrive achado no chão de um estacionamento parece um presente. Foi assim, segundo as histórias mais conhecidas, que um programa chamado Stuxnet teria chegado a uma usina nuclear isolada da internet, num ataque descoberto em 2010. A rede não tinha conexão com o mundo, mas tinha pessoas, e as pessoas usam pendrives. Esse caso virou o exemplo clássico de que o ponto mais forte de um sistema pode ser contornado pelo ponto mais comum: o cabo, o disco, o anexo, o clique.

Malware é qualquer programa feito para causar dano, roubar ou espionar. O nome junta as palavras inglesas para "software malicioso". Todo malware tem duas partes: um jeito de **entrar** e uma **tarefa** a cumprir depois que entra. Entender essas duas partes ajuda a separar a lista confusa de nomes.

Como o malware entra

As portas de entrada mais comuns são poucas. O **anexo ou link de e-mail** que você abre porque parecia uma nota fiscal. O **programa pirata ou falso**, como um "crack" gratuito ou um aplicativo clonado numa loja não oficial. O **site comprometido**, que explora uma falha no navegador sem que você clique em nada além de visitar. O **pendrive ou aparelho externo**. E a **falha não corrigida** de um programa desatualizado, que veremos no capítulo sobre vulnerabilidades.

A família dos malwares

O **vírus** precisa de você: ele se esconde dentro de um arquivo ou programa legítimo e só age quando esse arquivo é aberto, espalhando-se por cópia. O **worm**, ou verme, não precisa de ninguém: ele se copia sozinho pela rede, de máquina em máquina, como o de 1988 do primeiro capítulo. O **cavalo de Troia**, ou trojan, finge ser um programa útil, como um jogo ou um "limpador de computador", e carrega dentro dele a parte maliciosa. O nome vem da lenda grega.

O **spyware** espiona: lê o que você faz e envia para o atacante. O **keylogger** é um tipo de spyware que registra cada tecla digitada, o que inclui senhas. O **adware** enche a tela de anúncios e rastreia hábitos. O **rootkit** se esconde nas camadas mais profundas do

sistema, de modo que nem o antivírus enxerga direito, e é difícil de remover. O **backdoor**, ou porta dos fundos, deixa uma entrada aberta para o atacante voltar quando quiser. O **stalkerware** é instalado por alguém conhecido para vigiar o celular de outra pessoa, e é um problema sério de segurança pessoal.

O **botnet** é um caso especial: uma rede de milhares ou milhões de aparelhos infectados, chamados de zumbis, controlados à distância por um criminoso. O dono do aparelho não percebe nada, mas seu computador ou sua câmera passa a trabalhar para ele em ataques, envio de spam ou mineração de criptomoedas escondida. O **ransomware**, que sequestra seus arquivos, é tão importante que merece o próximo capítulo inteiro.

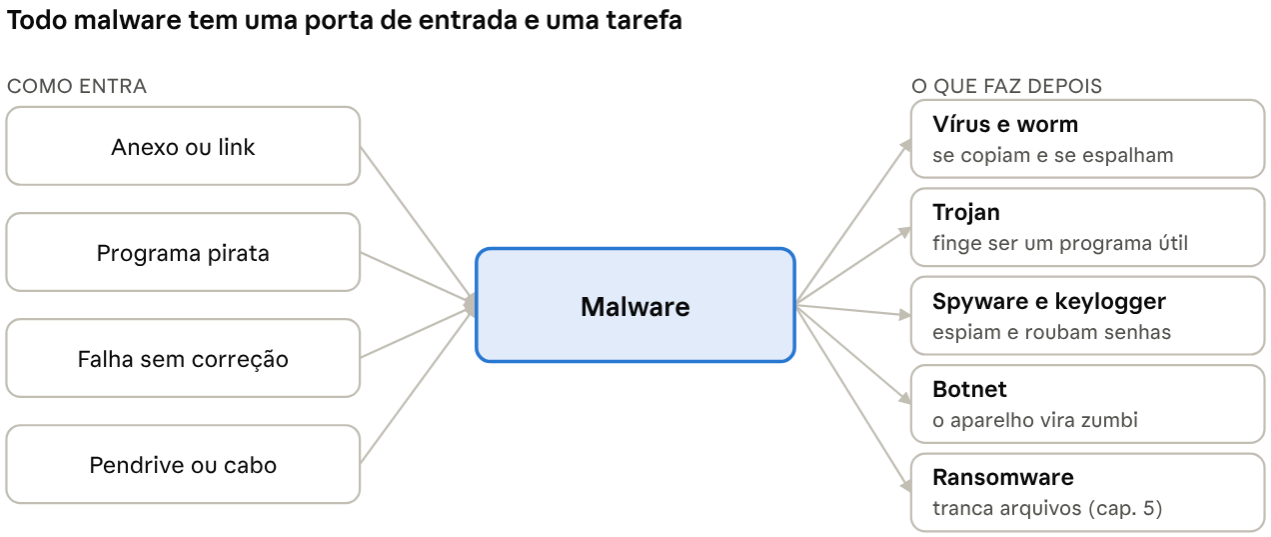


Figura 4.1 · mapa do malware: quatro portas de entrada e cinco tarefas

Os nomes mudam, mas o desenho é sempre o mesmo: uma porta de entrada, depois uma tarefa. Fechar a porta protege contra todas as tarefas.

Como se defender

A defesa contra malware tem camadas. Primeiro, **não abrir o que não foi pedido**: anexos inesperados, links em mensagens de desconhecidos, programas fora das lojas oficiais. Segundo, **manter tudo atualizado**: sistema, navegador e aplicativos, porque a maior parte do malware explora falhas que já têm correção publicada. Terceiro, usar um **antivírus ou proteção integrada**, como o que já vem no Windows, no Android e no macOS. Ele compara arquivos com uma lista de assínaturas conhecidas e, nas versões modernas, também observa o comportamento: um programa que de repente começa a criptografar centenas de arquivos é suspeito, mesmo que ninguém nunca o tenha visto antes.

Quarto, **trabalhar sem poderes demais**: usar no dia a dia uma conta comum, e não de administrador, limita o estrago que um programa infectado consegue fazer. Quinto, **fazer cópias de segurança**, que são a rede de proteção final e o assunto do capítulo 12.

Na prática: sinais de que algo está errado

Desconfie quando o aparelho ficar muito lento sem motivo, a bateria acabar rápido demais, aparecerem programas que você não instalou, o navegador abrir páginas sozinho ou a câmera acender sem você ter pedido. Nenhum sinal sozinho prova nada, mas vários juntos justificam rodar a verificação completa do antivírus e, se preciso, procurar um técnico de confiança.

Capítulo 5: Ransomware, quando seus arquivos viram refém

Numa segunda-feira, uma clínica abriu e não conseguiu atender ninguém. Em todas as telas, a mesma mensagem: os arquivos estavam trancados, e para destrancá-los era preciso pagar uma quantia em criptomoeda dentro de alguns dias, ou o preço dobraria. As fichas dos pacientes, a agenda, os exames, tudo estava ali, ilegível. A clínica era pequena, mas o roteiro é o mesmo que paralisou hospitais, prefeituras e até uma grande rede de oleodutos nos Estados Unidos, em 2021.

O **ransomware** é um tipo de malware que **criptografa** os arquivos da vítima, isto é, embaralha cada um com uma chave secreta, e só entrega a chave depois de um pagamento. O nome vem de *ransom*, resgate em inglês. É hoje uma das maiores indústrias do crime digital, e merece um capítulo próprio porque ataca os três pilares ao mesmo tempo: os dados ficam inacessíveis, o negócio fica parado e, em muitos casos, cópias dos arquivos são roubadas.

Como o ataque acontece

O roteiro costuma ter cinco etapas. Na **entrada**, o atacante consegue um primeiro acesso: um e-mail com anexo, uma senha vazada de um acesso remoto, uma falha em um programa que nunca foi atualizado. Na **exploração**, ele percorre a rede com calma, por dias ou semanas, para descobrir onde estão os dados valiosos e os backups. Depois vem o **roubo**: copia os arquivos mais sensíveis para um servidor dele. Só então chega a **criptografia**, disparada de uma vez, geralmente num fim de semana ou feriado, quando há menos gente olhando. E, por fim, a **exigência**: a mensagem na tela com o valor e o prazo.

A parte do roubo mudou o jogo. Antes, quem tinha boas cópias de segurança podia ignorar o resgate e restaurar os arquivos. Agora os criminosos também ameaçam **publicar os dados roubados**, o que se chama de dupla extorsão. Mesmo com backup, a vítima ainda enfrenta o vazamento de segredos, de dados de clientes e de prontuários. Alguns grupos chegam a uma terceira pressão: avisam os clientes e a imprensa, ou atacam o site da vítima para aumentar o desespero.



Figura 5.1 · as cinco etapas de um ataque de ransomware

A vítima só vê a quarta etapa. Quem tem backup fora da rede desfaz o bloqueio, mas a ameaça de publicar os dados roubados continua.

Por que pagar quase nunca é uma boa ideia

Pagar parece simples e rápido, mas não há garantia nenhuma. Parte das vítimas paga e não recebe a chave, ou recebe uma que não funciona direito. Quem paga fica marcado como pagador e costuma ser atacado de novo. E o dinheiro financia o próximo ataque. As autoridades de vários países recomendam não pagar, e alguns lugares estudam proibir o pagamento em certos casos. A decisão, no entanto, é de quem está no meio do incêndio, e é por isso que a preparação antes do ataque importa tanto.

Como se defender

A defesa tem três frentes. A primeira é **fechar as portas de entrada**: senhas fortes, verificação em dois passos nos acessos remotos, programas atualizados, filtro de e-mail. A segunda é **limitar a propagação**: dividir a rede em partes separadas (a chamada segmentação), de modo que um computador infectado não alcance todos os outros, e dar a cada pessoa só o acesso de que ela realmente precisa. A terceira, e mais importante, é ter **cópias de segurança que o ransomware não alcance**. A regra clássica é a **3-2-1**: três cópias dos dados, em dois tipos diferentes de mídia, com uma cópia guardada fora do local e desconectada da rede. Um backup que fica sempre ligado ao computador pode ser criptografado junto com os arquivos. E vale o teste mais ignorado de todos: restaurar de verdade, de tempos em tempos, para ter certeza de que a cópia funciona.

Na prática: seu plano de 15 minutos

Escolha a pasta mais valiosa do seu computador, com fotos, documentos e declarações. Copie-a para um disco externo ou um serviço de nuvem com histórico de versões. Depois desconecte o disco e guarde-o em outro lugar da casa. Uma vez por mês, reconecte, atualize a cópia e abra um arquivo para conferir. É pouco trabalho, e transforma o pior dia da sua vida digital em um inconveniente de uma tarde.

Capítulo 6: Ataques à rede, ouvir, imitar e derrubar

No aeroporto, Camila abriu o celular e viu duas redes de Wi-Fi com nomes quase iguais: "Aeroporto_Gratis" e "Aeroporto-Gratis". Escolheu a primeira, conectou, abriu o aplicativo do banco e seguiu viagem. Uma das duas redes era do aeroporto. A outra havia sido montada por um golpista numa mochila, a poucos metros dali, só para que as pessoas se conectassem a ela. Tudo o que passava por essa rede, ele podia observar.

Os dados que você manda pela internet viajam por muitos intermediários: o roteador de casa, o provedor, várias empresas no meio do caminho. Cada um deles é um ponto onde alguém pode escutar, alterar ou bloquear a mensagem. Os ataques à rede exploram justamente esse trajeto.

Escutar: o sniffing

O **sniffing**, ou farejamento, é a escuta do tráfego da rede. Em uma rede aberta, sem senha ou com criptografia fraca, os dados de quem está conectado podem ser lidos por quem estiver no mesmo ambiente com a ferramenta certa, como quem ouve uma conversa na mesa ao lado. Se o conteúdo não estiver criptografado, o atacante lê senhas, mensagens e páginas visitadas. Por isso o cadeado do navegador, assunto do capítulo 11, é tão importante: ele embaralha o conteúdo para que quem escuta só veja ruído.

Imitar: o homem no meio

No ataque do **homem no meio** (man-in-the-middle), o atacante se coloca entre você e o serviço que você quer usar. Você acha que fala com o banco, o banco acha que fala com você, mas tudo passa pelo atacante, que lê e pode até alterar as mensagens. O Wi-Fi falso da Camila é um exemplo, e se chama **evil twin**, ou gêmeo mau. Outras formas incluem enganar o endereço de destino do tráfego dentro de uma rede local e redirecionar você para um site falso por meio de uma consulta de nomes adulterada, o que se chama de **envenenamento de DNS**. O DNS é a "lista telefônica" da internet, que traduz o nome do site para o endereço numérico; se essa tradução for falsificada, o nome certo leva ao lugar errado.



Figura 6.1 · três ataques à rede lado a lado

Nos dois primeiros, o alvo é a conversa: um só escuta, o outro se coloca no caminho. No terceiro, o alvo é o servidor, que cai sob o peso dos pedidos.

Derrubar: o DoS e o DDoS

O terceiro ataque não quer roubar nada: quer **tirar o serviço do ar**. No **DoS**, ataque de negação de serviço, o atacante bombardeia um site ou servidor com tantos pedidos que ele não dá conta de atender os usuários reais. Pense numa loja com uma porta só: se mil pessoas entram sem comprar nada, os clientes de verdade não conseguem passar. No **DDoS**, a versão distribuída, os pedidos vêm de milhares ou milhões de aparelhos ao mesmo tempo, normalmente os zumbis de um botnet, o que torna quase impossível bloquear só uma origem. Em 2016, um ataque desse tipo, feito com câmeras e roteadores domésticos infectados por um programa chamado Mirai, tirou do ar por horas sites muito conhecidos nos Estados Unidos.

Os motivos variam: extorsão ("pague ou seu site fica fora do ar na Black Friday"), protesto, concorrência desleal ou simples vandalismo. Em qualquer caso, o ataque fere a disponibilidade, e o prejuízo de um site de vendas parado por um dia pode ser enorme.

Como se defender

Para o usuário comum, a regra é **desconfiar de rede aberta** e nunca fazer operações sensíveis nelas. Em viagem, prefira o próprio plano de dados do celular, ou use uma **VPN** confiável, que cria um túnel criptografado até um ponto seguro, de modo que a rede local só vê ruído. Confira o nome exato da rede com o estabelecimento, confirme que o site mostra o cadeado e o endereço correto, e desligue a conexão automática de Wi-Fi do celular. Em casa, troque a senha de fábrica do roteador e use criptografia moderna na rede.

As empresas combinam várias defesas. Um **firewall** filtra o que entra e sai. Serviços de proteção contra DDoS espalham o tráfego por muitos servidores e absorvem a inundação antes que ela chegue ao site. A criptografia em todas as conexões impede a escuta. E o **monitoramento** da rede detecta tráfego estranho, como um aparelho falando com um endereço que nunca falou antes.

Na prática: a regra do café

Sempre que usar um Wi-Fi público, faça o seguinte: confirme o nome da rede, use apenas para o que não é sensível (ler notícias) e deixe o banco e as compras para o plano de dados do celular. Se precisar muito, ligue a VPN primeiro.

Capítulo 7: Sites e aplicativos, quando o próprio programa tem a falha

Um site de ingressos tinha, na tela de login, dois campos: usuário e senha. Um pesquisador de segurança, trabalhando com autorização da empresa, digitou no campo do usuário não um nome, mas um texto estranho, cheio de aspas e símbolos. O site, em vez de recusar, respondeu como se o texto fosse uma ordem para o banco de dados, e mostrou uma lista de clientes. Ele não precisou descobrir nenhuma senha. Bastou o site confiar demais no que recebeu.

Nos capítulos anteriores, o ataque vinha de fora do programa: enganar a pessoa, roubar a senha, escutar a rede. Aqui o problema está dentro do próprio site ou aplicativo, que foi escrito com um descuido. Quem programa precisa tratar tudo o que recebe do usuário como possivelmente hostil, e quando não trata, aparecem os buracos.

Injeção: dados que viram ordens

A falha mais clássica se chama **injeção**. Um programa monta uma ordem para o banco de dados juntando um texto fixo com o que o usuário digitou. Se o programador não separar os dois, o usuário consegue escrever, no lugar de um nome, pedaços de ordem, que o banco executa como se fossem do próprio sistema. Quando a ordem é para o banco de dados, o ataque se chama **SQL injection**. Resultado possível: ver dados de outros clientes, alterar registros ou apagar tabelas. A mesma ideia vale para ordens ao sistema operacional e a outras camadas.

A defesa é conhecida há décadas: usar consultas **parametrizadas**, em que os dados do usuário ficam sempre separados da ordem e nunca são interpretados como código. Ainda assim, essa falha continua aparecendo em sistemas antigos e mal revisados.

Script entre sites: o texto que vira programa no seu navegador

O **XSS** (cross-site scripting) acontece quando um site mostra para você um texto digitado por outra pessoa sem filtrá-lo. Se esse texto contiver um pequeno programa, o seu navegador o executa como se fosse do site de confiança, e ele pode ler o que você está vendo ou agir em seu nome. Um comentário malicioso numa página de notícias, por exemplo, poderia tentar roubar a sessão de quem a lê. A defesa está em limpar e escapar o texto antes de exibi-lo.

Falhas de configuração e de controle de acesso

Muitas invasões não exigem nenhuma técnica sofisticada. Um servidor deixado aberto sem senha, uma pasta de arquivos pública por engano, uma conta de teste esquecida, uma senha padrão nunca trocada. Isso é a **configuração insegura**, e está entre as causas mais frequentes de vazamentos, sobretudo na nuvem. Outro erro comum é o **controle de acesso quebrado**: o sistema esquece de conferir se você pode ver aquela página. Se o endereço do seu pedido termina em "pedido=1001", e você troca por "pedido=1002" e vê o pedido de outro cliente, o sistema não verificou quem era o dono. Isso aconteceu com empresas grandes, e a falha é tão simples quanto parece.



Figura 7.1 · injeção: o mesmo campo, com e sem separação entre dado e ordem

O campo e o texto digitado são os mesmos nos dois lados. O que muda é se o programa deixa o texto virar parte da ordem.

APIs: as portas dos fundos dos aplicativos

Quase todo aplicativo de celular conversa com um servidor por meio de uma **API**, um conjunto de portas pelas quais o aplicativo pede e recebe dados. As APIs são um alvo cada vez mais comum, porque costumam expor mais dados do que a tela mostra e, às vezes, ficam sem a mesma proteção do site. Falhas típicas: não checar quem está pedindo, aceitar pedidos em quantidade ilimitada ou devolver campos que o aplicativo nem usa.

Como se defender

Para quem **constrói** sistemas, a lista é ensinada em toda formação séria: validar tudo o que chega, separar dados de ordens, conferir permissão em cada pedido, nunca confiar no que vem do navegador, guardar senhas apenas como hash e revisar o código. Existe até uma lista pública das dez falhas mais comuns em aplicativos, mantida por uma organização chamada OWASP, usada como guia por equipes do mundo todo. Muitas empresas contratam **testes de invasão** autorizados, em que profissionais tentam quebrar o sistema antes dos criminosos, e mantêm programas de **recompensa por falhas**, pagando a quem as encontra e avisa em vez de explorá-las.

Para quem **usa**, o que resta é escolher serviços confiáveis, desconfiar de sites sem cadeado e sem reputação, usar senhas únicas (assim, o vazamento de um site não afeta os outros) e instalar aplicativos só de lojas oficiais.

Na prática: um passeio pelos seus aplicativos

Abra a lista de aplicativos instalados no celular e apague os que você não usa há meses. Cada aplicativo guardado é uma superfície a mais para falhas. Nos que ficam, revise as permissões: uma lanterna não precisa dos seus contatos, e um jogo não precisa do microfone.

Capítulo 8: Vulnerabilidades, zero-days e a corrida das atualizações

Em 2017, uma grande empresa americana de análise de crédito, a Equifax, perdeu os dados pessoais de mais de cem milhões de pessoas. A falha usada pelos invasores já era conhecida, e a correção já estava disponível havia semanas. A empresa não aplicou a atualização em um dos seus sistemas a tempo. Um conserto de rotina, adiado, virou um dos maiores vazamentos da história.

Uma **vulnerabilidade** é uma falha num programa ou aparelho que pode ser usada para fazer algo que não devia ser permitido. Quase todo software tem alguma, por mais cuidado que se tenha. O que importa é o que acontece depois: quem a encontra primeiro, e o que faz com ela.

O ciclo de vida de uma falha

Quando alguém descobre uma falha, a sequência ideal é a **divulgação responsável**: o pesquisador avisa o fabricante em sigilo, o fabricante prepara uma **correção**, também chamada de patch, e só depois a falha é tornada pública, com um número de identificação. Esses números seguem um padrão mundial, os chamados CVE, para que todos falem da

mesma falha. A cada nova falha pública, os criminosos correm para criar um ataque antes que as pessoas atualizem, e passa a valer uma corrida: de um lado quem aplica a correção, do outro quem a explora.

Existe, porém, um caso pior: o **zero-day**. É uma falha que o atacante conhece e o fabricante não. O nome vem de a defesa ter tido "zero dias" para se preparar. Contra um zero-day não há correção nenhuma, e por isso essas falhas valem muito dinheiro, tanto no mercado criminoso quanto em empresas que as compram para fins legais. Mas a maioria dos ataques do dia a dia não usa zero-days: usa falhas antigas, com correção conhecida, em máquinas que ninguém atualizou.

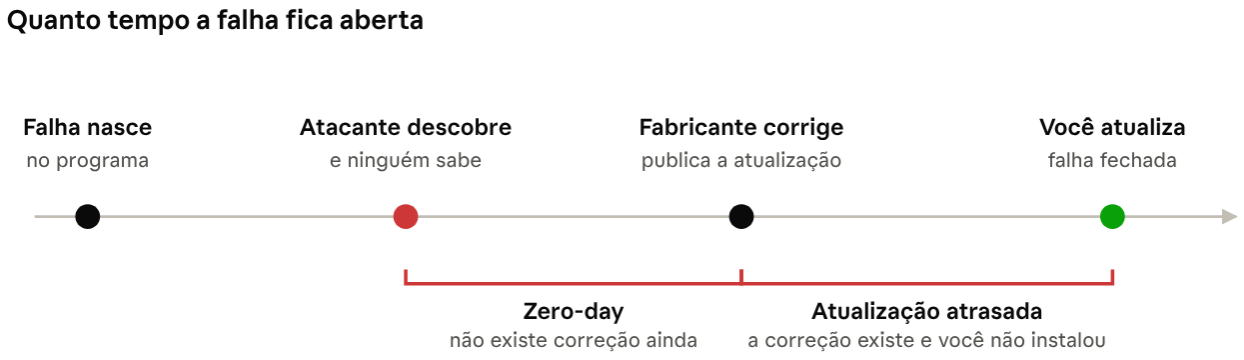


Figura 8.1 · a corrida entre o atacante, o fabricante e você

O primeiro trecho depende do fabricante, e o segundo, de você. Ligar as atualizações automáticas é a forma mais simples de encurtar o tempo em que a falha fica aberta.

Exemplos que marcaram

Em 2014, uma falha chamada **Heartbleed**, numa biblioteca usada para criptografia em muitos servidores, permitia que um atacante lesse pedaços da memória deles, com senhas e dados. Em 2017, o ransomware **WannaCry** se espalhou pelo mundo por uma falha do Windows que já tinha correção, e atingiu hospitais e empresas que não tinham atualizado. Em 2021, a falha **Log4Shell**, numa pequena biblioteca de registro de eventos usada em milhares de programas, mostrou outro problema: a maioria das empresas nem sabia que tinha aquele pedaço dentro dos seus sistemas.

A cadeia de suprimentos

Esse último ponto leva a um risco crescente: o ataque à **cadeia de suprimentos**. Um programa moderno é montado com centenas de peças de terceiros, e uma empresa depende da segurança de cada fornecedor. Se o atacante não consegue entrar pela porta da frente, entra pela porta de quem presta serviço. Em 2020, o caso **SolarWinds** mostrou

isso: invasores inseriram código malicioso numa atualização legítima de um programa de gestão de redes, que milhares de clientes instalaram com confiança, entre eles órgãos governamentais. Em 2013, a rede americana de lojas Target foi invadida por meio da conta de uma empresa de climatização que prestava serviço a ela. A atualização, que é a principal defesa, também pode ser o caminho do ataque.

Como se defender

Para o usuário, a regra é curta: **ligue as atualizações automáticas** do sistema, do navegador e dos aplicativos, e troque aparelhos que o fabricante parou de atualizar, como celulares muito antigos e roteadores sem suporte. Quase todo ataque em massa depende de gente que não atualizou.

Para as empresas, a defesa é um processo: manter um **inventário** do que existe na rede (não dá para proteger o que não se sabe que existe), acompanhar os avisos de novas falhas, priorizar as que já estão sendo exploradas, aplicar as correções em dias e não em meses, e testar as atualizações antes de espalhá-las. Contra zero-days, onde não há correção, restam as camadas gerais do capítulo 12: segmentação, monitoramento e o princípio de dar a cada programa o mínimo de acesso. E para a cadeia de suprimentos, as empresas passaram a exigir dos fornecedores listas de componentes e prova de práticas de segurança.

Na prática: a auditoria de cinco minutos

Abra as configurações do seu celular e do seu computador e confirme três coisas: a atualização automática está ligada, não há atualização pendente há mais de duas semanas e a versão do sistema ainda recebe suporte do fabricante. Se algum aparelho em casa não recebe mais atualizações, como um roteador antigo, considere substituí-lo.

Capítulo 9: O fator humano, de dentro e de perto

Uma funcionária de um escritório foi demitida numa sexta-feira. Ninguém lembrou de desativar o acesso dela ao sistema de arquivos da empresa. Na segunda, a lista de clientes tinha sido copiada, e o arquivo apareceu semanas depois na mão de um concorrente. Não houve invasão em nenhum sentido técnico: a porta estava aberta, e quem entrou tinha a chave.

Até aqui, os ataques vinham de fora. Mas um conjunto importante de riscos nasce dentro da organização, ou perto dela, e envolve pessoas com acesso legítimo, pessoas que erram e pessoas que chegam fisicamente ao lugar.

A ameaça interna

Chama-se **ameaça interna** (insider threat) qualquer risco causado por quem tem acesso autorizado: funcionário, ex-funcionário, terceirizado, parceiro. Ela tem três faces. A **maliciosa**: alguém que rouba dados ou sabota sistemas por vingança, dinheiro ou ideologia. A **negligente**: alguém que não quer fazer mal, mas ignora regras, compartilha senhas, manda planilhas de clientes para o e-mail pessoal. E a **comprometida**: alguém cuja conta foi roubada por um atacante, que passa então a agir com a identidade e os poderes daquela pessoa. Na prática, os casos negligente e comprometido são muito mais comuns do que o de maldade deliberada.

O que torna a ameaça interna difícil de barrar é que o acesso é legítimo. O sistema não vê um invasor, vê um usuário autorizado fazendo algo permitido, só que com intenção ou resultado errado.

Erros e descuidos

A maior parte dos incidentes não tem vilão. Alguém envia o e-mail para a pessoa errada, deixa um notebook no táxi, publica sem querer um arquivo com senhas num serviço público, deixa um banco de dados aberto na nuvem, usa a senha do trabalho em um site de compras. Isso tem nome: **erro humano**, e aparece em todos os estudos como uma das causas mais frequentes de vazamentos. Culpar a pessoa raramente resolve; o que funciona é projetar sistemas e processos em que um erro isolado não seja suficiente para causar um desastre.

O ataque físico

Segurança digital também depende de portas, crachás e gavetas. No **tailgating**, ou "carona", o invasor segue um funcionário por uma porta com controle de acesso, carregando caixas ou fingindo estar ao telefone, e ninguém ousa pedir o crachá. No **shoulder surfing**, ele só olha por cima do ombro para ver a tela ou a senha digitada. No **dumpster diving**, vasculha o lixo atrás de papel com dados. Outros ataques colocam aparelhos pequenos em tomadas ou portas USB, ou esperam num café pelo notebook deixado aberto por um instante. Num teste autorizado, equipes de segurança costumam provar que um crachá falso e uma camiseta de empresa de manutenção abrem muitas portas.

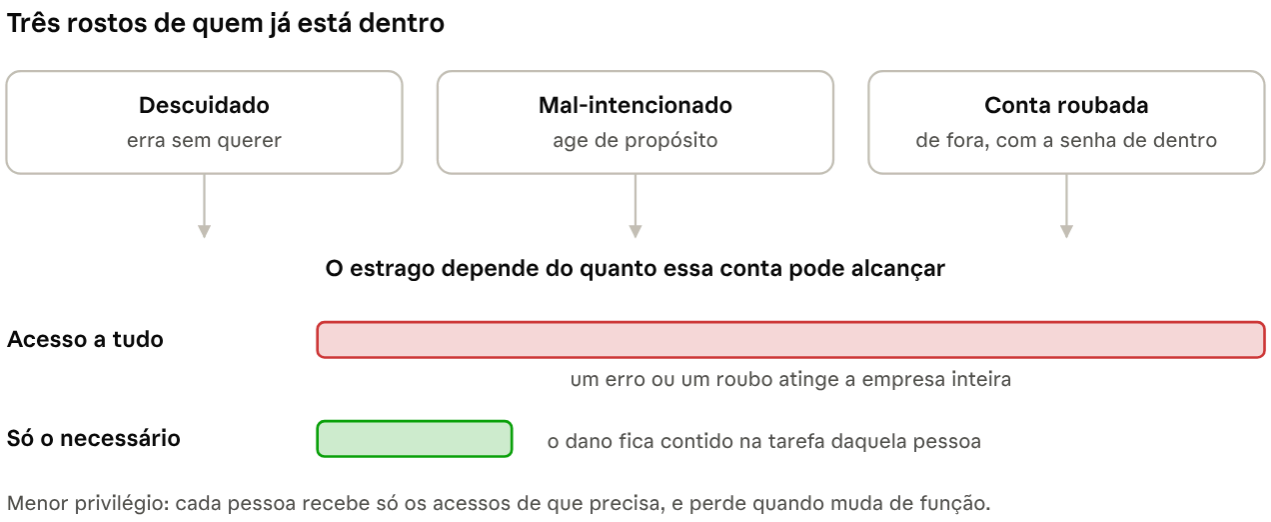


Figura 9.1 · os três rostos da ameaça interna e o limite que o menor privilégio impõe

Nos três casos o ponto de partida muda, mas o dano é medido da mesma forma: pelo tamanho do acesso que a conta tinha. Reduzir o acesso é a defesa que funciona contra os três.

Como se defender

A defesa técnica mais importante aqui é o **princípio do menor privilégio**: cada pessoa recebe apenas os acessos de que precisa para seu trabalho, e nada além. Assim, mesmo uma conta comprometida ou um funcionário mal-intencionado só alcança uma parte pequena do sistema. Junto com isso, vem a **revogação rápida**: quando alguém sai ou muda de função, os acessos são cortados ou revistos no mesmo dia. Registros de acesso, que mostram quem abriu o quê e quando, ajudam a detectar comportamentos estranhos, como alguém que baixa mil arquivos de madrugada.

A defesa humana é cultura: treinamento regular, regras simples e claras, e um ambiente em que as pessoas se sintam seguras para avisar "acho que cliquei em algo errado" logo, sem medo de punição. Quem esconde o erro por medo deixa o estrago crescer. E a defesa física é básica: crachás visíveis, o hábito de perguntar "posso ajudar?" a quem não conhece, tela bloqueada ao sair da mesa, trituração de papel sensível e portas USB controladas.

Na prática: bloqueie ao levantar

Crie o hábito de bloquear a tela sempre que se afastar do computador ou do celular, mesmo por um minuto. No Windows, as teclas Windows e L fazem isso na hora; no Mac, Controle, Comando e Q. É o menor hábito de segurança que existe, e fecha uma porta inteira.

Capítulo 10: Nuvem, celular e coisas conectadas, os novos alvos

Uma família instalou uma câmera na sala para ver o cachorro durante o dia. Pagou pouco, ligou na tomada e usou a senha de fábrica, que vinha impressa na caixa. Meses depois, perceberam que a câmera se mexia sozinha. Alguém, em outro lugar, estava olhando para dentro da casa. Aparelhos como esse, vendidos aos milhões, são um dos assuntos deste capítulo.

A segurança que se aprende com o computador de mesa não basta mais. Hoje, os dados ficam na nuvem, o banco cabe no celular e a casa tem dezenas de aparelhos conectados. Cada um traz fragilidades próprias.

A nuvem: o computador de outra pessoa

A **nuvem** é só um jeito bonito de dizer que seus arquivos e programas ficam em computadores de uma empresa, que você acessa pela internet. Isso traz uma vantagem enorme, porque os grandes provedores investem em segurança muito mais do que um usuário comum conseguiria, e um risco que não é tecnológico: a responsabilidade é dividida. O provedor cuida da segurança do prédio, dos servidores e da infraestrutura. Você cuida de quem acessa seus dados, de como foram configurados e das senhas. Esse arranjo se chama **modelo de responsabilidade compartilhada**, e os vazamentos na nuvem quase sempre nascem do lado do cliente: uma pasta aberta ao público por engano, uma chave de acesso esquecida num arquivo, uma conta sem verificação em dois passos. Em 2019, um banco americano teve dados de mais de cem milhões de clientes expostos por uma configuração errada de segurança na nuvem. A tecnologia da nuvem estava boa; a configuração não.

O celular: o computador mais pessoal

O celular guarda suas fotos, mensagens, contatos, aplicativos de banco, localização e códigos de verificação. Quem o controla controla sua vida digital. Os principais ataques incluem os aplicativos falsos ou infectados, os golpes por mensagem do capítulo 2, o **SIM swap**, em que o criminoso convence a operadora a transferir seu número para um chip dele para receber seus códigos por SMS, o roubo físico do aparelho com a tela desbloqueada, e o **stalkerware**, instalado por alguém próximo para vigiar. No Brasil, golpes de falsa central de atendimento e de clonagem de WhatsApp, em que o criminoso passa a se passar por você para pedir dinheiro a seus contatos, afetam milhões de pessoas.

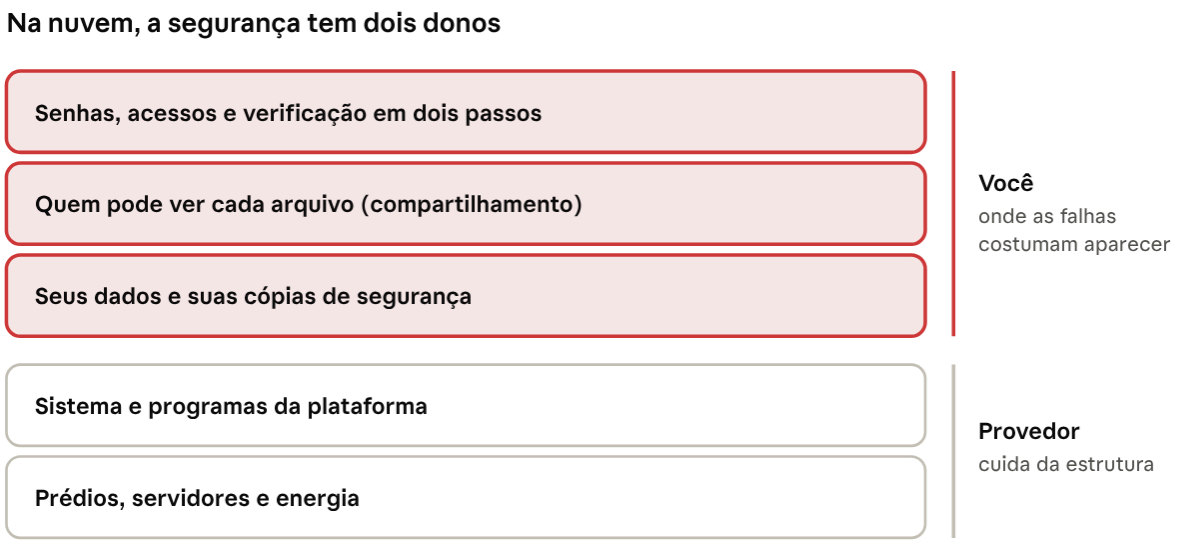


Figura 10.1 · responsabilidade compartilhada: o que cabe ao provedor e o que cabe a você

O provedor protege a estrutura. A parte de cima, que decide quem entra e o que fica aberto, é sua, e é onde as falhas costumam aparecer.

Internet das coisas: tudo com Wi-Fi

A **internet das coisas**, ou IoT, é o nome de tudo o que tem um chip e se conecta à rede: câmeras, campainhas, televisões, geladeiras, lâmpadas, babás eletrônicas, carros, medidores. Esses aparelhos costumam ter três problemas. São baratos, e a segurança custa dinheiro, então muitos são fabricados sem ela. Raramente são atualizados, e as falhas ficam para sempre. E vendem com **senhas de fábrica** iguais para milhares de unidades, que o dono nunca troca. Já vimos no capítulo 6 o resultado: o programa Mirai varreu a internet atrás de câmeras e roteadores com senha padrão e criou uma rede enorme de zumbis. E nem todos os alvos são domésticos: sistemas industriais, hospitais, redes de energia e de água também dependem de aparelhos conectados, e a invasão de um deles pode ter efeito no mundo físico.

Como se defender

Para a **nuvem**: ative a verificação em dois passos, não deixe pastas ou arquivos públicos sem necessidade, dê acesso só a quem precisa e revise de tempos em tempos quem tem permissão. Para o **celular**: mantenha o sistema atualizado, baixe apenas das lojas oficiais, use bloqueio de tela com senha ou biometria, peça à operadora um bloqueio contra troca de chip, ative o recurso de localização e apagamento remoto, e desconfie de pedidos de códigos por mensagem. Para os **aparelhos conectados**: troque a senha de fábrica no primeiro dia, instale as atualizações, compre de marcas com suporte conhecido e, se possível, coloque-os numa rede separada da rede onde você usa o computador e o banco. Muitos roteadores têm uma "rede de convidados" que serve exatamente para isso.

Na prática: o censo da sua casa

Faça uma lista de tudo o que, na sua casa, está ligado à internet. Você vai se surpreender com o tamanho. Para cada item, responda: troquei a senha de fábrica? Recebe atualizações? Se a resposta for não, esse é o próximo item da sua lista de tarefas de segurança.

Capítulo 11: Criptografia, o cadeado invisível da internet

Quando Júlio César queria mandar uma ordem secreta a um general, trocava cada letra da mensagem pela que vinha três casas depois no alfabeto: o A virava D, o B virava E. Quem interceptasse o recado veria um amontoado sem sentido. Só o general, que sabia a regra, desfazia a troca. É um dos exemplos mais antigos de criptografia, a arte de esconder mensagens, e a base de tudo o que protege seus dados hoje.

A criptografia é a principal defesa dos três pilares do capítulo 1 quando os dados estão em trânsito ou guardados. Ela embaralha a informação de um jeito que só quem tem a chave certa consegue desembaralhar. Você a usa dezenas de vezes por dia, sem perceber, toda vez que abre um site com o cadeado, manda uma mensagem de WhatsApp ou paga com o celular.

Duas famílias de chaves

Na **criptografia simétrica**, a mesma chave tranca e destranca, como a chave de uma porta. É muito rápida e serve para proteger grandes quantidades de dados, mas tem um problema: como entregar a chave a quem vai receber sem que ninguém a copie no caminho? Esse problema ficou sem solução prática por séculos.

A solução veio nos anos 1970 com a **criptografia assimétrica**, ou de chave pública. Cada pessoa tem um par de chaves matematicamente ligadas: uma **pública**, que pode ser distribuída a qualquer um, e uma **privada**, que fica só com o dono. O que uma chave tranca, só a outra destranca. Quem quer mandar um segredo usa a chave pública do destinatário para trancar, e só a chave privada dele abre. É como um cadeado aberto que qualquer pessoa pode fechar, mas só o dono tem a chave. Esse mesmo par de chaves também permite a **assinatura digital**: quem assina com a chave privada prova que a mensagem veio dele e não foi alterada.



Figura 11.1 · chave pública e chave privada

O cadeado pode circular à vontade, porque só serve para trancar. A segurança inteira repousa em manter a chave privada longe de todos.

O cadeado do navegador

Quando você abre um site com cadeado, e o endereço começa com "https", seu navegador e o site fazem em milissegundos um acordo: usam criptografia assimétrica para combinar uma chave simétrica de uso único, e depois conversam com ela. Ninguém que estiver no meio do caminho, do Wi-Fi do café ao provedor, consegue ler o conteúdo. Para ter certeza de que o site é mesmo o que diz ser, e não um impostor, o navegador confere um **certificado digital**, um documento assinado por uma entidade de confiança que confirma a quem pertence aquele endereço. Se algo estiver errado, ele mostra um aviso na tela inteira, e esse aviso merece ser levado a sério.

Um cuidado importante: o cadeado diz que a **conexão** é privada, não que o site é honesto. Sites de golpe também têm cadeado. Ele impede a escuta no caminho, mas não impede você de entregar sua senha a um site falso.

Onde mais a criptografia aparece

A **VPN** cria um túnel criptografado entre seu aparelho e um servidor, escondendo o tráfego de quem está no meio. O **WhatsApp e outros aplicativos** usam a chamada criptografia de ponta a ponta: só você e o destinatário têm as chaves, e nem a empresa consegue ler. A **criptografia de disco**, hoje ligada por padrão em muitos celulares, embaralha tudo o que está guardado, de modo que um aparelho roubado não entrega seus dados sem a senha. E os **hashes**, que vimos no capítulo 3, usam uma matemática de mão única para guardar senhas.

Os limites da criptografia

A matemática da criptografia moderna é muito sólida. Quase nunca é ela que é quebrada: o que se quebra é o resto, ou seja, a chave mal guardada, a senha fraca, o programa com falha ou a pessoa enganada. Existe ainda uma preocupação de longo prazo com os futuros computadores quânticos, que poderiam quebrar parte dos métodos atuais, e a indústria já trabalha em métodos novos, chamados de pós-quânticos, para se antecipar a isso.

Na prática: confira o cadeado de verdade

Antes de digitar uma senha num site, olhe o endereço inteiro, e não só o cadeado. Confira se a parte que vem logo antes do primeiro "/" é mesmo o nome do serviço. Em seguida, no seu celular, confirme que o bloqueio de tela está ligado, o que na maioria dos aparelhos modernos ativa a criptografia dos dados guardados.

Capítulo 12: Defesa em camadas, nenhuma porta sozinha basta

Os castelos medievais não dependiam de uma só muralha. Havia o fosso, a ponte levadiça, o portão, o pátio, a torre, as sentinelas. Se o inimigo passava por uma barreira, encontrava outra. A segurança digital funciona do mesmo jeito, e o nome tradicional dessa ideia é **defesa em profundidade**: várias camadas, de modo que a falha de uma não entregue tudo.

Você viu defesas isoladas ao longo do livro, como o segundo fator no capítulo 3, as atualizações no capítulo 8 e a criptografia no capítulo 11. Este capítulo mostra como elas se encaixam e acrescenta as que ainda faltam. A lógica é sempre a mesma: **prevenir** o que for possível, **detectar** o que passou e **responder** rápido ao que não pôde ser evitado.

As camadas

A primeira camada é a das **pessoas**: treinamento, regras claras e cultura de avisar sobre erros. A segunda é a da **identidade**: senhas fortes e únicas, verificação em dois passos e acessos mínimos, o que vimos nos capítulos 3 e 9. A terceira é a do **aparelho**: sistema e programas atualizados, antivírus e proteção contra comportamentos suspeitos e criptografia do disco.

A quarta é a da **rede**. O **firewall** funciona como um porteiro que só deixa passar o tráfego permitido por regras. A **segmentação** divide a rede em compartimentos, como as divisórias de um navio: se um deles for invadido, os outros continuam secos. O princípio mais recente, chamado de **confiança zero** (zero trust), diz que ninguém e nenhum aparelho é confiável só porque está dentro da rede: cada acesso é conferido, sempre. A quinta é a dos **dados**: criptografia, controle de quem pode ver o quê e, acima de tudo, as **cópias de segurança** que vimos no capítulo 5.

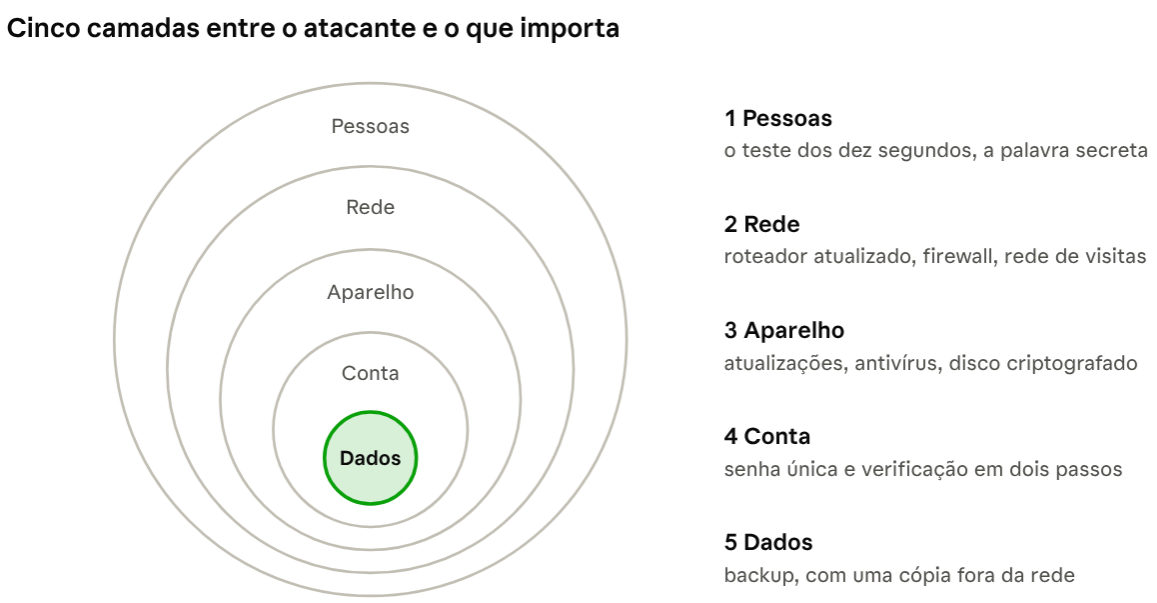


Figura 12.1 · defesa em camadas, de fora para dentro

Nenhuma camada é perfeita. O que protege é que, quando uma falha, a seguinte ainda está de pé.

Detectar: ver o que passou

Nenhuma barreira é perfeita, e um atacante que passou precisa ser percebido logo. Os **registros** (logs) guardam o que aconteceu nos sistemas: quem entrou, de onde, a que horas. Programas chamados de **EDR**, de detecção e resposta nos aparelhos, observam o comportamento de cada computador e conseguem isolar um deles da rede quando algo parece errado. O **SIEM** reúne os registros de toda a empresa num lugar só e cruza informações para achar padrões suspeitos, como um funcionário que entra no sistema de manhã em São Paulo e dez minutos depois em outro país. Muitas empresas têm um centro de operações de segurança, o **SOC**, com pessoas olhando esses alertas dia e noite. Para quem não tem uma equipe, serviços contratados fazem isso por eles.

Quem ataca contra quem defende

A tabela a seguir junta os ataques dos capítulos anteriores com a principal defesa de cada um. Ela serve como mapa de consulta: quando um ataque aparecer no noticiário, você sabe onde procurar a defesa.

Ataque	Pilar atingido	Defesa principal
Phishing e engenharia social	Confidencialidade	Confirmar por outro canal, treinamento

Ataque	Pilar atingido	Defesa principal
Força bruta e credential stuffing	Confidencialidade	Senhas únicas, verificação em dois passos
Malware, vírus, trojan	Todos	Atualizações, antivírus, não instalar de fontes duvidosas
Ransomware	Disponibilidade	Backup 3-2-1, segmentação
Sniffing e homem no meio	Confidencialidade e integridade	Criptografia (https, VPN)
DDoS	Disponibilidade	Proteção contra DDoS, redundância
Injeção e XSS	Todos	Código seguro, validação, testes
Falhas conhecidas e zero-day	Todos	Atualizar rápido, camadas, menor privilégio
Ameaça interna	Confidencialidade e integridade	Menor privilégio, registros, revogação rápida
Nuvem e IoT mal configurados	Todos	Configuração revisada, senhas trocadas

Na prática: as camadas da sua casa

Desenhe cinco círculos concêntricos: você no centro, depois suas contas, depois seus aparelhos, depois sua rede de casa, depois os serviços na nuvem. Para cada anel, escreva uma defesa que você já tem e uma que falta. O desenho mostra, de relance, onde a sua fortaleza tem um muro fino.

Capítulo 13: Quando acontece, resposta a incidentes e a lei

Sábado, três da manhã. O celular da gerente de TI de uma rede de lojas vibra com um alerta: um servidor está enviando uma quantidade estranha de dados para fora. Ela tem poucos minutos para decidir. Desligar o servidor? Isso pode apagar pistas. Deixar ligado? Os dados continuam saindo. Ninguém aprende a decidir isso na hora, e por isso as empresas que se saem bem são as que ensaiaram antes.

Ninguém consegue evitar todos os ataques. O que separa um susto de uma catástrofe é o que acontece nas primeiras horas depois de descobrir o problema. Esse trabalho se chama **resposta a incidentes**.

As seis etapas

A prática internacional organiza a resposta em etapas, que formam um ciclo. Na **preparação**, feita antes de qualquer problema, definem-se quem faz o quê, quem pode decidir, quais são os telefones de emergência e onde estão os backups. Na **identificação**, a equipe confirma que houve mesmo um incidente e descobre o tamanho: o que foi atingido, desde quando. Na **contenção**, isola-se o que foi afetado para impedir que o problema se espalhe, desconectando máquinas da rede, bloqueando contas, trocando senhas. Na **erradicação**, remove-se a causa: o programa malicioso, a conta invadida, a falha explorada. Na **recuperação**, os sistemas voltam ao ar com cuidado, usando as cópias de segurança limpas, e são monitorados de perto. E nas **lições aprendidas**, a equipe se reúne sem procurar culpados e pergunta como evitar o próximo.

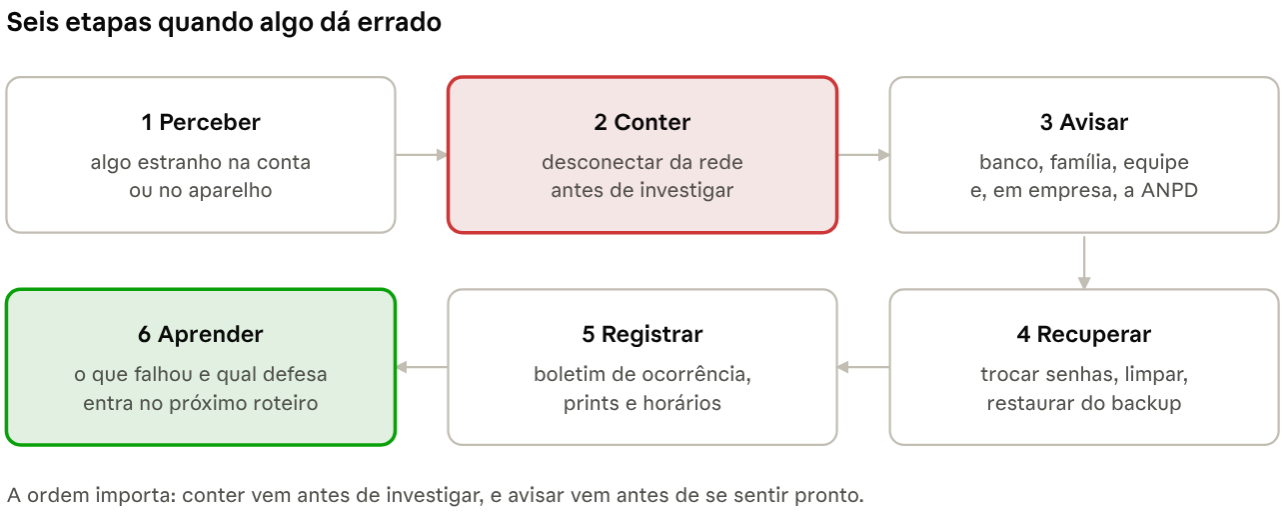


Figura 13.1 · as seis etapas da resposta a um incidente

A etapa 6 fecha o ciclo: o que você aprende vira o primeiro item do próximo roteiro de proteção.

A perícia digital

Em paralelo, especialistas em **perícia digital** (forense) tentam responder a perguntas: por onde o atacante entrou, o que fez, o que levou, quando. Eles preservam evidências, como cópias exatas de discos e registros de acesso, sem alterá-las, porque podem ser necessárias na Justiça. Por isso, um erro comum de amadores é formatar logo o computador infectado: o desejo de limpar apaga justamente as pistas.

O que dizer, a quem e quando

Na hora da crise, a comunicação conta quase tanto quanto a técnica. A empresa precisa avisar a diretoria, os clientes afetados e, em muitos casos, as autoridades. Mentir, minimizar ou demorar costuma piorar a reação de todos: a imprensa, os clientes e a

Justiça. No Brasil, a **LGPD**, Lei Geral de Proteção de Dados, em vigor desde 2020, obriga as empresas que cuidam de dados pessoais a protegê-los e, quando houver um incidente que possa causar risco ou dano relevante às pessoas, a comunicá-lo à **ANPD**, a Autoridade Nacional de Proteção de Dados, e aos titulares afetados. A lei prevê multas e outras sanções para quem não protege e não avisa. Outros países têm leis parecidas, como o GDPR, na Europa.

Você também tem direitos: saber quais dados uma empresa guarda sobre você, corrigi-los e, em muitos casos, pedir que sejam apagados. Se seus dados forem expostos, vale trocar as senhas dos serviços afetados, ativar a verificação em dois passos, desconfiar de mensagens que usem informações suas e acompanhar o extrato do banco.

Se acontecer com você

No nível pessoal, o roteiro é pequeno. Se perceber que foi enganado ou invadido: avise o banco imediatamente pelos canais oficiais para bloquear cartões e contas, troque as senhas a partir de um aparelho limpo, ative a verificação em dois passos, avise seus contatos se uma conta sua estiver sendo usada para golpes e registre um boletim de ocorrência, que pode ser feito online em muitos estados. Quanto mais rápido, menor o estrago, e nada disso é motivo de vergonha: golpes fazem vítimas de todas as idades e níveis de instrução.

Na prática: o cartão de emergência

Escreva num papel, e guarde na carteira ou numa gaveta, os telefones oficiais do seu banco, da operadora do seu celular e do seu provedor de e-mail, e uma frase: "se perceber algo estranho, bloquear cartões e trocar a senha do e-mail primeiro". Na hora do susto, ninguém pensa direito, e um papel pronto faz essa conta por você.

Capítulo 14: Inteligência artificial, deepfakes e o futuro da segurança

Uma analista financeira de uma empresa recebeu o convite para uma videochamada com o diretor e outros colegas. Na tela, todos estavam ali, com rostos e vozes conhecidos, e o diretor pediu uma transferência urgente e confidencial. Ela fez. Depois descobriu que ninguém naquela chamada era real: os rostos e as vozes tinham sido gerados por computador. Um caso desse tipo foi noticiado em 2024, envolvendo uma empresa em Hong Kong e uma perda de dezenas de milhões de dólares. O mundo em que ver e ouvir era prova de que alguém estava presente acabou.

A inteligência artificial entrou nos dois lados da segurança. Ela dá ao atacante ferramentas novas e aperfeiçoa as velhas, e dá ao defensor meios de enxergar padrões que humanos não perceberiam. Este capítulo mostra os dois lados.

O que a IA muda para quem ataca

A primeira mudança é de **qualidade e escala** dos golpes. Os e-mails de phishing sempre tiveram um ponto fraco: erros de português e frases estranhas denunciavam a fraude. Com programas que escrevem bem, esse sinal desapareceu, e as mensagens podem ser adaptadas a cada vítima em segundos, com nome, empresa e assunto reais colhidos na internet. O spear phishing, que antes exigia horas de trabalho por alvo, ficou barato.

A segunda é o **deepfake**, palavra que junta "aprendizado profundo" e "falso": vídeos, fotos e áudios sintéticos que imitam pessoas reais. Basta uma amostra curta da voz de alguém para gerar uma voz convincente, e já existem golpes em que um parente "liga" pedindo dinheiro com a voz clonada. A terceira é a **automação**: a IA ajuda a ler código em busca de falhas, a escrever programas e a conduzir conversas com vítimas em massa, o que baixa a barreira de entrada para atacantes menos técnicos.

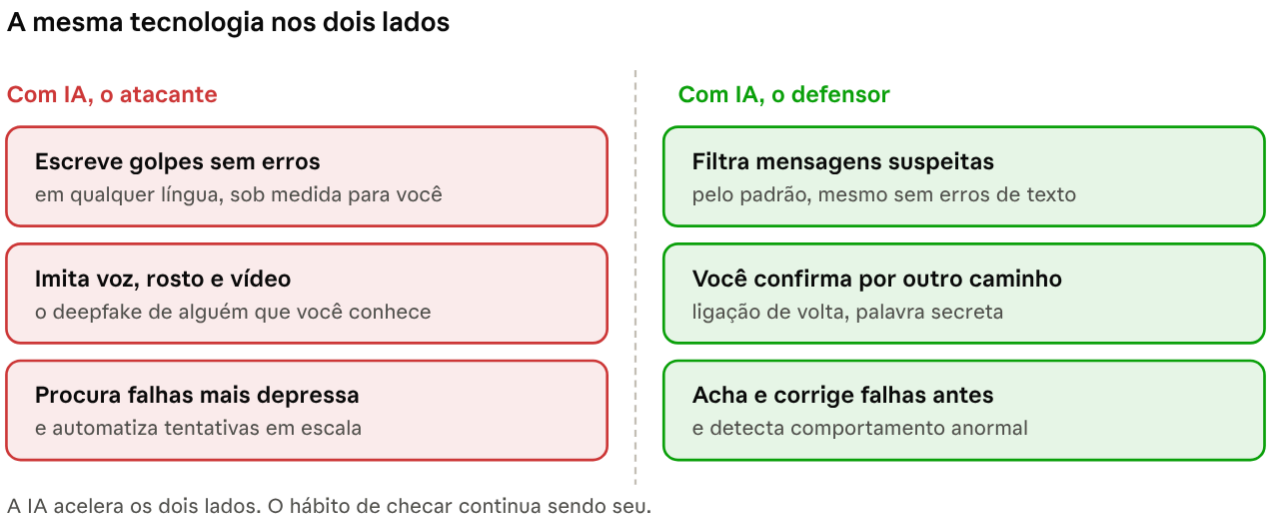


Figura 14.1 · o espelho da inteligência artificial: atacante e defensor

Cada vantagem do atacante tem um espelho do lado de quem defende. O que não muda é a regra de ouro: o pedido urgente se confirma por outro caminho.

Ataques contra os próprios sistemas de IA

Os sistemas de IA também são alvos. A **injeção de instruções** (prompt injection) acontece quando um texto escondido numa página, num e-mail ou num documento tenta dar ordens ao assistente de IA que o lê, para fazer com que vaze informações ou execute ações que o usuário não pediu. O **envenenamento de dados** corrompe os exemplos com que um modelo aprende, para que ele erre de um jeito escolhido pelo atacante. E o **vazamento por**

conversa acontece quando pessoas colam dados sensíveis de empresas em ferramentas de IA sem saber o que será feito deles. A regra é a mesma dos outros capítulos, com um acréscimo: trate o que uma IA lê como não confiável e dê a ela o mínimo de poderes necessários.

O que a IA muda para quem defende

Do lado da defesa, a IA ajuda a **detectar anomalias**: aprender o comportamento normal de uma rede ou de um usuário e acender o alerta quando algo foge dele, como um acesso às três da manhã de um lugar nunca visto. Ajuda a **filtrar** spam, phishing e malware em volumes que nenhuma equipe humana conseguiria ler, a **priorizar** milhares de alertas por dia, a **acelerar** a investigação de incidentes resumindo registros e sugerindo causas, e a encontrar falhas no código antes de o programa ser lançado. A segurança vira uma corrida em que os dois lados usam as mesmas ferramentas, e a vantagem muda de mão conforme quem se prepara melhor.

Como se proteger de golpes com IA

A defesa pessoal mais eficaz contra deepfakes não é técnica: é **não confiar em imagem e voz como prova única**. Combine com a família uma **palavra secreta**, que só vocês conhecem, para pedidos de dinheiro urgentes. Em empresas, exija que pedidos incomuns de pagamento sejam confirmados por um segundo canal e por duas pessoas, não importa quem peça. Desconfie de urgência, mesmo com voz conhecida. E desconfie de vídeos e áudios chocantes que circulam sem fonte: antes de compartilhar, procure a mesma notícia em veículos de confiança.

Para onde isso caminha

O futuro próximo da segurança tem três tendências claras. As **senhas vão diminuir**, substituídas por passkeys e biometria. A **autenticação contínua** vai conferir quem você é durante o uso, e não só na entrada. E a **comprovação de origem** de conteúdos, com assinaturas digitais que mostram quem criou uma imagem ou um vídeo e se foi alterado, deve virar parte do dia a dia. Mas a base continua a mesma: sistemas atualizados, acessos mínimos, cópias de segurança e pessoas que sabem parar e confirmar.

Na prática: a palavra da família

Conversem hoje, em família, e escolham uma palavra ou uma pergunta que só vocês conhecem, algo que não esteja em nenhuma rede social. Combinem que qualquer pedido urgente de dinheiro, por mais convincente que a voz ou o rosto seja, só vale se a palavra for dita. É o golpe mais fácil de bloquear de todo o livro.

Capítulo 15: Guia por sistema, como se proteger no Windows, macOS, Linux, Android e iPhone

Os princípios dos capítulos anteriores valem em qualquer aparelho, mas cada sistema tem seus recursos de proteção, seus nomes de menu e seus pontos fracos típicos. Este capítulo é um guia de consulta: para cada sistema, o que já vem pronto e só precisa ser ligado, o que vale configurar e onde costuma estar o golpe. Os nomes dos menus mudam entre versões, então procure pela função na busca das configurações se não achar o nome exato.

Antes de entrar em cada sistema, guarde a regra que vale para todos: **o aparelho mais seguro é o que recebe atualizações**. Um celular ou computador que o fabricante abandonou é uma porta aberta, por melhor que seja o resto da proteção.

Onde cada sistema costuma ser enganado

Sistema	Por onde o golpe costuma entrar	Primeira defesa
Windows	anexos e instaladores falsos	atualizar e não abrir o inesperado
macOS	programas baixados fora da loja	manter o Gatekeeper ligado
Linux	pacotes fora dos repositórios oficiais	instalar só de fontes confiáveis
Android	aplicativos fora da Play e permissões demais	usar a Play e revisar permissões
iPhone	phishing e códigos entregues por engano	nunca dizer o código a ninguém

Figura 15.1 · por onde cada sistema costuma ser enganado e a primeira defesa

Em todos os cinco, o ponto fraco mais comum não é o sistema, mas a decisão de quem o usa. Por isso os roteiros que se seguem começam pelo que mais pesa em cada um.

Windows

O Windows é o sistema mais usado em computadores e, por isso, o mais visado. A boa notícia é que ele traz de fábrica quase tudo de que um usuário comum precisa.

Mantenha o **Windows Update** em automático e não adie as atualizações por semanas. Confirme que o **Segurança do Windows** (o antigo Windows Defender) está ativo, com a proteção em tempo real e o **SmartScreen**, que avisa sobre sites e arquivos perigosos. Mantenha o **firewall** ligado. Ative a **proteção contra ransomware**, o recurso de acesso controlado a pastas, que impede programas desconhecidos de alterar suas pastas de documentos. Use o **Windows Hello** (PIN, digital ou rosto) para entrar, e ative a **criptografia**

do dispositivo ou o **BitLocker**, conforme a edição do Windows, para que um notebook roubado não entregue seus arquivos. No dia a dia, trabalhe com uma **conta comum** e deixe a conta de administrador só para instalar programas. Ative a exibição das **extensões de arquivo**, porque um "relatorio.pdf.exe" parece um PDF mas é um programa. Faça backup com o histórico de arquivos, com uma cópia na nuvem ou com um disco externo desconectado.

O ponto mais fraco costuma ser o **programa baixado de fontes duvidosas**: cracks, ativadores, instaladores "grátis" de aplicativos pagos. Evite-os. Desconfie também de anexos do Office que pedem para "habilitar conteúdo" ou "habilitar macros": isso quase sempre é o início de uma infecção. E atenção ao fim do suporte: o Windows 10 deixou de receber as atualizações gratuitas de segurança em outubro de 2025, e quem continua nele deve migrar de versão ou verificar as opções oficiais do fabricante.

Roteiro de proteção para Windows. Faça na ordem, em cerca de meia hora, marcando cada passo:

- [ ] Abra as Configurações, procure por "Windows Update" e busque atualizações. Instale tudo e ligue a opção de receber as atualizações assim que estiverem disponíveis.
- [ ] Procure por "Segurança do Windows" e confirme que as áreas "Proteção contra vírus e ameaças" e "Firewall" estão com o sinal verde. Se aparecer aviso amarelo ou vermelho, clique e siga a correção indicada.
- [ ] Dentro de "Proteção contra vírus e ameaças", ligue a proteção contra ransomware e escolha as pastas de documentos e fotos para ficarem protegidas.
- [ ] Crie uma conta comum, sem poderes de administrador, para o uso diário. Deixe a conta de administrador só para instalar programas, com senha forte.
- [ ] Configure o Windows Hello (PIN, digital ou rosto) e ative a criptografia do dispositivo ou o BitLocker, se sua versão oferecer.
- [ ] No Explorador de Arquivos, abra "Exibir" e marque a exibição das extensões de arquivo.
- [ ] Copie seus documentos e fotos para um disco externo ou para a nuvem e, no caso do disco, desconecte-o depois.
- [ ] Desinstale programas que você não conhece ou não usa e, a partir de agora, instale apenas de fontes oficiais.

macOS

O sistema dos computadores da Apple tem fama de ser "imune a vírus", e isso é um mito perigoso. O macOS é bem projetado, mas também é atacado, e os golpes de engenharia social funcionam nele tanto quanto em qualquer outro.

Ligue as **atualizações automáticas** em Atualização de Software. Mantenha ativos o **Gatekeeper**, que só deixa abrir programas de fontes confiáveis, e o **XProtect**, a proteção integrada contra malware, ambos já ligados por padrão e que não devem ser desativados. Ative o **FileVault**, que criptografa o disco inteiro, e o **firewall**. Use o **Touch ID** e exija a senha ao sair da proteção de tela. Ative o **Buscar**, que localiza o aparelho perdido e permite apagá-lo à distância. Faça backup com o **Time Machine** em um disco externo ou use o iCloud. No Safari e no navegador que usar, mantenha o bloqueio de janelas e de rastreadores ligado.

O ponto mais fraco é o **instalador fora da loja oficial**, principalmente quando uma janela pede sua senha de administrador para "liberar" algo, e as janelas falsas de "seu Mac está infectado" que levam a instalar um suposto antivírus. Instale programas pela App Store ou diretamente do site do desenvolvedor e desconfie de qualquer coisa que peça para você contornar as proteções do sistema.

Roteiro de proteção para macOS. Cerca de vinte minutos:

- [ ] Abra os Ajustes do Sistema, entre em "Geral" e depois em "Atualização de Software". Instale o que estiver pendente e ligue as atualizações automáticas.
- [ ] Em "Privacidade e Segurança", ative o FileVault, que protege o disco inteiro, e anote a chave de recuperação num lugar seguro, fora do computador.
- [ ] Ainda em "Privacidade e Segurança", confirme que o computador só abre apps da App Store ou de desenvolvedores identificados, e não mude isso para atender a uma janela que pede.
- [ ] Em "Rede", ligue o firewall.
- [ ] Cadastre o Touch ID e, em "Tela Bloqueada", exija a senha logo ao sair da proteção de tela.
- [ ] Nos ajustes do seu ID Apple, ative o Buscar, e confirme que a verificação em dois fatores está ligada.
- [ ] Conecte um disco externo e configure o Time Machine, ou ligue o backup no iCloud.
- [ ] Revise em "Privacidade e Segurança" quais apps têm acesso à câmera, ao microfone e à localização, e retire o que não faz sentido.

Linux

O Linux é usado em servidores e por quem o escolhe no computador de casa. Ele costuma ser mais resistente a golpes automatizados, em parte porque tem menos usuários comuns e em parte por seu projeto, mas "não tem vírus" é outro mito: existem malwares para Linux, e servidores são alvos frequentes.

A base é usar o **gerenciador de pacotes** da sua distribuição para instalar tudo a partir dos repositórios oficiais, e manter as atualizações em dia, com as de segurança automáticas ligadas quando a distribuição oferecer. Escolha a **criptografia de disco** (normalmente o LUKS) na hora da instalação, porque ligar depois é trabalhoso. Mantenha o **firewall** ativo, com uma ferramenta simples como o UFW ou o firewalld, e desligue os serviços que você não usa. Use sua conta comum no dia a dia e o **sudo** só quando necessário, lendo o que está sendo executado. Faça backup com ferramentas como Timeshift, Déjà Dup ou rsync. Se ativar acesso remoto por SSH, use chaves em vez de senha e restrinja quem pode entrar.

O ponto mais fraco é o **comando copiado da internet**: tutoriais que mandam colar uma linha no terminal, sobretudo as que baixam e executam um script de uma só vez, dão ao script os mesmos poderes que você tem. Só execute o que você entende e vem de fonte confiável. O mesmo vale para repositórios e pacotes não oficiais.

Roteiro de proteção para Linux. Cerca de vinte minutos. Os nomes dos programas mudam entre distribuições, então busque a função no menu da sua:

- [ ] Abra o gerenciador de atualizações ou de software da sua distribuição e instale tudo o que estiver pendente. Se ele oferecer atualizações automáticas de segurança, ligue.
- [ ] Confirme que o disco está criptografado. Se não estiver, o melhor momento para ativar é na próxima reinstalação, escolhendo a criptografia de disco no instalador.
- [ ] Ative o firewall pelo aplicativo gráfico que sua distribuição oferece, ou pelo UFW.
- [ ] Use sua conta comum para o dia a dia e só chame o sudo quando souber o que o comando faz.
- [ ] Instale programas apenas pelos repositórios e lojas oficiais da distribuição, e evite adicionar repositórios de terceiros sem necessidade.
- [ ] Nunca cole no terminal um comando de um tutorial sem entender o que ele faz, principalmente se baixa e executa um script.
- [ ] Desative serviços que você não usa, como compartilhamentos de rede e acesso remoto.
- [ ] Configure cópias automáticas com uma ferramenta como Timeshift ou Déjà Dup, para um disco externo.

Android

O Android é o sistema de celular mais usado do mundo, e o que mais varia: há centenas de marcas, e nem todas atualizam seus aparelhos por muito tempo.

Mantenha o **sistema** e o **Google Play** atualizados, e ligue o **Google Play Protect**, que examina os aplicativos instalados. Use bloqueio de tela com senha, PIN ou biometria, e deixe o **Encontre Meu Dispositivo** ativo. Instale aplicativos **apenas da Google Play** e

nunca marque a opção de instalar de fontes desconhecidas, a menos que saiba exatamente o que está fazendo. Revise as **permissões** de cada aplicativo e retire as que não fazem sentido. Faça backup das fotos e dos dados na conta Google ou em outro serviço. Peça à operadora o bloqueio contra troca de chip e, no aplicativo do banco, defina **limites para o Pix**, especialmente no período da noite.

O ponto mais fraco aparece em dois golpes muito comuns no Brasil. O primeiro é o **aplicativo falso, instalado por um link** enviado em mensagem, que promete benefício, aumento de limite ou pagamento. O segundo é o pedido para ativar a **acessibilidade** ou o **compartilhamento de tela** para um "atendente": esses recursos dão a um programa o poder de ler a tela e agir em seu nome, e só devem ser concedidos a aplicativos que você instalou de propósito e conhece. Nenhum banco legítimo pede isso por telefone. Por fim, lembre que um aparelho sem atualizações do fabricante deve ser trocado.

Roteiro de proteção para Android. Cerca de vinte minutos. Os menus variam por marca; use a busca das Configurações:

- [ ] Em Configurações, procure por "Atualização do sistema" e instale o que houver. Depois abra a Google Play, entre nas configurações e atualize também os aplicativos.
- [ ] Na Google Play, abra "Play Protect" e confirme que a verificação de aplicativos está ligada.
- [ ] Defina um bloqueio de tela forte, com PIN longo, senha ou biometria, e deixe o bloqueio automático em pouco tempo.
- [ ] Ative o "Encontre Meu Dispositivo" e teste, num outro aparelho, se o seu aparece.
- [ ] Confirme que a instalação de apps de fontes desconhecidas está desativada.
- [ ] Abra "Apps" e desinstale o que não usa. Nos que ficam, revise as permissões, e verifique quais aplicativos têm acesso à acessibilidade: se algum for desconhecido, desative.
- [ ] Ative a verificação em dois passos na conta Google, e ligue o backup das fotos e dos dados.
- [ ] No aplicativo do banco, defina limites para o Pix, principalmente à noite, e ligue o alerta de cada transação. Ligue para a operadora e peça o bloqueio contra troca de chip.

iPhone e iPad (iOS)

O iPhone traz uma defesa forte de fábrica: os aplicativos rodam isolados uns dos outros, só chegam pela App Store e a Apple controla as atualizações de todos os aparelhos compatíveis. Isso reduz muito o risco, mas não o elimina, principalmente contra golpes que enganam a pessoa.

Mantenha o **iOS** em atualização automática. Use um **código de desbloqueio de seis dígitos ou mais**, ou uma senha alfanumérica, além do Face ID ou Touch ID. Proteja o **ID Apple** com a verificação em dois fatores e guarde com cuidado as chaves de recuperação: quem controla o ID Apple controla o aparelho. Ative o **Buscar**, e nas versões recentes ligue a **Proteção de Dispositivo Roubado**, que exige o rosto ou a digital, e não apenas o código, para mudar configurações sensíveis fora de locais conhecidos. Revise as **permissões** e o relatório de privacidade dos aplicativos. Faça backup no iCloud ou no computador. Para quem corre risco elevado, como jornalistas e ativistas, existe o **Modo de Isolamento**, que reduz drasticamente o que o aparelho aceita. E quem teme ser vigiado por alguém próximo pode usar a **Verificação de Segurança**, que mostra e permite encerrar compartilhamentos de localização e de dados.

O ponto mais fraco é o **phishing do ID Apple**: mensagens e e-mails que dizem que sua conta foi bloqueada ou que um aparelho foi encontrado, levando a uma página falsa. Também há os golpes em que alguém pede o código de seis dígitos que chega ao seu aparelho. Não o informe a ninguém, e nunca instale "perfis de configuração" ou certificados enviados por desconhecidos.

Roteiro de proteção para iPhone e iPad. Cerca de quinze minutos:

- [ ] Abra Ajustes, entre em "Geral" e "Atualização de Software". Instale o que estiver pendente e ligue as atualizações automáticas.
- [ ] Em "Face ID e Código" (ou "Touch ID e Código"), troque o código por um de seis dígitos ou mais, ou por uma senha alfanumérica.
- [ ] Toque no seu nome, no topo dos Ajustes, e confirme que a autenticação de dois fatores do ID Apple está ligada. Anote a chave de recuperação, se tiver criado uma, num lugar seguro.
- [ ] Ainda ali, em iCloud, confirme que o Buscar está ativo, e nas versões recentes ligue a Proteção de Dispositivo Roubado, em "Face ID e Código".
- [ ] Em "Privacidade e Segurança", revise quais aplicativos têm acesso à câmera, ao microfone, à localização e às fotos, e retire o que não faz sentido.
- [ ] Ligue o backup do iCloud, ou conecte o aparelho a um computador de vez em quando e faça a cópia.
- [ ] Apague aplicativos que não usa e nunca instale perfis de configuração enviados por mensagem ou por desconhecidos.
- [ ] Combine consigo mesmo a regra: o código de seis dígitos que chega ao aparelho nunca é dito a ninguém, nem a quem diga ser da Apple ou do banco.

Roteiros por tema: Internet, redes sociais, e-mail e conexões

Roteiro de proteção na Internet. Vale para qualquer aparelho, e leva cerca de vinte minutos:

- [ ] Use um navegador atualizado (Chrome, Firefox, Edge, Safari ou Brave) e ligue as atualizações automáticas dele e das extensões. Apague as extensões que você não reconhece.
- [ ] Antes de digitar senha ou número de cartão, olhe o endereço: ele deve começar com https e o nome do site deve estar escrito certo. Em dúvida, digite o endereço você mesmo ou use o aplicativo oficial.
- [ ] Não entre em sites de banco, loja ou governo clicando em links de mensagens, anúncios ou resultados patrocinados de busca. Salve os endereços que você realmente usa nos favoritos.
- [ ] Ative a verificação em dois passos no e-mail, nas redes sociais e nos serviços de compra, e use um gerenciador de senhas para ter uma senha diferente em cada site.
- [ ] Desconfie de qualquer janela que diga que seu aparelho está infectado, que você ganhou um prêmio ou que precisa instalar algo para ver um vídeo. Feche a aba, e nunca baixe programas fora das lojas oficiais ou do site do fabricante.
- [ ] Nas compras, prefira cartão virtual ou um meio de pagamento com proteção ao comprador. Desconfie de preço muito abaixo do normal, de pagamento só por Pix a desconhecidos e de lojas sem CNPJ ou canal de atendimento claro.
- [ ] Nas redes sociais, deixe o perfil restrito a quem você conhece, revise quem pode ver suas fotos e dados, e não publique documentos, bilhetes, cartões nem a fachada de casa com a rota da sua rotina.
- [ ] Em Wi-Fi público, evite banco e compras, e ligue o navegador para avisar quando uma página não for segura. Se precisar, use o plano de dados do celular.
- [ ] Procure seu e-mail em um serviço de vazamentos, como o Have I Been Pwned. Se aparecer, troque a senha daquele site e de qualquer outro onde a tenha repetido.
- [ ] Combine consigo mesmo: se algo na tela cria pressa, medo ou promessa boa demais, pare, saia do site e confirme por outro caminho.

Roteiro de proteção nas redes sociais e nos aplicativos de mensagem (WhatsApp, Facebook, Instagram, TikTok e outros). Cerca de vinte minutos, em cada aplicativo que você usa:

- [ ] Ligue a verificação em dois passos em cada conta. No WhatsApp, é em Configurações, Conta, Confirmação em duas etapas, com um PIN de seis dígitos que você nunca informa a ninguém. No Facebook, Instagram e TikTok, procure "Segurança" ou "Senha e segurança" nas configurações.
- [ ] Use uma senha diferente em cada rede, guardada no gerenciador de senhas. Se uma rede vazar, as outras não caem junto.
- [ ] Nunca diga a ninguém o código de seis dígitos que chega por SMS ou pelo próprio aplicativo. Quem pede esse código está tentando entrar na sua conta, mesmo que seja um amigo ou um "suporte".

- [ ] No WhatsApp, em Privacidade, limite quem vê sua foto, seu recado e suas informações a "Meus contatos", e escolha quem pode adicionar você a grupos. Isso reduz convites de desconhecidos e golpes em grupos.
- [ ] Desconfie de mensagem de número desconhecido com foto de conhecido, "troquei de número" ou pedido urgente de dinheiro. Antes de pagar, ligue para a pessoa no número antigo ou combine a palavra secreta da família.
- [ ] Não clique em links de promoções, premiações, "veja quem visitou seu perfil" ou "seu perfil será banido". Esses links levam a páginas falsas de login. Para tratar de algo da conta, abra o aplicativo, não o link.
- [ ] No Instagram, Facebook e TikTok, deixe o perfil privado se não precisa ser público, aceite só quem você conhece e revise quem pode comentar, marcar e enviar mensagens.
- [ ] Revise os dispositivos conectados e os "aparelhos ativos" em cada conta (no WhatsApp, Aparelhos conectados). Desconecte o que não reconhece e confira com frequência o WhatsApp Web.
- [ ] Em Configurações, revise os aplicativos e sites ligados à sua conta ("Entrar com o Facebook", por exemplo) e remova os que não usa.
- [ ] Cuidado com vídeos e áudios de pessoas pedindo dinheiro ou apoio: podem ser deepfakes. Desconfie de ofertas de ganho fácil, de investimento com retorno garantido e de perfis de celebridades que mandam mensagem direta.
- [ ] Pense no que publica: fotos de documentos, passagens, cartões, crachás e a fachada da sua casa ajudam golpistas. Evite informar o período em que a casa ficará vazia.
- [ ] Se a conta for invadida: avise seus contatos por outro canal, use a opção "Minha conta foi hackeada" ou a recuperação de acesso do próprio aplicativo, troque a senha e registre um boletim de ocorrência. Para crianças e adolescentes, ative os controles parentais e converse sobre quem pode falar com eles.

Roteiro de proteção do e-mail. O e-mail é a chave de todas as outras contas, porque é por ele que se recupera qualquer senha. Cerca de quinze minutos:

- [ ] Proteja primeiro a conta de e-mail: senha longa e única, que não seja usada em nenhum outro lugar, e verificação em dois passos, de preferência por aplicativo autenticador ou chave de segurança, e não só por SMS.
- [ ] Confira o endereço de quem enviou, e não só o nome. Golpistas usam nomes de bancos e empresas com endereços parecidos, como letras trocadas ou domínios estranhos.
- [ ] Passe o mouse sobre o link, sem clicar, e veja para onde ele vai de verdade. No celular, segure o dedo sobre o link para ver o endereço. Na dúvida, abra o site digitando o endereço você mesmo.

- [ ] Não abra anexos inesperados, em especial arquivos compactados (zip), documentos que pedem "habilitar edição ou macros" e programas de instalação. Boleto, nota fiscal e currículo de desconhecido merecem checagem antes.
- [ ] Desconfie de mensagens com urgência, ameaça ou promessa: "sua conta será bloqueada", "você tem uma encomenda parada", "pagamento pendente". Bancos e empresas sérias não pedem senha, código ou dados do cartão por e-mail.
- [ ] Use o botão de "Denunciar phishing" ou "Marcar como spam" do seu serviço de e-mail. Isso ensina o filtro e protege outras pessoas. Não responda nem clique em "cancelar inscrição" em spam suspeito.
- [ ] Em pedidos de dinheiro, mudança de conta bancária ou troca de dados de pagamento, confirme por telefone, com um número que você já tinha, e não por um número informado no próprio e-mail.
- [ ] Revise as regras de encaminhamento e os filtros nas configurações do e-mail. Invasores costumam criar uma regra que copia tudo para outro endereço, e isso passa despercebido por meses.
- [ ] Veja os acessos recentes e os aparelhos conectados à conta, desconecte o que não conhece e revise os aplicativos com acesso ao seu e-mail.
- [ ] Tenha um segundo e-mail, só para cadastros e promoções, e mantenha o principal para banco, governo e trabalho. Isso reduz o spam e limita o estrago de vazamentos.
- [ ] Mantenha o e-mail de recuperação e o telefone atualizados e protegidos também, porque são a porta dos fundos da sua conta.

Roteiro de proteção para pendrives e outras conexões (USB, Bluetooth, NFC, cabos e carregadores). Cerca de dez minutos para ajustar, e alguns hábitos para o dia a dia:

- [ ] Nunca ligue ao computador um pendrive achado na rua, recebido de brinde ou deixado por desconhecido. É uma técnica antiga de ataque, porque o aparelho pode se passar por teclado e executar comandos. Se for seu e você não sabe de onde veio, descarte.
- [ ] Use pendrives e discos externos só seus, comprados em lojas confiáveis. Evite emprestar o seu a outras pessoas e não o ligue em computadores de lan house, hotel ou eventos para guardar documentos importantes.
- [ ] No computador, mantenha o antivírus ativo e desligue a execução automática de mídias removíveis. Ao conectar um pendrive de outra pessoa, peça ao antivírus que o analise antes de abrir qualquer arquivo.
- [ ] Desconfie de arquivos com extensão dupla ou que não combinam com o ícone, como uma "foto" que termina em .exe ou um "documento" que é um atalho. Pastas que viram atalhos após ligar o pendrive são sinal de infecção.

- [ ] Criptografe pendrives e discos externos com dados sensíveis (BitLocker no Windows, FileVault no macOS, LUKS no Linux), para que, se o aparelho for perdido, ninguém consiga ler o conteúdo.
- [ ] Em carregadores públicos de aeroporto, hotel ou evento, prefira a tomada da parede com o seu próprio carregador. Se precisar usar a porta USB, use um cabo só de carga, ou um bloqueador de dados, e, se o celular perguntar "Confiar neste computador?" ou sobre transferência de arquivos, responda não.
- [ ] Não aceite cabos ou carregadores desconhecidos de brinde. Compre cabos de marcas conhecidas, porque cabos adulterados existem e podem se passar por teclado ou transmitir dados.
- [ ] No Bluetooth, deixe desligado quando não usar, mantenha o aparelho como "não visível", não aceite pareamento de quem você não conhece e apague da lista os aparelhos antigos. Atualize fones, caixas de som e relógios, que também recebem correções de segurança.
- [ ] Desligue o recebimento por proximidade (AirDrop no iPhone, Compartilhamento por Proximidade no Android) ou deixe só para contatos, e recuse arquivos de desconhecidos. No iPhone, a opção fica em Geral, AirDrop.
- [ ] No NFC, o pagamento por aproximação é seguro quando o celular está bloqueado por senha ou biometria. Não aproxime o celular de adesivos, QR codes ou tags desconhecidos em locais públicos, e ative a confirmação em cada pagamento.
- [ ] Com QR codes, confira o endereço que aparece antes de abrir, desconfie de códigos colados sobre outros em parquímetros e cardápios, e nunca digite senha em página aberta por um QR code que não veio de fonte conhecida.
- [ ] Nas conexões de TV, impressora e outros aparelhos da casa, troque a senha de fábrica, desligue o que não usa (como o compartilhamento sem senha) e mantenha-os atualizados.

Quadro de consulta: o mesmo cuidado, em cada sistema

Cuidado	Windows	macOS	Linux	Android	iPhone
Atualizações	Windows Update	Atualização de Software	Gerenciador de pacotes	Sistema e Google Play	Atualização de Software
Proteção contra malware	Segurança do Windows	Gatekeeper e XProtect	Repositórios oficiais e firewall	Google Play Protect	Isolamento e App Store
Criptografia	BitLocker ou do dispositivo	FileVault	LUKS, escolhido na instalação	Ativa nos modelos recentes	Ativa com código definido
Localizar e apagar	Encontrar meu dispositivo	Buscar	Sem recurso padrão	Encontre Meu Dispositivo	Buscar

Cuidado	Windows	macOS	Linux	Android	iPhone
Backup	Histórico de arquivos, OneDrive	Time Machine, iCloud	Timeshift, Deja Dup, rsync	Conta Google	iCloud ou computador

Na prática: a verificação do seu aparelho

Escolha o aparelho que você mais usa e percorra, na ordem, a coluna correspondente do quadro: confirme que as atualizações estão ligadas, que a proteção está ativa, que o disco está criptografado, que o recurso de localização está ligado e que existe um backup recente. São cinco conferências de poucos minutos, e cobrem a maior parte dos ataques que você viu neste livro.

Capítulo 16: Backups, a defesa que desfaz o estrago

Haverá um dia em que o celular cai na água, o computador não liga, uma conta é invadida ou um ransomware tranca tudo. Contra o roubo, o vírus e o erro, nenhuma defesa é perfeita, mas existe uma que desfaz quase todos os danos: a cópia de segurança. Quem tem backup recente perde algumas horas de trabalho. Quem não tem pode perder fotos de anos, documentos, conversas e o negócio inteiro.

A regra 3-2-1

O jeito mais simples de pensar em backup é a regra 3-2-1: tenha três cópias dos dados importantes (o original e duas cópias), em dois tipos diferentes de mídia, com uma delas fora de casa. Na prática, para uma família, isso quer dizer o original no aparelho, uma cópia em disco externo guardado em outro cômodo, e outra na nuvem.



Figura 16.1 · a regra 3-2-1 de backup

A ordem das cópias importa. Uma cópia que fica sempre ligada ao computador, na mesma rede, pode ser criptografada junto pelo ransomware. Por isso, pelo menos uma delas precisa ficar desconectada depois do backup, ou numa nuvem que guarde versões antigas dos arquivos.

O que guardar

Antes de configurar qualquer coisa, faça uma lista curta do que não pode ser perdido: fotos e vídeos, documentos pessoais e profissionais, o gerenciador de senhas e suas chaves de recuperação, as conversas do WhatsApp, os contatos, os e-mails importantes, as planilhas e os arquivos do trabalho. O sistema operacional e os programas se reinstalam, e os seus dados não. Para cada item da lista, pergunte onde ele está hoje e quantas cópias existem.

Os roteiros de backup

Cada roteiro leva de dez a vinte minutos para configurar, e depois quase tudo roda sozinho. Os menus mudam entre versões e marcas, então use a busca das configurações se não encontrar a opção com o mesmo nome.

Roteiro de backup no Windows. Cobre arquivos e o sistema:

- [ ] Escolha onde guardar: um disco externo (HD ou SSD) e, se quiser, a nuvem da sua conta Microsoft (OneDrive).
- [ ] Nas Configurações, procure "Backup do Windows" (ou "Histórico de Arquivos"). Ligue o backup das pastas Documentos, Imagens e Área de Trabalho, e conecte o disco externo para o Histórico de Arquivos.
- [ ] Confirme que o backup roda: abra a tela e veja a data da última cópia.
- [ ] Ative a proteção do sistema e crie um ponto de restauração antes de grandes atualizações, para poder voltar atrás se algo der errado.
- [ ] Crie uma imagem do sistema ou um pendrive de recuperação do Windows, e guarde-o. Servem para reinstalar o computador do zero se ele não ligar.
- [ ] Desconecte o disco externo depois da cópia e guarde-o em outro lugar.

Roteiro de backup no macOS.

- [ ] Conecte um disco externo e abra Ajustes do Sistema, procurando por "Time Machine". Selecione o disco como destino do backup. Para ter uma cópia fora de casa, você pode instalar o Google Drive para computador e guardar lá as pastas de documentos.
- [ ] Ligue o backup automático e deixe a primeira cópia terminar, o que pode demorar horas.
- [ ] Confirme em Time Machine a data da última cópia, e faça o teste de abrir uma versão antiga de um arquivo.

- [ ] Se usar o iCloud Drive, saiba que ele sincroniza, mas não substitui o backup: apagar um arquivo num aparelho apaga nos outros.
- [ ] Desconecte o disco quando não estiver copiando e guarde-o fora do computador.

Roteiro de backup no Linux.

- [ ] Instale o Timeshift (que guarda pontos de restauração do sistema) e um programa de cópia dos seus arquivos, como o Deja Dup, ou use o rsync para quem tem mais experiência.
- [ ] Escolha como destino um disco externo ou outro computador, e defina uma cópia diária ou semanal.
- [ ] Inclua a pasta pessoal ("home"), que contém seus documentos, fotos e configurações, e guarde uma lista dos programas instalados.
- [ ] Se o disco estiver criptografado, guarde a senha de recuperação em local seguro, porque sem ela o backup não ajuda.
- [ ] Teste restaurar um arquivo, e depois desconecte o disco.

Roteiro de backup no Android.

- [ ] Em Configurações, procure "Backup" ou "Google One" e ligue o backup para a sua conta Google, que guarda aplicativos, contatos, configurações e mensagens SMS.
- [ ] Ligue o backup de fotos e vídeos no Google Fotos, ou em outro serviço de sua confiança, e confirme que a cópia está em dia.
- [ ] Sincronize os contatos e o calendário com a conta Google.
- [ ] Uma vez por mês, copie as fotos e os arquivos importantes para o computador e para o disco externo.
- [ ] Anote a senha e a verificação em dois passos da conta Google em um lugar seguro, porque ela é a porta de volta aos seus dados.

Roteiro de backup no iPhone e iPad.

- [ ] Em Ajustes, toque no seu nome, vá em iCloud e ligue o "Backup do iCloud". Escolha o que entra no backup e use "Fazer backup agora" para a primeira cópia.
- [ ] Confira o espaço disponível no iCloud. Se não couber, aumente o plano ou use um computador.
- [ ] Ligue o iCloud Fotos, mas lembre que ele sincroniza as fotos entre aparelhos, e não é uma cópia independente: apagar uma foto no iPhone a remove em todos.
- [ ] De tempos em tempos, conecte o aparelho a um computador e faça um backup local, de preferência criptografado, que inclui senhas salvas e dados de saúde.
- [ ] Guarde a senha do ID Apple e a chave de recuperação em local seguro.

Roteiro de backup do WhatsApp. As conversas ficam no celular, e o backup é o que permite recuperá-las num aparelho novo:

- [ ] Abra o WhatsApp, vá em Configurações, Conversas, "Backup de conversas" (ou "Backup das conversas").
- [ ] No Android, escolha a conta Google e a frequência (diária, semanal ou mensal). No iPhone, o backup vai para o iCloud, e o iCloud precisa estar ligado.
- [ ] Toque em "Fazer backup" para a primeira cópia e confira a data e o tamanho do backup na mesma tela.
- [ ] Ligue o "Backup criptografado de ponta a ponta" e crie uma senha ou chave de 64 dígitos, que são necessárias para restaurar. Guarde-as no gerenciador de senhas, porque sem elas o backup não abre.
- [ ] Decida se quer incluir vídeos, que aumentam muito o tamanho do backup.
- [ ] Antes de trocar de celular, faça um backup novo. No aparelho novo, instale o WhatsApp, confirme o mesmo número e escolha "Restaurar" quando o aplicativo oferecer.
- [ ] Use a opção "Exportar conversa" para guardar fora do aplicativo as conversas realmente importantes, como combinados e comprovantes.

Roteiro de backup do e-mail e dos contatos. O e-mail fica no servidor do provedor, mas ele não é um backup: se a conta for invadida, apagada ou bloqueada, tudo some:

- [ ] No Gmail, use o Google Takeout (takeout.google.com) para baixar uma cópia dos e-mails, contatos, calendário e fotos da conta Google. Escolha o que incluir e programe a exportação a cada alguns meses.
- [ ] No Outlook e no Microsoft 365, exporte o arquivo de dados (.pst) ou use a opção de exportar da sua conta, e guarde a cópia no disco externo.
- [ ] Em outros provedores, use um programa de e-mail (como o Thunderbird) que baixe as mensagens para o computador, e inclua essa pasta no backup do computador.
- [ ] Exporte os contatos para um arquivo (.vcf ou .csv) e guarde junto com os outros.
- [ ] Guarde fora da caixa de e-mail os documentos importantes que chegam por anexo, como contratos, notas fiscais e comprovantes.

Roteiro de backup das redes sociais. Em geral, a rede guarda seus dados, mas você pode perder a conta e tudo o que ela contém. Todas oferecem uma ferramenta para baixar uma cópia:

- [ ] No Facebook e no Instagram, procure em Configurações a Central de Contas, e ali "Suas informações e permissões" e "Baixar suas informações". Escolha as fotos, vídeos, publicações e mensagens, e o formato do arquivo.
- [ ] No TikTok, procure em Configurações e privacidade, Conta, "Baixar seus dados", e peça o arquivo. Ele fica disponível por alguns dias.

- [ ] No X (antigo Twitter), no YouTube, no LinkedIn e em outras redes, procure "Baixar arquivo dos seus dados" ou "Exportar" nas configurações da conta.
- [ ] Salve os arquivos baixados no disco externo, e não só no mesmo celular, e repita a cada seis meses ou antes de grandes mudanças.
- [ ] Guarde, para quem trabalha com as redes, as fotos e os vídeos originais fora do aplicativo, porque a rede reduz a qualidade e pode remover conteúdo.
- [ ] Anote os e-mails e telefones de recuperação de cada conta, para o caso de precisar recuperar o acesso.

O backup que nunca foi testado não conta

Muita gente descobre que o backup não funcionava no dia em que precisa dele. Marque no calendário, a cada três meses, um teste curto: escolha um arquivo, restaure-o em outra pasta e abra-o, e confira a data da última cópia de cada roteiro. Se o disco externo não foi conectado há meses, conecte-o e atualize a cópia. Crie, também, o hábito de revisar o que mudou: novas fotos, novos documentos, novas contas.

Quadro de consulta: onde guardar cada coisa

O que	Onde está o original	Primeira cópia	Segunda cópia
Fotos e vídeos	Celular	Nuvem (Google Fotos ou iCloud)	Disco externo
Documentos	Computador	Disco externo	Nuvem com versões (OneDrive ou Google Drive)
Conversas do WhatsApp	Celular	Google Drive ou iCloud	Backup criptografado e exportação das importantes
E-mails e contatos	Servidor do provedor	Arquivo exportado	Disco externo
Redes sociais	Servidor da rede	Arquivo baixado	Disco externo
Sistema operacional	Computador	Imagem ou ponto de restauração	Pendrive de recuperação
Senhas	Gerenciador de senhas	Exportação criptografada	Cópia em papel das chaves de recuperação, em lugar seguro

Capítulo 17: Segurança no dia a dia, seu roteiro, o glossário e as fontes

No capítulo 1, você fez uma lista de cinco coisas digitais que seriam um problema se saíssem do seu controle. Agora que conhece os ataques e as defesas, volte a ela. Para cada item, pergunte: que ataque poderia atingi-lo, e qual defesa ainda falta? A resposta, quase sempre, está numa dessas poucas ações. A segurança pessoal não exige ser um especialista, e sim repetir dez ou doze hábitos até que eles virem rotina.

O roteiro dos doze hábitos

A lista abaixo reúne o que o livro ensinou, em ordem de impacto. Faça um item por semana e, em três meses, você terá uma defesa melhor do que a da maioria das pessoas e empresas.

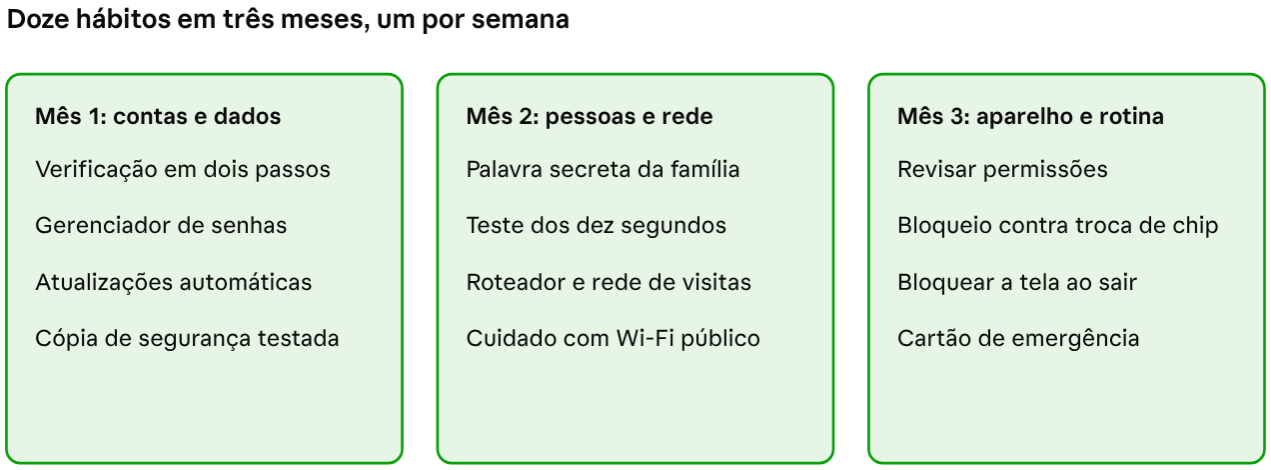


Figura 17.1 · os doze hábitos em três meses

A lista a seguir detalha cada hábito, com o capítulo onde ele foi explicado.

- [ ] Ativar a verificação em dois passos no e-mail, no banco e nas redes sociais (capítulo 3)
- [ ] Instalar um gerenciador de senhas e trocar as senhas das contas mais importantes por frases longas e únicas (capítulo 3)
- [ ] Ligar as atualizações automáticas do celular, do computador e dos aplicativos (capítulo 8)
- [ ] Fazer uma cópia de segurança das fotos e documentos importantes, uma delas desconectada, e testar a restauração (capítulos 5 e 16)
- [ ] Combinar com a família uma palavra secreta para pedidos urgentes de dinheiro (capítulo 14)
- [ ] Adotar o teste dos dez segundos antes de clicar, pagar ou responder a algo com pressa (capítulo 2)

- [ ] Trocar as senhas de fábrica do roteador e dos aparelhos conectados, e criar uma rede separada para visitas e coisas da casa (capítulos 6 e 10)
- [ ] Evitar Wi-Fi público para banco e compras, e usar o plano de dados ou uma VPN confiável (capítulo 6)
- [ ] Revisar as permissões e apagar os aplicativos que não usa mais (capítulo 7)
- [ ] Pedir à operadora o bloqueio contra troca de chip e ativar a localização e o apagamento remoto do celular (capítulo 10)
- [ ] Bloquear a tela sempre que sair de perto do aparelho (capítulo 9)
- [ ] Escrever o cartão de emergência, com os telefones oficiais do banco e da operadora (capítulo 13)

Para empresas pequenas

Quem tem um negócio, mesmo pequeno, soma a esses hábitos quatro medidas. Dar a cada pessoa só os acessos de que precisa, e cortar os acessos de quem sai no mesmo dia. Exigir verificação em dois passos em tudo o que for acesso remoto, e-mail e sistemas financeiros. Manter backups testados, com uma cópia fora da rede. E definir, antes do problema, quem decide o quê se algo der errado, e quem avisa os clientes. As regras de duas pessoas para pagamentos novos protegem contra a fraude do falso chefe, e a LGPD exige cuidado com os dados de quem confia em você.

Glossário

Termo	Em palavras simples
Backdoor	Entrada escondida que o atacante deixa para voltar depois
Backup	Cópia de segurança dos dados
Botnet	Rede de aparelhos infectados controlados à distância
Criptografia	Técnica que embaralha dados para que só quem tem a chave os leia
DDoS	Ataque que derruba um serviço com uma enxurrada de pedidos
Deepfake	Vídeo, foto ou áudio falso criado por IA que imita uma pessoa
EDR	Programa que observa o comportamento do aparelho e reage a ameaças

Termo	Em palavras simples
Firewall	Porteiro que filtra o que entra e sai de uma rede
Hash	Impressão digital de um dado, usada para guardar senhas
Malware	Programa feito para causar dano, roubar ou espionar
MFA	Verificação em dois passos ou mais
Patch	Correção de uma falha num programa
Phishing	Mensagem falsa que tenta roubar dados ou dinheiro
Ransomware	Malware que tranca arquivos e pede resgate
Engenharia social	Ataque que engana pessoas, e não máquinas
VPN	Túnel criptografado entre seu aparelho e um ponto seguro
Vulnerabilidade	Falha que pode ser usada para um ataque
Zero-day	Falha que o atacante conhece e o fabricante ainda não

Para saber mais

- **Cartilha de Segurança para Internet**, do CERT.br (NIC.br), gratuita e em português.
- **ANPD**, Autoridade Nacional de Proteção de Dados, para direitos e orientações sobre a LGPD.
- **OWASP**, organização que mantém a lista das falhas mais comuns em aplicativos.
- **NIST**, instituto americano de padrões, com guias de gestão de segurança.
- **Have I Been Pwned**, serviço gratuito que informa se um e-mail apareceu em vazamentos conhecidos.

A segurança digital nunca fica pronta. Ela é um hábito, como escovar os dentes, e quem entende como os ataques funcionam passa a enxergar os golpes antes de cair neles.nuar