// STORM NEXUS · SAVIX SHIELD · 2026

Segurança Digital para Toda a Família

O guia completo de proteção digital para você, seus filhos e seus pais — sem jargão técnico.

35
páginas

12
capítulos

100%
gratuito

Wanderley Abreu Jr. — "Storm"
FUNDADOR · GRUPO STORM · STORM NEXUS CIBERSEGURANÇA

Com agradecimento especial a Felipe Neto — co-fundador do SAVIX Shield

BIS-2026-FAM-001 · Edição 2026

// SUMÁRIO

Conteúdo

// ABERTURA

Por que escrevi este livro

Tinha 17 anos quando invadi a NASA.

Não por mal — por curiosidade, pelo desafio, pela adrenalina de entender sistemas que ninguém deveria conseguir entrar. O que veio depois mudou minha vida: em vez de processo, recebi um convite para mostrar o que tinha feito no Goddard Space Flight Center.

Trinta anos depois, já trabalhei para a ESA no projeto Galileo, desenvolvi criptografia para tropas da OTAN no Afeganistão, participei do time de comunicação que pousou o Rover Perseverance em Marte — e identifiquei mais de 200 predadores sexuais online na primeira operação contra pedofilia da internet no Brasil.

Vi a tecnologia do melhor e do pior ângulo possível.

Hoje, o que me tira o sono não são mais as ameaças sofisticadas contra infraestrutura crítica. É a minha vizinha de 68 anos que perdeu R$ 47.000 para um golpista que se passou pelo filho dela em uma ligação de WhatsApp. É o adolescente de 14 anos que entregou dados pessoais para um estranho em troca de uma skin de videogame. É o pai que não sabia que o chip do celular tinha sido clonado até ver a conta bancária zerada.

Essas são as batalhas que mais importam agora. E elas não se vencem com tecnologia — vencem-se com conhecimento.

Este livro não é para hackers. É para famílias.

Não tem jargão, não exige formação técnica e não vai te pedir para instalar nada complicado. O que vai pedir é atenção — porque a maioria dos ataques digitais que chegam à sua família são psicológicos, não tecnológicos. Eles exploram pressa, medo, afeto e confiança.

Cada capítulo foi escrito pensando em alguém real: a avó que precisa saber diferenciar uma ligação legítima do banco de uma falsa central. O adolescente que não percebe que está sendo manipulado numa rede social. O empresário que usa a mesma senha em 15 lugares diferentes.

> *"A segurança mais forte que existe não está em nenhum sistema. Está no conhecimento de quem usa a tecnologia."*

Leia. Compartilhe. E comece pelo capítulo que mais parece com alguém que você ama.

Wanderley Abreu Jr. — Storm
Rio de Janeiro, 2026

CAPÍTULO 01

Panorama: o Brasil no centro da mira digital

Por que somos um dos países mais atacados do mundo — e o que isso significa para a sua família.

R$ 10,1 bi	+220%	40,8 mi
perdidos em fraudes/ano	crescimento de malware	vítimas anuais

O país mais atacado da América Latina

O Brasil ocupa consistentemente o topo dos rankings de crimes digitais na América Latina. Segundo a Febraban, as fraudes financeiras digitais custaram R$ 10,1 bilhões ao país em 2025 — um valor que supera o PIB de muitos municípios brasileiros.

Mas o que esses números significam na prática? Significa que, estatisticamente, você ou alguém da sua família já foi alvo de uma tentativa de golpe digital. A questão não é se o ataque vai acontecer — é se você vai reconhecê-lo antes de ser tarde demais.

Por que o Brasil é tão visado?

Três fatores combinados tornam o Brasil um alvo preferencial para criminosos digitais:

- **Adoção massiva do PIX:** mais de 150 milhões de usuários e R$ 17 trilhões em transações anuais. Nenhum outro sistema de pagamento instantâneo do mundo tem esse volume — e isso atrai criminosos de todo o planeta.
- **Alta penetração de smartphones:** mais de 240 milhões de celulares ativos para 215 milhões de habitantes. A maioria das pessoas faz tudo pelo celular, incluindo operações bancárias de alto valor.
- **Baixa educação digital:** ainda há uma disparidade enorme entre o quanto usamos tecnologia e o quanto entendemos sobre segurança digital. Essa lacuna é exatamente o que os golpistas exploram.

Os 5 tipos de ataque mais comuns no Brasil

Entender as categorias principais ajuda a criar um mapa mental de defesa:

- **Engenharia social:** manipulação psicológica para fazer você agir sem pensar. Inclui falsa central bancária, golpe do WhatsApp, falso suporte técnico.
- **SIM Swap:** clonagem do seu chip de celular para desviar SMS de verificação e assumir suas contas.
- **Phishing:** links falsos que imitam sites legítimos para roubar senhas e dados.
- **Ransomware:** sequestro de arquivos com pedido de resgate. Atinge empresas, mas também pessoas físicas.
- **Fraude financeira via PIX:** combinação de engenharia social e tecnologia para desviar pagamentos.

O golpe mais eficaz não é tecnológico.

92% dos ataques bem-sucedidos contra pessoas físicas envolvem engenharia social — não vulnerabilidades técnicas. O criminoso não invade seu celular; ele convence você a abrir a porta.

O que mudou em 2025-2026

A inteligência artificial transformou o cenário de ameaças de forma dramática. Golpistas agora têm acesso a:

- Clonagem de voz com 30 segundos de áudio (disponível em apps gratuitos)
- Deepfakes de vídeo em tempo real para videochamadas falsas
- Mensagens personalizadas geradas por IA que conhecem seu nome, cidade e contexto
- Tradução automática que elimina os erros de português que antes denunciavam golpes internacionais

A boa notícia: as defesas também são simples. Os próximos capítulos mostram exatamente como ativá-las.

CAPÍTULO 02

Golpes no celular: WhatsApp, PIX e falsa central

Os 8 golpes mais comuns no smartphone brasileiro — e como reconhecer cada um deles.

O celular como porta de entrada

O smartphone brasileiro médio tem apps de 3 bancos, 2 carteiras digitais, WhatsApp com acesso a toda a família, e autenticação por SMS para tudo. Para um criminoso, comprometer um celular equivale a comprometer a vida financeira e social de uma pessoa.

Golpe 1: Sequestro do WhatsApp

É o golpe mais reportado no Brasil. O criminoso liga ou manda mensagem se passando por uma empresa, banco ou até amigo, e pede o código de verificação de 6 dígitos que o WhatsApp acabou de enviar por SMS.

Como funciona: O WhatsApp manda um código quando detecta uma tentativa de login novo. Se você passar esse código para o criminoso, ele assume sua conta — e imediatamente começa a pedir dinheiro para todos os seus contatos.

- Nunca compartilhe o código de verificação do WhatsApp com NINGUÉM
- Ative a confirmação em dois passos: Configurações > Conta > Confirmação em duas etapas
- Se perder acesso, use o próprio número para recuperar — não aceite ajuda de terceiros

Golpe 2: Falsa central bancária

O golpista liga se passando pelo banco, afirma que detectou uma transação suspeita, e pede que você confirme dados ou transfira dinheiro para uma 'conta segura'. O número pode aparecer como legítimo (spoofing).

Bancos reais NUNCA ligam pedindo senha, código, ou para você transferir dinheiro. Se receber essa ligação: desligue, aguarde 10 minutos, e ligue você mesmo para o número do cartão.

Golpe 3: SIM Swap (clonagem de chip)

O criminoso vai a uma loja de operadora com documentos falsos ou dados comprados e pede uma segunda via do seu chip. A partir daí, recebe todos os seus SMS — incluindo códigos de verificação bancária.

Sintoma: seu celular perde sinal de repente sem motivo aparente. Ligue imediatamente para a operadora se isso acontecer.

- Ative verificação por app autenticador, não por SMS, em todos os bancos
- Configure uma senha adicional na operadora para portabilidade
- Se o celular perder sinal inexplicavelmente, ligue da linha fixa ou de outro celular para a operadora

Golpe 4: Falso parente no WhatsApp

'Oi mãe, troquei de número.' Essa mensagem simples já causou prejuízos de bilhões no Brasil. O golpista usa uma foto de perfil igual à do seu filho/filha e pede uma transferência urgente.

Defesa: ligue para o número antigo ou para outro familiar antes de qualquer transferência. Sempre.

Golpe 5: Maquininha falsa / PIX laranja

Em compras presenciais, a maquininha é adulterada para cobrar valor diferente. No PIX, o criminoso manda um comprovante falso ou substitui a chave no último segundo.

- Confira sempre o valor na tela da maquininha antes de digitar a senha
- No PIX: confirme o nome do destinatário antes de confirmar — não apenas a chave
- Desconfie de comprovantes enviados por WhatsApp — consulte seu extrato

O padrão de todos os golpes

Todo golpe eficaz usa a mesma fórmula: **urgência + autoridade + medo**. O golpista cria uma situação em que você precisa agir AGORA, sem pensar. Reconhecer esse padrão

é sua principal defesa.

> Toda vez que sentir pressão para agir rápido com dinheiro: PAUSE. Respire. Desligue. Ligue de volta você mesmo para um número que você conhece. 10 minutos de pausa já eliminam 90% dos golpes.

CAPÍTULO 03

Phishing, ransomware e golpes por e-mail

Como reconhecer links falsos, e-mails fraudulentos e o que fazer se clicar em um.

Phishing: a isca digital

Phishing é o ato de enganar alguém para que entregue informações ou clique em links maliciosos, geralmente através de e-mails, mensagens ou sites falsos que imitam fontes confiáveis.

1 em 3	R$ 2,1 bi	3 seg
e-mails no Brasil é phishing	prejuízo em 2025	tempo médio para clicar

Como reconhecer um e-mail de phishing

- **Remetente suspeito:** o nome exibido pode ser 'Banco Bradesco', mas o endereço real é bradesco-seguranca@gmail.com
- **Urgência artificial:** 'Sua conta será bloqueada em 24h', 'Ação necessária imediata'
- **Links diferentes:** passe o mouse sobre o link sem clicar — o endereço real aparece na barra inferior
- **Erros de português:** ainda comum em golpes internacionais mal traduzidos
- **Pedido de dados:** nenhum banco pede senha por e-mail

Ransomware: quando seus arquivos são sequestrados

Ransomware é um tipo de vírus que criptografa todos os seus arquivos e pede pagamento (geralmente em Bitcoin) para devolver o acesso. Empresas pagaram resgates de milhões — mas pessoas físicas também são alvos.

- Mantenha backup em local separado: regra 3-2-1 (3 cópias, 2 mídias diferentes, 1 offsite)

- Nunca abra anexos .exe, .vbs, .bat de remetentes desconhecidos
- Mantenha Windows/macOS sempre atualizado — patches corrigem vulnerabilidades exploradas
- Se infectado: desconecte da internet imediatamente, não pague o resgate, contate a Polícia Federal

Checklist: e-mail seguro ou golpe?

- O remetente é exatamente o domínio oficial? (banco.com.br, não banco-seguro.com)
- O link leva para o domínio correto? (verifique antes de clicar)
- Está pedindo para confirmar dados que a empresa já tem?
- Criou urgência com prazo curto?
- Chegou sem você ter solicitado algo?

Se respondeu 'sim' para qualquer uma dessas perguntas: **não clique**. Delete o e-mail.

CAPÍTULO 04

Redes sociais: armadilhas e configurações essenciais

Instagram, TikTok, Facebook e LinkedIn — o que você compartilha e o que isso revela.

O problema da superexposição

A maioria dos golpes começa com pesquisa. Antes de ligar para uma vítima, golpistas profissionais passam horas nas redes sociais coletando informações: nome dos filhos, cidade, banco que usa (pela foto do cartão), aniversários, viagens.

Um perfil público no Instagram com fotos do dia a dia pode revelar mais sobre você do que imagina.

Configurações essenciais por rede

Instagram e TikTok

- Perfil: configurar como Privado (Configurações > Privacidade > Conta privada)
- Histórias: limitar quem pode responder às suas histórias
- Tags: aprovar manualmente fotos em que você é marcado
- Localização: nunca postar em tempo real — apenas depois que sair do lugar

Facebook

- Revisar quem pode ver suas publicações passadas (Configurações > Privacidade > Limitar público)
- Desativar a indexação por motores de busca
- Revisar apps conectados — muitos têm acesso a dados que você esqueceu de revogar
- Nunca fazer login em outros sites via 'Entrar com Facebook'

LinkedIn

- Desativar a exibição do seu perfil para não-conexões se atuar em área sensível
- Cuidado com convites de recrutadores falsos — phishing profissional é comum

- Não sincronizar contatos do celular com o LinkedIn

Romance scam: o golpe do amor

Criminosos criam perfis atraentes, iniciam conversas longas, constroem relacionamento emocional por semanas — e depois pedem dinheiro para uma 'emergência'. No Brasil, o prejuízo médio por vítima é de R$ 23.000.

> A pessoa é perfeita demais para alguém desconhecido. Nunca aceita videochamada. Sempre tem uma emergência que precisa de dinheiro. Pede transferência por PIX ou criptomoeda. Se identificar esses sinais: bloqueie e reporte.

CAPÍTULO 05

Crianças e adolescentes online — ECA Digital

Como proteger seus filhos sem criar um clima de vigilância — e o que a nova lei exige.

87%	Lei 15.211	19s
crianças online antes dos 10 anos	ECA Digital em vigor	tempo médio de abordagem

O que é o ECA Digital (Lei 15.211/2025)

Em vigor desde 2025, a Lei 15.211 estabelece deveres concretos para plataformas digitais que atendem crianças e adolescentes. Ela exige verificação de idade, controles parentais efetivos, e proíbe o uso de dados de menores para publicidade comportamental.

Para os pais, a lei é uma ferramenta: plataformas que descumprirem podem ser multadas em até R$ 50 milhões pela ANPD.

Os 5 riscos principais para menores

- **Grooming:** adultos que constroem relacionamento online com crianças para fins de abuso. Ocorre em jogos, Discord, Instagram e plataformas de chat.
- **Cyberbullying:** assédio, humilhação e exclusão social através de plataformas digitais.
- **Sexting involuntário:** envio de imagens íntimas sob pressão — que frequentemente se espalham sem controle.
- **Dependência digital:** algoritmos projetados para maximizar engajamento podem criar padrões compulsivos em cérebros em desenvolvimento.
- **Desinformação:** jovens são alvos de conteúdo de ódio, teorias conspiratórias e notícias falsas.

A conversa mais importante

Tecnologia de controle parental é útil, mas não substitui a conversa. Crianças que têm um adulto confiável para reportar situações desconfortáveis têm muito mais proteção do que aquelas monitoradas em silêncio.

- Estabeleça que não há punição por reportar algo assustador online
- Pergunte regularmente sobre as amizades online — com curiosidade, não interrogatório
- Ensine a Regra do Não Brigo: se algo online fizer você se sentir mal, você não precisa responder
- Combine 'palavras de segurança' para situações de pressão online

Controles parentais por plataforma

Google Family Link

Gerencia dispositivos Android para menores, controla tempo de tela, aprova apps, monitora localização. Gratuito e integrado ao Google.

Apple Screen Time

Para iPhones e iPads, permite definir limites de tempo, filtrar conteúdo e aprovar compras. Configurável em Ajustes > Tempo de Uso.

Controles no roteador

Roteadores modernos (e apps como Google Home) permitem pausar a internet para dispositivos específicos em horários definidos — muito mais eficaz do que tentar controlar app por app.

> Monitorar os filhos em segredo sem contar para eles. Além de quebrar a confiança quando descoberto (e sempre descobrem), transmite a mensagem de que privacidade não é um direito. Seja transparente sobre o monitoramento.

CAPÍTULO 06

Guia para idosos: os 7 golpes mais comuns

57% das vítimas de fraude financeira digital têm mais de 60 anos. Por que — e como mudar isso.

Por que idosos são alvos prioritários

Não é por serem menos inteligentes. É porque cresceram em uma época onde o contato humano era a base da confiança — e os golpistas exploram exatamente isso. Alguém que liga com autoridade, urgência e conhece seu nome têm enorme poder sobre quem foi criado a confiar em instituições.

Os 7 golpes mais comuns

1. Golpe da central bancária

Liga alguém do 'banco' dizendo que seu cartão foi clonado. Pede para você digitar a senha e enviar o cartão com um motoboy. Bancos nunca enviam motoboys para buscar cartões.

2. Golpe do neto / parente em apuros

'Vovó, sou eu, tô em apuros, não conta para ninguém.' Depois pede transferência urgente. A arma: a vergonha de contar para outros familiares antes de agir.

3. Falso desconto de INSS / benefício

Ligam oferecendo revisão de aposentadoria ou desconto suspeito. Pedem dados bancários para 'cancelar o desconto'. Resultado: acesso à conta.

4. Prêmio / sorteio falso

'Você ganhou um prêmio, mas precisa pagar uma taxa para liberar.' Não existe prêmio legítimo que exija pagamento prévio.

5. Suporte técnico falso

Liga alguém da 'Microsoft' ou 'Claro' dizendo que o computador está com vírus. Pede para instalar um app de acesso remoto. Resultado: acesso completo ao dispositivo e

contas bancárias.

6. Golpe do PIX errado

'Caiu dinheiro na sua conta por engano, pode devolver?' O pagamento nunca foi real ou foi feito com conta laranja. Você devolve dinheiro do seu próprio bolso.

7. Falso médico / plano de saúde

Ligam sobre exame alterado ou cobertura negada, criam urgência médica e pedem dados pessoais ou pagamento imediato.

O método dos 5 passos para famílias

Ensine este protocolo simples para seus pais ou avós:

- **PARA** — não tome nenhuma ação imediata por telefone
- **DESLIGA** — encerre a ligação sem explicações
- **ESPERA** — aguarde 10 minutos
- **LIGA** — para um familiar ou para o número oficial do banco no verso do cartão
- **CONTA** — nunca guarde segredo de solicitações financeiras por telefone

> Não explique apenas uma vez. Repita o protocolo com carinho periodicamente. Pratique com perguntas: 'Se o banco ligar pedindo sua senha, o que você faz?' A repetição cria memória muscular para momentos de pressão.

CAPÍTULO 07

Deepfakes, IA e clonagem de voz

A nova fronteira das fraudes: quando não dá mais para confiar no que você vê e ouve.

O que é um deepfake

Deepfake é conteúdo audiovisual (imagem, vídeo ou áudio) gerado ou manipulado por inteligência artificial para fazer parecer que uma pessoa disse ou fez algo que nunca aconteceu.

30 seg	US$ 25 mi	100%
de áudio para clonar voz	maior fraude por deepfake	gratuito o acesso à tecnologia

Clonagem de voz: o caso real

Em 2024, uma empresa de Hong Kong transferiu US$ 25 milhões depois que um gerente financeiro participou de uma 'videochamada com o CEO'. Todos eram deepfakes em tempo real.

No Brasil, o golpe mais comum usa 30 segundos de áudio do Instagram ou TikTok do seu filho para criar mensagens de voz pedindo dinheiro urgente.

Como reconhecer um deepfake

- Movimentos labiais que não sincronizam perfeitamente com o áudio
- Bordas do rosto levemente borradas ou piscando em videochamadas
- Ausência de movimentos naturais (piscar irregular, falta de micromovimentos)
- Audio com qualidade uniforme demais, sem ruídos de ambiente
- Em vídeo: pedir para a pessoa virar de perfil ou fazer um gesto específico — modelos têm dificuldade com perspectivas incomuns

Protocolo de verificação

Se receber uma mensagem de voz ou vídeo pedindo dinheiro ou ação urgente de alguém que você conhece:

- Ligue de volta para o número que você conhece de memória ou agenda
- Faça uma pergunta que só a pessoa real saberia responder
- Para transferências acima de R$ 1.000: exija videochamada ao vivo com uma ação específica ('coloca a mão na cabeça')
- Nunca transfira dinheiro baseado apenas em áudio ou vídeo recebido via mensagem

Desinformação e fake news

A IA também acelera a criação de notícias falsas. Antes de compartilhar qualquer notícia alarmante:

- Verifique em pelo menos dois portais de notícia conhecidos
- Use o Google Fact Check ou Agência Lupa para checar fatos
- Notícias que causam raiva intensa ou medo extremo devem acionar suspeita automática
- Data da notícia: conteúdo antigo é frequentemente reaproveitado fora de contexto

CAPÍTULO 08

Segurança em casa: roteador, senhas e 2FA

O checklist que leva uma tarde para implementar e protege a família por anos.

O roteador: a porta de entrada ignorada

A maioria das casas brasileiras tem o roteador com a senha padrão de fábrica e o firmware desatualizado. Para um atacante na vizinhança, isso é uma porta aberta.

- Trocar a senha padrão do roteador (acesse pelo navegador: 192.168.0.1 ou 192.168.1.1)
- Atualizar o firmware: no painel do roteador, procurar 'Atualização' ou 'Update'
- Criar uma rede Wi-Fi separada para visitantes e dispositivos IoT (câmeras, smart TV)
- Desativar WPS (Wi-Fi Protected Setup) — tem vulnerabilidades conhecidas
- Trocar o nome do Wi-Fi (SSID) para algo que não revele o modelo do roteador

Senhas: o guia definitivo

As regras que realmente importam

- Senha diferente para cada serviço — especialmente e-mail e bancos
- Mínimo de 12 caracteres combinando letras, números e símbolos
- Nunca use dados pessoais: nome, CPF, data de nascimento, nome de pet
- Use um gerenciador de senhas: Bitwarden (gratuito), 1Password ou Apple Keychain

> Uma frase fácil de lembrar vira uma senha forte: 'Meu primeiro carro era um Gol em 2003!' vira MpceuGem2003! — 13 caracteres, maiúsculas, números e símbolo. Memorável para você, impossível para um robô.

Autenticação em dois fatores (2FA)

O 2FA exige um segundo elemento além da senha: um código temporário gerado por app ou enviado por SMS. Ative em TODOS os serviços financeiros e no e-mail principal.

Hierarquia de segurança do 2FA (do mais ao menos seguro)

- **Chave física (YubiKey):** mais seguro, imune a phishing
- **App autenticador (Google Authenticator, Authy):** muito seguro, imune a SIM Swap
- **SMS:** aceitável, mas vulnerável a SIM Swap
- **E-mail de recuperação:** mínimo aceitável — proteja bem o e-mail principal

Nunca use SMS como 2FA para serviços bancários se houver opção de app autenticador.

Checklist de segurança doméstica

- [ ] Senha do roteador trocada da padrão de fábrica
- [ ] Firmware do roteador atualizado
- [ ] Rede de visitantes criada e separada
- [ ] Gerenciador de senhas instalado e em uso
- [ ] 2FA ativado no e-mail principal
- [ ] 2FA ativado nos apps bancários
- [ ] Backup automático de fotos e documentos configurado
- [ ] Atualização automática do sistema operacional habilitada

CAPÍTULO 09

Proteção financeira: PIX, MED 2.0 e emergências

O que fazer nas primeiras 24 horas após descobrir uma fraude.

O PIX e a janela de 30 minutos

O Banco Central criou o MED 2.0 (Mecanismo Especial de Devolução) exatamente para os casos de fraude por PIX. Se você reportar a fraude em até 80 horas, o banco tem obrigação de iniciar o processo de devolução em até 7 dias.

Protocolo para as primeiras 24 horas

- **Imediato:** ligue para o banco e informe a fraude — peça bloqueio do acesso digital
- **Primeiras 2h:** registre Boletim de Ocorrência (online: delegaciaonline.mj.gov.br)
- **Nas 24h:** formalize a solicitação de devolução via MED 2.0 com o banco
- **Em 48h:** notifique o Banco Central via fale.bcb.gov.br se o banco não responder
- **Em 7 dias:** se a resposta for negativa, acione o Procon e registre queixa no SENACON

Limites de PIX e configurações de segurança

- Reduzir o limite noturno do PIX (normalmente R$ 1.000 a R$ 2.000 — o suficiente para emergências)
- Ativar o 'Modo Férias' quando viajar — bloqueia temporariamente transações de alto valor
- Configurar o Pix Agendado para novas chaves: banco exige 24h de espera para chaves novas
- Desativar a câmera para pagamentos por QR Code quando não usar

Seguro contra fraudes digitais

Alguns bancos oferecem seguro de até R$ 50.000 contra fraudes digitais por menos de R$ 15/mês. Vale verificar com seu banco — especialmente se você faz transações frequentes de alto valor.

Banco Central: 145

Procon: 151

Delegacia Online: delegaciaonline.mj.gov.br

SaferNet (crimes na internet): safernet.org.br/denuncie

CAPÍTULO 10

LGPD: seus direitos e como exercê-los

A Lei Geral de Proteção de Dados em linguagem humana — o que você pode exigir.

O que é a LGPD

A Lei Geral de Proteção de Dados (Lei 13.709/2018) regula como empresas e órgãos públicos coletam, armazenam e usam seus dados pessoais no Brasil. Em vigor desde 2020, com multas de até R$ 50 milhões por infração.

Seus 8 direitos como titular de dados

- **Confirmação:** saber se uma empresa tem seus dados
- **Acesso:** receber uma cópia de todos os dados que a empresa tem sobre você
- **Correção:** exigir atualização de dados incorretos ou incompletos
- **Anonimização ou bloqueio:** suspender o uso dos seus dados
- **Eliminação:** pedir a exclusão dos seus dados (com exceções legais)
- **Portabilidade:** transferir seus dados para outro fornecedor
- **Informação:** saber com quem seus dados foram compartilhados
- **Revogação do consentimento:** retirar uma autorização que você deu antes

Como exercer seus direitos

Toda empresa que trata dados deve ter um Encarregado de Proteção de Dados (DPO) e um canal de atendimento. Para solicitar acesso ou exclusão dos seus dados:

- Identifique o contato de privacidade da empresa (geralmente em politica-privacidade@empresa.com)
- Envie e-mail identificando-se com CPF e especificando o direito que deseja exercer
- A empresa tem 15 dias para responder
- Se não responder: registre reclamação na ANPD (anpd.gov.br/ouvidoria)

Vazamentos de dados: o que fazer

Se uma empresa da qual você é cliente sofrer um vazamento que afete seus dados, ela é obrigada a:

- Notificar a ANPD em até 72 horas
- Comunicar os titulares afetados
- Descrever os dados comprometidos e as medidas tomadas

Se não notificada: registre queixa na ANPD. Você pode ter direito a indenização por danos materiais ou morais.

> Circula a notícia de que 'o INSS vai pagar R$ 15.000 por uso indevido de dados'. Isso é golpe. Não existe esse programa. Se alguém entrar em contato com essa proposta, é fraude.

CAPÍTULO 11

Plano de 30 dias para toda a família

Uma tarefa por dia. 30 minutos no máximo. Família protegida ao final.

Segurança digital não se constrói em um dia — mas se constrói em 30. Este plano foi projetado para ser factível: uma ação por dia, nunca mais de 30 minutos, com impacto imediato e duradouro.

Semana 1 — Fundações

Dia 1	Ativar confirmação em dois passos no WhatsApp de todos da família	[ ]
Dia 2	Trocar a senha do roteador doméstico	[ ]
Dia 3	Instalar e começar a usar um gerenciador de senhas	[ ]
Dia 4	Ativar 2FA por app (não SMS) nos bancos principais	[ ]
Dia 5	Revisar privacidade do Instagram e Facebook para perfil privado	[ ]
Dia 6	Criar uma rede Wi-Fi separada para visitantes	[ ]
Dia 7	Conversar com os filhos sobre a 'Regra do Não Brigo'	[ ]

Semana 2 — Proteção financeira

Dia 8	Reduzir limite noturno do PIX para R$ 1.000	[ ]
Dia 9	Verificar se há apps bancários instalados em dispositivos antigos não usados — desinstalar	[ ]
Dia 10	Checar se seu CPF tem pendências no Serasa/SPC (gratuito online)	[ ]
Dia 11	Ativar notificação por push para todas as transações bancárias	[ ]
Dia 12	Rever os apps que têm acesso à sua conta Google ou Apple	[ ]
Dia 13	Ensinar o protocolo de 5 passos para pais e avós	[ ]

Dia 14	Verificar se alguma senha sua aparece em vazamentos: haveibeenpwned.com	[ ]

Semana 3 — Dispositivos e backups

Dia 15	Atualizar todos os sistemas operacionais e apps dos dispositivos da família	[ ]
Dia 16	Configurar backup automático de fotos (Google Fotos ou iCloud)	[ ]
Dia 17	Fazer backup dos documentos importantes em HD externo ou nuvem	[ ]
Dia 18	Atualizar firmware do roteador	[ ]
Dia 19	Desinstalar apps não usados de todos os celulares	[ ]
Dia 20	Ativar localização remota para encontrar celulares perdidos	[ ]
Dia 21	Configurar PIN de bloqueio de SIM no celular de todos da família	[ ]

Semana 4 — Proteção avançada e manutenção

Dia 22	Revisar apps de redes sociais das crianças com elas — sem julgamento	[ ]
Dia 23	Criar um e-mail de recuperação seguro separado do principal	[ ]
Dia 24	Checar as configurações de privacidade do Google Account	[ ]
Dia 25	Definir um 'código familiar anti-golpe' (palavra de verificação para emergências)	[ ]
Dia 26	Cadastrar número de confiança no banco para validação de transações altas	[ ]
Dia 27	Ensinar crianças a identificar phishing com exemplos reais	[ ]
Dia 28	Criar pasta compartilhada com documentos digitalizados da família	[ ]
Dia 29	Revisar controles parentais nos dispositivos das crianças	[ ]
Dia 30	Celebrar: você implementou proteção digital real para sua família.	[ ]

CAPÍTULO 12

Casos reais brasileiros e lições aprendidas

História real, nomes alterados para proteger as vítimas. Cada caso tem uma lição concreta.

Caso 1: Maria, 67 anos, Belo Horizonte

"O rapaz sabia tudo: meu nome, o nome do meu banco, até o saldo aproximado."

Maria recebeu uma ligação de um 'gerente do banco' informando que sua conta estava sendo clonada. Com tom profissional e informações detalhadas (obtidas de um vazamento), o golpista convenceu Maria a transferir R$ 28.000 para uma 'conta segura'.

Lição: Informações pessoais vazadas são usadas para criar autoridade falsa. O nível de conhecimento do golpista não é garantia de legitimidade. Nenhum banco pede transferência para outra conta.

Caso 2: Carlos, 42 anos, São Paulo

"Meu filho me mandou uma mensagem no WhatsApp pedindo R$ 2.000 urgente. Era o número dele."

O número era o mesmo pois o WhatsApp tinha sido clonado. O golpista assumiu a conta do filho e mandou mensagens para todos os contatos. Carlos transferiu antes de ligar para confirmar.

Lição: Verificação de identidade por outro canal (ligação para número salvo na agenda, não o número que mandou mensagem) é mandatória para qualquer transferência.

Caso 3: Beatriz, 15 anos, Recife

Beatriz começou a conversar online com alguém que afirmava ter 17 anos. Após 3 semanas de conversa intensa, a pessoa pediu fotos íntimas, ameaçando expô-la se não colaborasse.

Lição: Grooming não tem perfil fixo. A conversa sobre quem são os amigos online, sem julgamento, é a defesa mais eficaz. Beatriz conseguiu contar para os pais porque tinham essa abertura — e o caso foi denunciado à polícia.

Caso 4: Empresa familiar, Rio de Janeiro

O sócio recebeu um e-mail 'do CEO' (que estava viajando) pedindo uma transferência urgente de R$ 85.000 para um fornecedor novo. O e-mail era idêntico ao padrão da empresa.

Lição: O BEC (Business Email Compromise) atinge empresas de todos os tamanhos. Protocolo: qualquer transferência acima de um valor definido exige confirmação por ligação, independente de quem pediu.

> Em 100% dos casos reais de fraude bem-sucedida que analisei ao longo de 30 anos, havia um momento em que a vítima sentiu desconforto mas decidiu ignorá-lo. Ensine sua família a confiar nesse desconforto. Se algo parece errado, está errado.

// REFERÊNCIA

Glossário

2FA / MFA	Autenticação em dois (ou múltiplos) fatores. Exige algo além da senha para acessar uma conta.
BEC	Business Email Compromise — fraude que usa e-mails corporativos falsos para desviar pagamentos.
Botnet	Rede de computadores infectados controlados remotamente por criminosos.
Criptografia	Técnica de codificar informações para que só o destinatário autorizado possa lê-las.
Deepfake	Conteúdo audiovisual manipulado por IA para parecer que uma pessoa disse ou fez algo que não aconteceu.
DPO	Data Protection Officer — responsável pela proteção de dados em uma empresa (exigido pela LGPD).
Engenharia social	Manipulação psicológica para obter informações confidenciais ou acesso não autorizado.
Firmware	Software interno de um dispositivo de hardware (como o roteador). Deve ser mantido atualizado.
Grooming	Processo pelo qual um adulto constrói relação de confiança com uma criança para fins de abuso.
Hash	Código único gerado a partir de um arquivo ou mensagem — usado para verificar integridade.
IP	Endereço Internet Protocol — identificador numérico de um dispositivo na rede.
Keylogger	Software malicioso que registra tudo que você digita no teclado.

LGPD	Lei Geral de Proteção de Dados (Lei 13.709/2018) — regula o tratamento de dados pessoais no Brasil.
MED 2.0	Mecanismo Especial de Devolução — protocolo do Banco Central para devolver valores de fraudes por PIX.
Phishing	Tentativa de enganar alguém para entregar dados ou clicar em links maliciosos.
Ransomware	Malware que criptografa arquivos e exige pagamento para devolver o acesso.
SIM Swap	Clonagem do chip de celular para desviar SMS e assumir contas do usuário.
Spoofing	Falsificação de identidade digital — número de telefone, e-mail ou endereço IP falso.
VPN	Virtual Private Network — criptografa sua conexão com a internet para maior privacidade.
Zero-day	Vulnerabilidade de software ainda desconhecida pelo fabricante — altamente explorada por hackers.

// RECURSOS

Canais oficiais e ferramentas gratuitas

Golpes e fraudes

Banco Central — Pix e MED 2.0	bcb.gov.br | Tel: 145
Delegacia Online (BO digital)	delegaciaonline.mj.gov.br
SaferNet Brasil (crimes na internet)	safernet.org.br/denuncie
Procon	procon.rj.gov.br | Tel: 151

Verificação e segurança

Have I Been Pwned (checar vazamentos)	haveibeenpwned.com
Agência Lupa (fact-checking)	lupa.news
ANPD (proteção de dados)	anpd.gov.br
Serasa Score (checar CPF)	serasa.com.br

Ferramentas gratuitas

Bitwarden (gerenciador de senhas)	bitwarden.com
Google Authenticator (2FA)	Google Play / App Store
Google Family Link (controle parental)	families.google.com
VirusTotal (checar arquivos suspeitos)	virustotal.com

// SOBRE O AUTOR

Wanderley Abreu Jr. — "Storm"

Wanderley José de Abreu Junior nasceu no Rio de Janeiro em 17 de janeiro de 1978. Conhecido no mundo da cibersegurança pelo nickname Storm, é empresário, pesquisador e ex-hacker com mais de 30 anos de atuação internacional.

Aos 17 anos, invadiu sistemas da NASA e, em vez de processo, foi convidado ao Goddard Space Flight Center (GSFC) para demonstrar o que havia feito. A trajetória que se seguiu inclui trabalho no projeto Galileo (sistema de navegação da Agência Espacial Europeia), desenvolvimento de criptografia multinível para tropas da OTAN no Afeganistão e participação na equipe de comunicação do Mars2020/Perseverance, que pousou o rover em Marte em fevereiro de 2021.

Aos 20 anos, identificou mais de 200 pedófilos como parte da Operação Catedral-Rio — a primeira operação contra pedofilia online realizada no Brasil, conduzida pelo Ministério Público do Rio de Janeiro.

Durante a pandemia, fundou o Mercado Gaia, iniciativa que ajuda no escoamento da safra do Cinturão Verde Fluminense em comunidades do Rio de Janeiro e da Baixada Fluminense.

É Diretor Executivo do Grupo Storm, holding de cibersegurança com atuação em segurança ofensiva e defensiva, consultoria em LGPD, desenvolvimento de software e criação de produtos digitais. Fundador e CEO da Storm Nexus Cibersegurança e co-fundador do SAVIX Shield.

Reconhecimentos

- Medalha Tiradentes — ALERJ (março/2021)
- Medalha Pedro Ernesto — Câmara Municipal do Rio de Janeiro (outubro/2021)
- Medalha do Cinquentenário das Forças de Paz do Brasil — ABFIPONU (maio/2022)
- Biografia publicada pela Editora Objetiva (Grupo Companhia das Letras, novembro/2022): *'Storm: A história do hacker brasileiro que invadiu a NASA, desbaratou crimes na rede e inovou no empreendedorismo digital'* — jornalista Alessandro Greco

savix.stormnexus.com.br

// AGRADECIMENTOS

Obrigado

Este livro não existiria sem a generosidade de pessoas que acreditam que conhecimento é a melhor forma de proteção.

Felipe Neto

Ao Felipe Neto — criador de conteúdo, empreendedor e, acima de tudo, alguém que usa seu alcance para proteger quem mais precisa.

Nossa parceria no SAVIX Shield nasceu de uma crença compartilhada: que segurança digital não pode ser privilégio de quem entende de tecnologia. Tem que ser acessível para a avó de 70 anos, para a mãe que trabalha duas jornadas, para o adolescente que passa horas no TikTok sem saber que está sendo monitorado.

Sua trajetória — da criação de conteúdo que formou uma geração inteira até a atuação junto à ONU em 2023, ao G20 em 2024 e à construção do marco regulatório do ECA Digital em 2025 — inspira o que tentamos fazer aqui: comunicar de forma simples o que é complexo, para que as pessoas possam tomar decisões melhores.

Obrigado por acreditar que uma empresa de segurança pode ter impacto social de verdade.

Às vítimas da Operação Catedral

Este livro também é para as crianças que não tiveram quem as protegesse. E para que isso nunca mais aconteça com nenhuma criança brasileira.

À família Storm

A cada profissional do Grupo Storm que dedica seu trabalho a construir um ambiente digital mais seguro para o Brasil.

Rio de Janeiro, 2026.