UMA PUBLICAÇÃO BLACK ICE SECURITY • EDIÇÃO 1.0 • 2026

STORM NEXUS
GRUPO STORM

BLACK ICE

ALERTA • R$ 10,1 BILHÕES PERDIDOS • UMA FRAUDE A CADA 3 SEGUNDOS NO BRASIL

SEGURANÇA DIGITAL PARA FAMÍLIAS

Como proteger seus filhos, seus pais e seus dados no Brasil de 2026.

O QUE VOCÊ VAI PROTEGER

FILHOS	IDOSOS	PAIS	DADOS
Grooming, sextortion, Roblox, ECA Digital	82% já foram alvo de golpe digital	WhatsApp clonado, falsa central, Pix	LGPD, vazamentos, deepfakes & IA

AUTOR • WANDERLEY ABREU JUNIOR

"STORM"

+30 anos em cibersegurança
NASA • ESA • OTAN • MP-RJ (Catedral-Rio, 1998)
Fundador do Grupo Storm e da Black Ice Security

EDUCATIVO • USO LIVRE

BIS-2026-FAM-001

PROTEGER • EDUCAR • DEFENDER

SEGURANÇA DIGITAL PARA FAMÍLIAS

Como proteger seus filhos, pais e seus dados
no Brasil de 2026

Wanderley J. Abreu Jr.
"STORM"

Storm Nexus • Black Ice Security
Rio de Janeiro, 2026
Edição 1.0

SEGURANÇA DIGITAL PARA FAMÍLIAS

Como proteger seus filhos, pais e seus dados no Brasil de 2026

Autor
Wanderley J. Abreu Jr., "Storm"

Publicação
Storm Nexus, Black Ice Security
stormnexus.com.br • blackice-security.com.br

Pesquisa, redação e curadoria técnica
Equipe técnica Black Ice Security

Revisão
Alessandro Greco

Pós-edição, diagramação e capa
Mayara Reis de Abreu

Identificador
BIS-2026-FAM-001 • Edição 1.0 • Maio de 2026

Aviso legal
O conteúdo deste livro tem caráter informativo e educativo. As recomendações apresentadas não substituem consulta a profissionais especializados em direito, segurança da informação ou saúde mental. O autor e a editora não se responsabilizam por danos decorrentes do uso indevido das informações aqui contidas. Dados, leis e recursos citados refletem o cenário até maio de 2026.

Versão dinâmica, atualizações em stormnexus.com.br/familia

Dedicatória

Àqueles que carregaram comigo o peso desta jornada

Às crianças

Àquelas cujo rosto nunca vi.
Àquelas cujo rosto nunca esqueci.

A todas as vítimas dos crimes da Internet
que cruzaram os arquivos das madrugadas
e nunca mais saíram de mim.

À minha família

que sustentou minhas angústias,
as lágrimas de quem não pôde salvar a todos,
e o peso de ter visto, de perto,
o pior do ser humano,
vezes e mais vezes.

Aos irmãos de tantas operações

que arriscaram a vida por mim e comigo,
sob fogo, sob noite, sob silêncio.
Vocês sabem quem são. Eu também sei…

STORM

Agradecimentos

A quem caminhou comigo até aqui

A Felipe Neto
meu amigo, meu sócio,
e a voz pública mais consequente
na defesa das crianças brasileiras na Internet.
Sem a sua mobilização não haveria ECA Digital;
sem a sua parceria
este livro teria menos esperança
do que o mundo precisa.

À Elba Boechat
que passou tantas madrugadas comigo
no escuro do MP,
compartilhando o café, o silêncio
e o peso das telas
que nenhum de nós deveria ter visto.

Ao Dr. Romero Lyra
por acreditar em um jovem estudante,
por abrir as portas do Ministério Público
a um garoto de vinte anos com um teclado
e uma vontade enorme de ajudar.
O que sou hoje começou ali,
no gabinete que o senhor me confiou.

Ao Dr. José Muiños Piñeiro Filho
então Procurador-Geral de Justiça do Rio de Janeiro,
que deu cobertura institucional
a uma operação inédita no país
e nos amparou quando o caminho era novo demais
até para a própria lei.

Ao Dr. Luiz Noronha Dantas
juiz que assinou os mandados
sem os quais nada teria sido possível.
Cada porta que derrubamos
carregava a sua assinatura
e a sua coragem.

À equipe do Grupo Storm e da Black Ice Security
engenheiros, analistas, pesquisadores e operadores
que respondem incidentes às três da manhã,
fecham CVEs em silêncio,
e fazem o trabalho que ninguém vê
para que famílias inteiras
tenham um sono que ninguém lhes contou que existiu.
Vocês são a muralha real.

E às famílias brasileiras
que carregam, cada uma a seu modo,
o peso de proteger filhos, pais e dados
num mundo projetado para capturá-los.
Este livro é, antes de tudo,
um abraço técnico e afetivo
em torno de vocês.
Se uma única família for poupada de um único golpe,
tudo terá valido.

Wanderley J. Abreu Jr. • Storm
Rio de Janeiro, maio de 2026
Storm Nexus • Black Ice Security • Grupo Storm

Sumário

O que você vai encontrar neste livro

✓ DICA RÁPIDA — Como usar este livro

Se você é pai ou mãe: comece pelo Capítulo 5 (Crianças).
Se você cuida de um pai ou mãe idoso: Capítulo 6 (Idosos).
Se quer agir agora: vá direto ao Capítulo 11 (Plano de 30 dias).
Se já caiu em um golpe: Capítulo 9, seção 9.4 (Primeiras 24 horas).
O livro também pode ser lido em sequência, cada capítulo se sustenta sozinho.

Prefácio

Por que escrevi este livro

Era 1998. Eu tinha 20 anos.

Trabalhei voluntariamente, por mais de um ano, ao lado do então promotor Romero Lyra no Ministério Público do Rio de Janeiro. Toda noite, depois que a cidade dormia, eu me sentava em um quartinho do MP e criava personas falsas para entrar em redes onde pedófilos negociavam crianças como se fossem mercadorias. A Operação Catedral-Rio identificou mais de 200 criminosos. Hoje, eles têm rosto, nome e endereço, e a lei brasileira mudou em parte por causa do que vimos.

Em 1995, três anos antes daquilo, eu havia invadido sistemas da NASA. Em vez de processo, recebi um convite: a agência me chamou ao Goddard Space Flight Center para demonstrar as falhas que encontrei. Voltei para o Brasil com um diploma. Anos depois, trabalhei com a Agência Espacial Europeia no projeto Galileo, escrevi criptografia multinível para tropas da OTAN no Afeganistão, e meu trabalho viajou até Marte com o rover Perseverance.

Conto isso não por vaidade. Conto porque o que aprendi nessas três décadas se resume a uma única lição:

> *"Nenhuma tecnologia, por mais sofisticada, protege uma família que não conversa."*

O Brasil de 2026 é hoje o segundo país do mundo em tentativas de fraude digital, atrás somente da China. Em 2024, famílias brasileiras perderam **R$ 10,1 bilhões** para golpistas. Uma tentativa de fraude a cada três segundos. Mais da metade dos adolescentes brasileiros já sofreu algum tipo de violência sexual online. Oito em cada dez idosos paulistas já foram alvo de pelo menos uma tentativa de golpe.

Esses números não são estatística. São **sua tia, seu filho, seu pai**.

Eu passei a vida do lado técnico da história, descobrindo vulnerabilidades, protegendo infraestruturas críticas, prendendo criminosos. Mas há um lado da guerra que nenhum firewall corporativo resolve: o lado de casa. O lado em que sua mãe recebe um áudio do "neto" pedindo Pix de R$ 2.000 e a voz é exatamente a do seu filho, porque um algoritmo clonou em 15 segundos.

Este livro é o manual que eu queria ter dado para a minha família há dez anos. Está escrito em português direto, sem jargão desnecessário. Onde precisei usar termos técnicos, expliquei. Onde citei um número, indiquei a fonte. Onde recomendei uma ação, mostrei exatamente como fazer.

Você não precisa virar especialista em cibersegurança para proteger sua família. Precisa de três coisas: **informação atualizada**, **configurações certas nos lugares certos**, e **uma conversa honesta com as pessoas que você ama**. Este livro entrega as duas primeiras. A terceira é com você.

Wanderley J. Abreu Jr., Storm
Rio de Janeiro, maio de 2026

CAPÍTULO 01

O Brasil é hoje um campo de batalha digital

Por que toda família brasileira já é alvo, e o que isso significa na prática

Em uma quinta-feira qualquer de março de 2024, em Santo André (SP), uma aposentada de 79 anos recebeu uma ligação. Do outro lado, uma voz educada identificou-se como gerente do seu banco. Disse que havia movimentações suspeitas e que precisava da ajuda dela para "bloquear o golpe em andamento". A conversa durou **quatro horas**. Quando ela desligou, sua conta tinha um saldo a menos de **R$ 25 mil**.

■ CASO REAL — Anatomia técnica do golpe: Santo André, março de 2024

Pré-requisito do criminoso: base vazada com CPF, nome completo, endereço e últimos quatro dígitos do cartão da vítima (provavelmente oriunda dos megavazamentos de 2021-2023 negociados por R$ 200-500 na dark web).

Vetor inicial: ligação VoIP com identificador clonado (spoofing do 0800 oficial do banco), a vítima viu no visor o número real da central de atendimento.

Engenharia social aplicada: uso dos dados vazados na primeira frase para gerar confiança ("confirma os últimos quatro dígitos do cartão: 1247?"). Em seguida, criação de urgência artificial ("tem uma tentativa de Pix de R$ 8.300 saindo agora").

Captura prolongada: o criminoso manteve a vítima ao telefone por 4 horas, tempo calculado para impedir que ela ligasse para familiares ou ao banco real. Cada transferência foi orientada como "medida de segurança para uma conta-cofre temporária em seu próprio nome".

Lavagem do dinheiro: os Pix saíram em pequenas parcelas (abaixo de R$ 5.000 cada, justamente para não disparar alertas de antifraude do banco) e foram para contas de "laranjas" que os pulverizaram em mais 3-4 transferências em minutos.

Defesas que teriam impedido: (1) *limite Pix noturno e diário baixo* (R$ 200/dia para idosos); (2) *regra familiar de palavra-código* antes de qualquer transação por orientação telefônica; (3) *política de "desligar e ligar de volta no número do cartão"* diante de qualquer pedido de movimentação; (4) *cadastro de contato de confiança* que receba alertas de transações incomuns.

Status do MED-Pix: aberto contestação 5 horas após o golpe, banco recuperou aproximadamente R$ 7.000 dos R$ 25.000 nos primeiros 11 dias de análise. O restante havia sido sacado em espécie antes do bloqueio cautelar.

Esse não é um caso isolado. É a fotografia exata do Brasil de hoje. Vamos aos números, e depois ao que fazer com eles.

1.1 Os números que você precisa enxergar

R$ 10,1 bi
PERDAS COM FRAUDES EM 2024
Febraban

+220%
CRESCIMENTO DE MALWARE EM 2025
BioCatch (1º sem.)

51%
DOS BRASILEIROS FORAM VÍTIMAS
Painel gov.br 2024

1 a cada 3s
TENTATIVAS DE FRAUDE EM 2024
1º sem., gov.br

R$ 6.311
PREJUÍZO MÉDIO POR VÍTIMA
TransUnion 2025

87.689
DENÚNCIAS DE CRIMES CIBERNÉTICOS
SaferNet 2025 (+28%)

O Painel de Fraudes Bancárias Digitais, lançado em dezembro de 2025 pelo governo federal em parceria com a Febraban, confirmou: o Brasil é hoje o **segundo país do mundo em tentativas de golpes**, atrás apenas da China. Em apenas dois anos, os golpes via Pix causaram **R$ 2,7 bilhões em prejuízo**, com crescimento de 43%. A Serasa Experian bloqueou **6,9 milhões** de tentativas só no primeiro semestre de 2025, uma a cada 2,3 segundos.

■ **ATENÇÃO — O que mudou em relação aos anos anteriores**

O alvo migrou para o celular. A Kaspersky aponta que o Brasil concentra mais de 80% das detecções de trojan bancário da América Latina, 1,5 milhão de ataques entre agosto/2024 e junho/2025, média de 4.109 por dia.

A IA virou ferramenta de golpe em massa. Bastam 15 a 30 segundos de áudio público para clonar uma voz. No Brasil, o crescimento de golpes com deepfake foi de 830% em um ano.

O jovem virou alvo principal. Fraudes contra jovens cresceram mais de 40% no 1º semestre de 2025, superando idosos pela primeira vez (Serasa Experian).

1.2 Quem está sendo atacado

A imagem clássica do golpe, o idoso ingênuo sendo enganado por um falso gerente, ainda existe, mas é cada vez menos representativa. A guerra digital de 2026 ataca os **três núcleos** da família brasileira ao mesmo tempo, com táticas diferentes para cada um:

Perfil	Principal vetor de ataque	Característica explorada
Crianças (6–12)	Predadores em jogos online (Roblox, Discord)	Curiosidade, busca de afeto, fragilidade
Adolescentes (13–17)	Sextortion, cyberbullying, deepfake íntimo	Vergonha, busca de validação, impulsividade
Jovens adultos (18–25)	Golpe do investimento, apps de namoro	Excesso de confiança em tech, FOMO
Adultos (26–55)	Falsa central, WhatsApp clonado, Pix	Pressa, sobrecarga, multitarefa
Idosos (60+)	Falso parente, falso médico, consignado fraudulento	Solidão, hierarquia, dificuldade tech

Em uma família típica de cinco pessoas (pai, mãe, dois filhos, um avô), hoje convivem **cinco superfícies de ataque simultâneas**, cada uma exigindo uma defesa diferente. É por isso que segurança digital familiar não é uma decisão técnica: é uma política de casa.

1.3 As três camadas da defesa familiar

Ao longo deste livro, você vai ver que toda recomendação se encaixa em uma de três camadas. Memorize-as agora, elas são o esqueleto do pensamento defensivo:

TECNOLOGIA , Configurações certas nos lugares certos
Senhas fortes em gerenciador, 2FA por app, MED-Pix ativado, controle parental, limites de transação, biometria no chip.

PROCESSO , Regras combinadas em família
Palavra-código familiar para emergências, regra das 24 horas para Pix urgente, lista de contatos de emergência impressa.

DIÁLOGO , Conversa honesta e contínua
Reuniões mensais de "atualização de golpes", abertura para que filhos contem erros sem julgamento, escuta dos idosos.

1.4 Por que os criminosos atacam famílias agora

A indústria do crime digital brasileiro amadureceu. Não estamos mais falando de adolescentes solitários em um quarto. Existem **quadrilhas organizadas** com divisão de trabalho:

1. Operadores de phishing compram bases de dados vazadas (o vazamento "MORGUE" de 2026 colocou 251 milhões de CPFs à venda por US$ 500 em bitcoin). Com CPF, nome da mãe e endereço, montam spear phishing personalizado.

> **■ SAIBA MAIS — O que é o vazamento MORGUE**
>
> Em **abril de 2026**, um ator anônimo colocou à venda na **dark web** (parte da Internet acessível apenas por navegadores especiais como Tor) um pacote chamado "MORGUE" contendo registros de **251 milhões de CPFs brasileiros**, com nomes completos, datas de nascimento, nomes de mães, endereços e telefones.
>
> O preço pedido foi **US$ 500 em bitcoin**, equivalente a uma camiseta de futebol. Para comparação, o vazamento anterior, "Fim do Mundo" (2021), tinha 223 milhões de CPFs e era oferecido por milhares de dólares.
>
> **Por que importa para a sua família:** qualquer ligação que você ou seu pai receba pode começar com o golpista citando seu CPF, endereço completo e nome da sua mãe. Isso não significa que ele conhece você, significa que ele comprou um banco de dados. A defesa não é esconder os dados (impossível), é desconfiar de qualquer pedido de transação feito por telefone, mesmo de "atendentes" que aparentam ter informações privilegiadas.

2. Engenheiros sociais em call centers clandestinos (muitos em Goiás e SP) ligam para as vítimas munidos desses dados e mantêm pessoas até quatro horas ao telefone.

3. Mulas financeiras emprestam contas de pessoas físicas ("laranjas") em troca de comissão para receber os Pix das vítimas.

4. Desenvolvedores de malware mantêm famílias de trojans • Grandoreiro, GoPix, Casbaneiro, em constante evolução, mirando bancos brasileiros especificamente.

5. Especialistas em IA oferecem serviços de clonagem de voz e deepfake como produto: pagam-se centavos por minuto de voz clonada. Aproveitam plataformas comerciais que não bloqueiam usos não consensuais.

> **■ PERIGO — A nova economia do crime**
>
> Estima-se que o lucro do crime cibernético brasileiro supere o tráfico de drogas em algumas regiões. A barreira de entrada é baixa, o risco de prisão é menor (estelionato qualificado tem pena máxima de 8 anos), e a recompensa pode chegar a milhões por operação.
>
> É contra **essa indústria** que sua família está jogando.

1.5 A boa notícia: 90% dos golpes podem ser evitados

Apesar do cenário, a maioria absoluta dos golpes que atingem famílias brasileiras é evitável com medidas simples. Isso porque o crime digital trabalha em **escala**: o golpista que liga para a sua mãe também ligou para outras 200 mães naquela tarde. Ele aposta na lei dos grandes números. Basta que **1%** caia para o golpe ser lucrativo.

O nosso trabalho como família é simples: deixar de ser esse 1%.

Não precisamos ser perfeitos. Não precisamos blindar-nos contra um serviço de inteligência estrangeiro. Precisamos apenas estar um pouco acima do esforço médio que o criminoso espera encontrar. Quando ele percebe que sua mãe tem PIN no SIM, que seu pai sempre liga de volta antes de Pix, que seu filho tem conta privada no Instagram, ele simplesmente vai embora para a próxima família.

✓ DICA RÁPIDA — A regra de ouro do livro

Se você implementar **tudo** que está neste livro, sua família estará mais protegida que 99% das famílias brasileiras. Você nunca terá proteção total, mas terá **proteção suficiente** para que o criminoso prefira atacar outra pessoa.

Esse é, sinceramente, o melhor desfecho possível.

CAPÍTULO 02

Os golpes que mais atacam seu celular

WhatsApp clonado, falsa central, Pix, SIM swap e trojans bancários

O celular substituiu a agência bancária, o cartório, a foto de família e até a chave de casa. Por isso, ele se tornou o **alvo número um** dos criminosos. Segundo a Febraban, três golpes respondem pela maior parte do prejuízo causado a brasileiros em 2025:

#	Golpe	Como ataca	Defesa-chave
1	Clonagem de cartão por NFC	Aproximação não autorizada de cartão na rua/transporte	Carteira RFID-blocker; desabilitar contactless de alto valor
2	Falsa central / falso funcionário	Ligação convincente após vazamento de dados pessoais	Nunca falar de transações no telefone; sempre desligar e ligar de volta
3	WhatsApp clonado	Engenharia social pedindo Pix para "novo número" de parente	Confirmação em duas etapas; palavra-código familiar

2.1 Golpe do WhatsApp clonado

Apesar do nome, na maioria dos casos **nada é clonado tecnicamente**. É puro teatro digital:

Como funciona, passo a passo:

1. O criminoso pega uma foto pública sua no Instagram, Facebook ou WhatsApp (foto de perfil visível para "todos"). Pega também seu nome completo, talvez profissão, talvez o nome de um filho ou neto.
2. Cria uma conta nova de WhatsApp com um número aleatório (chip descartável ou virtual). Coloca sua foto e seu nome como nome do contato.
3. Aborda seus parentes mais próximos: "Oi mãe, é o João. Quebrei meu celular, perdi o chip, estou usando o número de um amigo. Anota aí para me salvar."
4. Espera 1–2 dias para criar familiaridade. Conversa naturalmente. Pergunta como vai a família, finge interesse.
5. Cria a emergência: "Mãe, preciso pagar um boleto que vence hoje, tô sem internet no banco. Pode fazer um Pix de R$ 1.800 para essa chave aqui? Depois te devolvo."
6. A "chave" é o CPF de um laranja contratado pela quadrilha. Em segundos, o dinheiro desaparece em uma cadeia de transferências.

Como blindar sua família contra esse golpe:

■ CHECKLIST — Configuração obrigatória do WhatsApp

1. Ativar Confirmação em Duas Etapas: Configurações → Conta → Confirmação em duas etapas → ATIVAR. Crie um PIN de 6 dígitos que você se lembre. Anote-o em local seguro (gerenciador de senhas).

2. Limitar a foto de perfil: Configurações → Privacidade → Foto do perfil → "Meus contatos".

3. Limitar o "Visto por último" e "Info": também para "Meus contatos", golpistas usam essas informações.

4. Esconder grupos: Privacidade → Grupos → "Meus contatos" (impede que estranhos te adicionem em grupos de golpe).

5. Verificar dispositivos conectados mensalmente: WhatsApp Web → Dispositivos conectados. Desconecte qualquer sessão que você não reconheça imediatamente.

✓ DICA RÁPIDA — A "palavra-código familiar"

Combine com toda a família estendida (pais, filhos, irmãos, avós, tios, primos) **uma palavra ou frase curta** que jamais aparecerá por escrito. Pode ser uma piada interna, o nome do cachorro da infância, qualquer coisa fácil de lembrar mas impossível de adivinhar de fora.

Sempre que houver pedido urgente de Pix, vídeo ou áudio em situação de emergência, pergunte a palavra-código. Se o interlocutor titubear, é golpe.

Atenção: não compartilhe essa palavra em chat algum. Combine pessoalmente, em reunião familiar.

2.2 Golpe da falsa central / falso funcionário do banco

É o que mais cresceu em 2025: **dobrou no Brasil**, segundo o relatório BioCatch. É também o mais devastador, porque combina engenharia social profissional com dados pessoais vazados.

O script clássico:

> • *"Bom dia, Sr. Antônio. Falo da Central de Segurança do Banco X. Estamos identificando movimentações suspeitas na sua conta agora há pouco. O senhor está em casa? Para sua segurança, vou pedir que confirme alguns dados. O senhor é portador do CPF terminado em 47, correto? E reside na rua tal, número tal? Perfeito. Olha, temos uma tentativa de Pix de R$ 8.300 partindo da sua conta agora. O senhor autorizou?"*

Como o criminoso já tem dados básicos vazados (CPF, endereço, talvez últimos 4 dígitos de cartão), **tudo parece legítimo**. A vítima, em pânico, segue as instruções: "transferir para uma conta de segurança em seu próprio nome", "instalar o app oficial do banco" (que é trojan), "informar o token para o atendente verificar".

■ PERIGO — A regra simples que invalida 100% desse golpe

Nenhum banco do Brasil liga pedindo:

• para você transferir dinheiro;

• para você instalar nenhum aplicativo;

• para você informar senha, token, código SMS ou biometria;

• para você dizer códigos lidos pela máquina.

O que fazer SEMPRE, sem exceção: desligue. Pegue o cartão. Disque o número que está atrás dele. Ligue para o banco. Se houver problema real, eles confirmam.

2.3 Golpes de Pix

O Pix democratizou a transferência instantânea, e a fraude instantânea. Há cinco variações principais que sua família precisa reconhecer:

A. Pix errado intencional

Golpista envia Pix para sua conta "por engano", em seguida pede a devolução. Você devolve, mas depois o banco do golpista contesta o Pix original, descobrindo que veio de uma vítima de fraude. **Você fica no prejuízo.**
Defesa: nunca devolva por iniciativa própria. Diga: "abra a contestação pelo seu banco, pelo MED, eu devolvo automaticamente". Se for legítimo, ele aceita.

B. Falso depósito

Golpista envia comprovante falso de Pix recebido em pagamento. Você libera o produto/serviço. Não chega Pix nenhum.
Defesa: nunca confie em prints. Sempre confirme no extrato do app do banco (não no SMS, que pode ser falso).

C. QR Code falso

Em adesivos sobrepostos em estabelecimentos, ou em sites de e-commerce, o QR redireciona para conta do criminoso com valor adulterado.
Defesa: sempre leia o nome do recebedor e o valor antes de confirmar. Se houver discrepância, cancele.

D. Pix com chave digitada errada

Você digita uma chave errada (1 dígito). O dinheiro vai para outra pessoa. **O MED-Pix não cobre erro do usuário.**
Defesa: cadastre destinatários frequentes na agenda Pix do app. Para qualquer Pix novo acima de R$ 200, confira nome do recebedor antes de confirmar.

E. Golpe da maquininha "venda paga"

Em comércio, golpista finge problema na maquininha após primeira tentativa e te induz a fazer Pix "direto para o dono". O Pix vai para outro CPF.
Defesa: sempre confira o nome do recebedor antes de confirmar Pix. Se for diferente do estabelecimento, recuse.

2.4 SIM swap: o golpe que entra pela operadora

Talvez o golpe mais subestimado pelo brasileiro médio. O criminoso não precisa hackear o seu celular: ele convence a operadora a **transferir o seu número para o chip dele**. A partir desse momento, todos os SMS de recuperação de senha do seu banco, WhatsApp, e-mail e Instagram passam a chegar no celular do golpista.

Como acontece:

1. Criminoso coleta seus dados em vazamentos: CPF, RG, endereço, data de nascimento, nome da mãe.
2. Liga (ou vai a uma loja) da sua operadora se passando por você. Diz que "perdeu o celular" e quer "ativar um novo chip".
3. O atendente, pressionado por metas ou despreparado, aciona o novo chip, e seu chip original vira "pirueta de plástico". Você fica **sem sinal**.
4. Em minutos, o criminoso recebe SMS de recuperação de senha do seu banco, WhatsApp, e-mail, Instagram. Esvazia tudo.

■ PERIGO — O sinal que sua família deve aprender a reconhecer

Se o seu celular ficar **sem sinal de uma operadora subitamente** (mas com Wi-Fi funcionando), em horário comercial e sem chuva, considere SIM swap até prova em contrário.

Ação imediata: em outro telefone, ligue para a operadora e bloqueie o chip. Ligue para o seu banco e bloqueie a conta. Acesse seu e-mail (do computador) e troque a senha. Você tem **minutos**, não horas.

■ CHECKLIST — Defesa em camadas contra SIM swap

1. PIN no chip (SIM PIN): ative no seu celular (4-8 dígitos exigidos a cada reinicialização). Mesmo que o chip caia em mãos erradas, fica inutilizado sem o PIN. Configurações → Celular → SIM → PIN do SIM.

2. Senha de atendimento na operadora: Vivo, Claro, TIM e Algar permitem cadastrar uma senha extra exigida em qualquer atendimento. Peça isso por telefone ou no app da operadora.

3. Biometria contra base gov.br: a Resolução Anatel 658/2023 (vigência desde junho/2024) tornou obrigatória a biometria facial para ativação de linhas e portabilidade. Em abril de 2026, a Anatel apertou ainda mais: a validação agora é feita contra a base do **gov.br/Serpro** (não mais contra foto interna da operadora), o que dificulta o uso de selfies vazadas em pacotes de dados antigos.

4. Bloqueio automático de 48 horas: também desde abril de 2026, qualquer alteração cadastral significativa (mudança de endereço, e-mail principal ou senha) trava automaticamente pedidos de portabilidade ou troca de chip por 48 horas.

5. Notificação dupla obrigatória: a operadora atual deve avisar você **por SMS e por e-mail** sempre que receber um pedido de portabilidade ou troca de chip. Se você receber esse aviso e não foi você que pediu, tem 30 minutos para contestar antes do bloqueio do chip antigo. Aja imediatamente.

6. 2FA sem SMS: sempre que possível, troque SMS por app autenticador (Google Authenticator, Authy, Microsoft Authenticator) ou chave física FIDO2 (YubiKey). O SMS é o elo mais fraco e continuará sendo, mesmo com todas as proteções novas da Anatel.

■ ATENÇÃO — Próxima fronteira: golpe do eSIM

À medida que a Anatel fechou o cerco sobre a troca de chip físico, criminosos começaram a testar variações com **eSIM** (chip digital, sem cartão físico, presente em iPhones e Androids mais novos). O ataque é o mesmo: convencer a operadora a provisionar seu número em um eSIM controlado pelo criminoso. Como o eSIM dispensa visita à loja, a engenharia social fica mais difícil de barrar.

Defesa: nas operadoras que oferecem eSIM, peça o **bloqueio explícito de migração para eSIM** sem autenticação presencial. Vivo, Claro e TIM já oferecem essa opção pelo app (procure por "bloqueio de transferência de eSIM" ou contate o atendimento).

2.5 Trojans bancários: o inimigo invisível no Android

O Brasil concentra **80% das detecções de trojan bancário da América Latina**, segundo a Kaspersky. São aplicativos maliciosos que se disfarçam de utilitários comuns (atualizações do WhatsApp, falsos apps de banco, "limpadores de cache") e, uma vez instalados, sobrepõem telas falsas sobre o app legítimo do banco para roubar credenciais e códigos.

Famílias de trojans ativas no Brasil em 2026:

Família	Plataforma	Como age
Grandoreiro	Windows + macOS	Sobrepõe telas falsas em sessões bancárias; mira 1.700 bancos em 45 países.
GoPix	Windows	Injeta certificado-raiz no navegador para man-in-the-middle em Pix.
Brata / Coper	Android	Distribuído como falso app de banco; rouba SMS e overlay de tela.
Casbaneiro	Windows	Trojan brasileiro veterano; ativo desde 2018 com novas variantes.
Mamont / Agent / Creduz	Android (novas, 2025)	Foco em mobile; explora permissões de acessibilidade do Android.

■ CHECKLIST — Como blindar o Android da sua família

1. Instale aplicativos **apenas da Play Store oficial**. Recuse APKs de WhatsApp, links de "atualização" enviados por SMS, qualquer instalação fora da loja.

2. Desative "fontes desconhecidas" em Configurações → Segurança.

3. Revise permissões de Acessibilidade: Configurações → Acessibilidade. Se houver app que você não reconhece com permissão de acessibilidade ativa, **desinstale imediatamente**, é provável que seja trojan.

4. Mantenha o Play Protect ATIVO e o sistema operacional atualizado. Telefones que não recebem mais atualização há mais de 3 anos estão fora de uso seguro para banco.

5. Use o app oficial do banco, nunca o site mobile, que pode ser falsificado.

2.6 Outros golpes de celular que sua família precisa conhecer

■ **Falso motoboy de cartão.** "Seu cartão foi clonado, vamos mandar um motoboy buscar para destruir." Nunca aconteceu na história, bancos não buscam cartões em domicílio.

■ **Falso boleto.** Boleto recebido por e-mail ou WhatsApp com código de barras adulterado. Sempre confirme o beneficiário antes de pagar; banco mostra antes da confirmação.

■ **Falso suporte técnico.** Pop-up "Seu PC tem vírus, ligue para esse 0800". O técnico pede acesso remoto via AnyDesk/TeamViewer e instala ransomware.

■ **Falso emprego.** Mensagem oferecendo trabalho remoto com salário alto. Pede taxa de cadastro/uniforme/exame admissional. Emprego não cobra taxa de adesão.

■ **Investimento em cripto / pirâmide.** Promessa de retorno garantido acima do CDI. Toda promessa de rentabilidade garantida em investimento de risco é fraude.

■ **Smishing.** SMS com link encurtado: "Sua encomenda dos Correios está retida. Clique para regularizar". Os Correios nunca pedem regularização por SMS.

■ **Golpe da nudez.** Mensagem alegando ter vídeos íntimos seus (mesmo sem ter). Pede Bitcoin. Bluff puro, apague, bloqueie, reporte.

✓ DICA RÁPIDA — A heurística que pega 95% dos golpes em celular

Antes de qualquer ação que envolva clique em link, pagamento, envio de código ou instalação de app:

Pergunte-se: "Estou agindo sob pressão de tempo? Estou com sentimento de urgência, medo ou ganância?"

Se a resposta for **sim**, pare. Levante da cadeira. Espere 10 minutos. Ligue para alguém da família para "narrar" o que aconteceu. Em 95% dos casos, contar a história em voz alta revela a fraude imediatamente.

A pressa é o melhor amigo do golpista. A pausa é a sua melhor defesa.

CAPÍTULO 03

Sites falsos, e-mails fraudulentos e ransomware doméstico

A guerra pelo navegador, pela caixa de entrada e pelos arquivos da família

Se o celular é o campo de batalha mais quente, o navegador é o segundo. Em 2025, o Google bloqueou ou removeu **8,3 bilhões de anúncios maliciosos** e suspendeu 24,9 milhões de contas, números que dão a dimensão do volume industrial de ataques aos quais sua família é exposta diariamente.

3.1 Phishing: o golpe que envelheceu, e ficou mais perigoso

Phishing é o e-mail/SMS/mensagem que se passa por instituição legítima (banco, Receita, INSS, Correios) para enganar você. A versão antiga, cheia de erros de português, foi substituída pela versão com IA: textos perfeitos, logos corretos, urls quase idênticas à oficial.

Anatomia de um phishing moderno:

Remetente: `atendimento@bancos-segura.com.br` ← domínio falso (banco real seria @bancodobrasil.com.br)
Assunto: "URGENTE: tentativa de Pix bloqueada, confirme em 24h"
Corpo: bem escrito, logo do banco, pedindo clique em botão "Verificar Agora"
Link: `bb-verificacao.app/login` ← URL falsa que parece oficial

> ■ **CHECKLIST — Os 5 sinais de phishing que sua família deve memorizar**
>
> **1. Urgência artificial:** "responda em 24h ou sua conta será bloqueada".
>
> **2. Remetente com domínio levemente diferente:** `bancodobrasil-seguro.com` (falso) vs `bb.com.br` (real).
>
> **3. Link encurtado ou disfarçado:** passe o mouse sobre o link (no celular, mantenha apertado) e veja a URL real. Se não bater com o banco, é fraude.
>
> **4. Pede informações que o banco nunca pede:** senha completa, CVV do cartão, token, código SMS, biometria por foto.
>
> **5. Saudação genérica:** "Caro cliente" em vez do seu nome (embora a IA já personalize, não confie só nisso).

A regra de ouro do navegador: nunca clique em link de e-mail/SMS para acessar seu banco. Sempre **digite o endereço você mesmo** ou abra o aplicativo oficial. Esse hábito sozinho elimina 99% do risco de phishing bancário.

3.2 E-commerce fake: a loja que não existe

Pesquisa Seade SP TIC 2025: **26% dos idosos e 40% dos brasileiros** em geral já compraram em loja online inexistente. Os picos acontecem em Black Friday, Natal e Dia das Mães. O modus operandi é simples: criar um site bonito, anunciar produto desejado com 50% de desconto, aceitar apenas Pix, sumir após o pagamento.

■ CHECKLIST — Checklist antes de comprar em loja desconhecida

✓ Verifique o **CNPJ** no rodapé do site. Consulte em `solucoes.receita.fazenda.gov.br/Servicos/cnpjreva`. Sem CNPJ no rodapé? Saia.

✓ Pesquise no **Reclame Aqui** e no **Google** com termos "[nome da loja] golpe", "[CNPJ] fraude".

✓ Desconfie de **preço 50%+ abaixo** do mercado. iPhone novo a R$ 3.000 em 2026 é golpe.

✓ Verifique se o site aceita **cartão de crédito**. Loja que só aceita Pix para CPF de pessoa física é red flag gigantesco, cartão dá direito a contestação (chargeback).

✓ Confira se o **nome do recebedor do Pix** bate com o CNPJ da empresa. Quase nunca bate em sites falsos.

✓ Pague com **cartão virtual** de uso único quando disponível (Nubank, Itaú, C6 oferecem). Limita o prejuízo a uma única compra.

3.3 Falsos sites governamentais

Receita Federal, INSS, Bolsa Família e Caixa são os órgãos mais imitados, porque emocionam (medo de imposto, esperança de auxílio). Em 2025, golpistas usaram IA generativa para criar mensagens cobrando "taxa de R$ 59,90 para liberar indenização do vazamento Serasa".

■ SAIBA MAIS — Cinco verdades imutáveis sobre órgãos do governo

1. Nenhum órgão público pede pagamento para liberar benefício, indenização ou restituição.

2. A Receita Federal nunca envia link por SMS, e-mail ou WhatsApp pedindo "regularização".

3. O INSS não pede recadastramento por aplicativo baixado em link.

4. O gov.br só usa o domínio **.gov.br**. Endereços com **.com**, **.org** ou **.app** não são oficiais.

5. Se há dúvida, vá ao site digitando o endereço você mesmo ou use o app oficial baixado da loja.

3.4 Ransomware doméstico

Ransomware é o vírus que **criptografa todos os arquivos** do seu computador (fotos, documentos, vídeos da família) e exige pagamento em bitcoin para liberar. Antes era problema corporativo. Hoje atinge famílias com NAS, backups locais ou pequenos negócios em casa.

Como entra:

Tipicamente por anexo de e-mail (planilha que pede "habilitar macros"), instalação de software pirata, ou clique em propaganda maliciosa em site de download de filme/série. Em 2025, golpistas começaram a distribuir ransomware como "atualização do Windows" em SMS, principalmente para pequenas empresas e profissionais autônomos em home office.

✓ DICA RÁPIDA — Estratégia 3-2-1: o backup que salva sua família

3 cópias de tudo que importa, fotos, documentos, trabalhos escolares dos filhos, vídeos.

2 mídias diferentes, por exemplo: o próprio computador e um HD externo.

1 cópia offsite, em nuvem (Google Drive, iCloud, OneDrive, Backblaze) ou em casa de um parente.

Com o 3-2-1, mesmo se o ransomware criptografar tudo, você reformata o computador e restaura os arquivos. Sem pagar um centavo ao criminoso.

■ PERIGO — Não pague o resgate

1. Pagar não garante recuperação. Em 30% dos casos, mesmo após pagamento, a chave de descriptografia não funciona ou nem chega.

2. Pagar financia novos ataques. Você está custeando o próximo golpe contra outra família.

3. Você pode estar pagando criminosos sancionados, em alguns países (não no Brasil ainda), isso é crime.

4. A polícia tem chaves públicas: o site **nomoreransom.org** oferece descriptografadores gratuitos para mais de 150 famílias de ransomware. Tente lá antes de qualquer pagamento.

3.5 Falso antivírus e scareware

Pop-ups gritando "SEU PC TEM 47 VÍRUS!! CLIQUE AGORA!!" são o golpe mais antigo da Internet, e ainda funcionam, especialmente com idosos. O clique instala malware ou cobra licença de "antivírus premium" inexistente.

■ SAIBA MAIS — Regras sobre antivírus em casa

1. No Windows 10/11, o **Windows Defender** nativo é suficiente para uso doméstico médio. Mantenha-o ativo e atualizado.

2. No macOS e iOS, a Apple não oferece "antivírus" porque o sistema tem proteções suficientes, desconfie de qualquer "antivírus para Mac/iPhone" oferecido por pop-up.

3. Se quiser camada adicional, instale apenas **antivírus pago legítimo** (Kaspersky, Norton, Bitdefender, ESET), baixe do site oficial, nunca via link de pop-up.

4. Pop-up de antivírus em navegador é **sempre** fraude. Antivírus real não anuncia em janela do navegador.

CAPÍTULO 04

Redes sociais: privacidade, golpe do amor e stalkerware

O que você posta hoje é a matéria-prima do golpe de amanhã

Toda foto pública é um dado. Todo Stories de viagem é uma confissão de que sua casa está vazia. Todo áudio postado é matéria-prima para clonagem de voz. Em redes sociais, **menos é segurança**.

4.1 Romance scam: o golpe do amor

1 em 5
BRASILEIROS EM APPS DE NAMORO
já foi alvo (Norton 2025)

R$ 440 mi
PERDAS PROJETADAS ATÉ 2028
ACI Worldwide

40+
IDADE-ALVO PREFERIDA
mulheres divorciadas/viúvas

O romance scam é um dos golpes **mais lucrativos** por vítima, em 2025, uma mulher capixaba perdeu R$ 5,7 milhões; outra, no Rio, R$ 500 mil. O criminoso investe semanas ou meses construindo um relacionamento emocional antes de pedir dinheiro.

■ CASO REAL — Anatomia técnica do golpe: Espírito Santo, 2025 (R$ 5,7 milhões)

Vetor inicial: contato no Instagram por perfil de "engenheiro de petróleo americano trabalhando em plataforma offshore". Fotos roubadas de perfil legítimo de um engenheiro da Noruega (descoberto depois por reversão de imagem), montagens em frente a plataformas, em viagens, com filhos genéricos.

Construção de confiança (4 meses): chamadas de voz frequentes com áudio levemente granulado ("ruído da plataforma") • tática para esconder o sotaque real do operador, que era brasileiro. Mensagens em inglês mediadas por Google Translate, com tradução rebuscada que a vítima atribuía ao "estilo formal" do engenheiro.

O ponto de virada técnico: em vez do clássico "preciso de taxa para vir ao Brasil", o criminoso apresentou um "fundo de investimento offshore", um site falso muito bem feito, com painel de controle simulando rendimentos diários. A vítima podia "acompanhar seu dinheiro crescendo". Foi convencida a transferir em três grandes blocos.

Lavagem em escala industrial: os R$ 5,7 milhões foram para contas de PJ de fachada (lojas que abrem e fecham em meses), fragmentados em compras de criptoativos via P2P (LocalBitcoins, Binance P2P) e cash-out em diversos países por mulas.

Defesas que teriam impedido: (1) *reversão de imagem no Google Images* nas primeiras semanas teria revelado o engenheiro norueguês real; (2) *conversa com filhos/amigos próximos* antes do primeiro Pix, o padrão de "fundo de investimento exclusivo com retorno garantido" é red flag absoluto; (3) *consulta à CVM* antes de qualquer investimento, fundo legítimo é registrado; (4) *regra de ouro*: não existe relacionamento online verdadeiro que precise de transferência financeira antes do primeiro encontro presencial.

O ciclo clássico em três fases:

FASE 1, Love Bombing (2-4 semanas)

Atenção excessiva, mensagens carinhosas dia e noite, "alma gêmea", compartilhamento intenso de "vida" (foto de filho fictício, trabalho em plataforma de petróleo no exterior, militar em missão).

FASE 2, Ponto de virada (1 mensagem)

Surge uma emergência: acidente, doença súbita da mãe, taxa para vir ao Brasil pelo primeiro encontro, problema no embarque do navio onde "está com seu dinheiro preso".

FASE 3, Extração (vai durar enquanto pagar)

Vítima envia primeira quantia. Mais "emergências" vêm em sequência. Se ela parar de pagar, ameaça expor conversas íntimas ou some.

■ PERIGO — Sinais de alerta em apps de relacionamento

1. Pessoa "perfeita demais": foto modelo, profissão glamourosa (médico militar, engenheiro de petróleo, piloto), morando em outro país, viúvo recente.

2. Recusa videochamada com desculpas frequentes ("trabalho não permite", "área sem sinal", "câmera quebrada").

3. Move a conversa rapidamente do app para WhatsApp/Telegram particular.

4. "Te amo" em menos de duas semanas; planos de casamento antes de se conhecer pessoalmente.

5. Em algum momento, surge problema financeiro que SOMENTE você pode resolver.

Defesa: faça **reversão de imagem** em `images.google.com` com a foto dele. Quase sempre é foto roubada de outro perfil.

4.2 Catfishing e deepfake romance

Catfishing é assumir identidade falsa em redes sociais, geralmente fotos roubadas de outra pessoa. Em 2025, a Norton documentou que **29%** das vítimas brasileiras de fraudes em apps caíram em catfishing.

A novidade é o uso de **deepfake em chamadas de vídeo**: em janeiro de 2025, uma mulher nos EUA perdeu US$ 60 mil acreditando estar em relacionamento com Elon Musk, com FaceTime falso. No Brasil, o golpe mais comum é o "militar americano em missão na Síria", quase sempre usando fotos roubadas de soldados reais dos EUA.

■ CASO REAL — Anatomia técnica do golpe: Acadiana, janeiro de 2025

Vetor inicial: contato no Facebook por perfil que se apresentava como "Elon Musk verificado em conta secundária". A vítima, divorciada, 50+ anos, isolada socialmente, foi selecionada por algoritmo de perfilamento que rastreia engajamento com posts de notícias sobre celebridades.

Construção de confiança (love bombing, 6 semanas): mensagens diárias, áudios "do Elon" gerados por IA com voz clonada de entrevistas públicas, fotos editadas com a vítima incluída em cenários (jato particular, Tesla), todas geradas com modelos generativos.

O salto técnico, FaceTime deepfake: quando a vítima exigiu videochamada para confirmar identidade, os criminosos usaram pipeline em tempo real (DeepFaceLive ou similar) sobre um operador humano que mimetizava gestos do Elon Musk. A vítima viu o "Elon" em vídeo ao vivo, com voz clonada e movimentos sincronizados. Por se tratar de chamada de 3-5 minutos, com luz controlada, foi suficiente para superar a desconfiança.

O gatilho financeiro: história de "fundo de investimento exclusivo bloqueado por questão regulatória, preciso de US$ 10 mil para liberar; te devolvo com 200% de lucro". Após o primeiro pagamento, sucessivas "novas exigências regulatórias" levaram a vítima a transferir US$ 60 mil em 4 meses.

Lavagem: transferências cripto (BTC e USDT) para wallets que foram fragmentadas em mixer services antes de cash-out em exchanges fora dos EUA.

Defesas que teriam impedido: (1) *reversão de imagem* (images.google.com) da foto do perfil, quase sempre revela origem real da imagem; (2) *regra absoluta*: celebridades NUNCA fazem aproximação romântica por DM em rede social; (3) *peer review familiar*, contar o relacionamento para um filho ou amigo próximo nas primeiras semanas frequentemente detecta o padrão antes do dano; (4) *nenhum amor verdadeiro pede transferência financeira antes de encontro presencial*; (5) *desconfiar de deepfake* em chamadas curtas com enquadramento fixo, luz controlada e poucos gestos amplos.

Por que isso interessa à sua família: o golpe não pega pessoas "burras". Pega pessoas **isoladas emocionalmente**. Manter sua tia viúva, seu pai divorciado ou sua amiga em luto em conexão real com a família é defesa concreta, não conselho genérico.

4.3 Stalkerware: o espião dentro de casa

Apps como mSpy, Cerberus, FlexiSpy e Hoverwatch são vendidos como "controle parental", mas são frequentemente usados em contextos de **violência doméstica** para monitorar parceiras: leem mensagens, ouvem ligações, rastreiam GPS, registram tudo que é digitado.

■ ATENÇÃO — Sinais de stalkerware no celular

1. Bateria que dura significativamente menos sem motivo (o app fica enviando dados o tempo todo).

2. Consumo de dados móveis muito acima do normal.

3. Aparelho quente mesmo em standby.

4. App estranho no menu de Acessibilidade (Android) ou perfil MDM não reconhecido (iPhone, em Ajustes → Geral → VPN e gerenciamento de dispositivos).

5. Parceiro/ex-parceiro sabe coisas que você nunca contou.

O que fazer: a Coalition Against Stalkerware (que reúne Kaspersky, ESET, Avast, Norton) recomenda **não desinstalar imediatamente** • isso alerta o agressor. Procure orientação no Disque 180 e em um centro de violência contra a mulher antes de agir.

4.4 Configurações de privacidade essenciais

Em vez de teoria, vamos ao prático. Reserve **15 minutos por rede social** e siga este checklist para toda a família. Faça com filhos e idosos junto:

Instagram

• Conta privada ativa (Configurações → Privacidade → Conta privada).
• Mensagens de não seguidores: desativar.
• Lista de seguidores: oculta para outras pessoas.
• Atividade: desativar status online.
• Marcações em fotos: revisar antes de aparecer no seu perfil.
, 2FA via app autenticador.

Facebook

• "Quem pode ver suas publicações futuras": Amigos.
• "Quem pode te enviar solicitações de amizade": Amigos de amigos.
• "Visualizar como": rode mensalmente para auditar perfil público.
• Aplicativos conectados: remover tudo que você não usa há 6+ meses.
• Reconhecimento facial: desativar.

WhatsApp

• Foto de perfil, "Visto por último", "Info" e Status: "Meus contatos".
• Grupos: "Meus contatos" (impede adição em grupos de golpe).
• Confirmação em duas etapas: ATIVA com PIN forte.
• Dispositivos conectados: revisar mensalmente.

TikTok

• Conta privada (obrigatória por padrão para menores de 16 no Brasil em 2026).
• "Sugerir sua conta a outros": desativar.
• Mensagens diretas: somente quem você segue.
• Duetos/Stitch: somente seguidores ou desabilitado.

Google (em myaccount.google.com)

• Verificação em duas etapas: ATIVA (com app autenticador ou chave física).
• Apps de terceiros com acesso: remover tudo que você não usa.
• Histórico de localização: revisar e desativar se não usar.
• Dispositivos conectados: deslogar de tudo que não é seu.

✓ DICA RÁPIDA — A regra dos 30 dias

Toda família deve reservar **uma noite a cada 30 dias** para revisar privacidade junta. Filhos ajudam os pais, pais ajudam os avós, todo mundo revisa o próprio.

É menos chato do que parece e gera conversas valiosas sobre o que cada um faz online. Bons golpes morrem em famílias que conversam.

CAPÍTULO 05

Protegendo crianças e adolescentes online

O capítulo mais importante deste livro

Atenção: este capítulo aborda temas sensíveis como abuso, sextortion e ideação suicida. Se você está lendo com a presença ou possibilidade de leitura por um adolescente em situação de fragilidade, considere fazer essa leitura primeiro sozinho e mediar a conversa em seguida.

54%	72%	19 seg
ADOLESCENTES VÍTIMAS DE VIOLÊNCIA SEXUAL ONLINE ChildFund Brasil 2025	DAS DENÚNCIAS SAFERNET 2025 foram sobre abuso infantil	TEMPO MÍNIMO DE ALICIAMENTO WeProtect / DHS 2025

Em 2025, a SaferNet recebeu **87.689 denúncias** de crimes cibernéticos • quase três quartos delas relacionadas a abuso e exploração sexual infantil. O Mapeamento dos Fatores de Vulnerabilidade de Adolescentes na Internet (ChildFund Brasil, 2025) revelou que **mais da metade** dos adolescentes brasileiros já sofreu alguma forma de violência sexual online.

A resposta legal brasileira foi a **Lei 15.211/2025**, conhecida como **ECA Digital** (ou "Lei Felca"), sancionada em 17 de setembro de 2025 e em vigor desde 17 de março de 2026. Trataremos dela em detalhe na seção 5.5.

5.1 Cyberbullying

Dados da TIC Kids Online Brasil 2025 (Cetic.br/NIC.br): **92%** dos jovens brasileiros de 9 a 17 anos usam Internet (24,5 milhões); **66%** têm perfil em rede social; **mais de um terço** dos jovens de 16 a 24 anos relatam já ter sofrido cyberbullying. Apenas **8% dos pais** percebem a violência que **29% dos jovens** relatam viver, a invisibilidade é parte do problema.

A **Lei 14.811/2024** tornou bullying e cyberbullying crimes específicos (pena de 2 a 4 anos no caso digital), e classificou indução ao suicídio online como crime hediondo.

■ ATENÇÃO — Sinais de que seu filho está sendo vítima de cyberbullying

Mudanças bruscas no humor após usar o celular.

Evita ir à escola; cai no rendimento; perde apetite ou sono.

Para de falar sobre amigos que antes mencionava.

Pede para mudar de escola, de turma ou de número.

Apaga contas de redes sociais sem explicação.

Reage de forma desproporcional quando você pede o celular.

Ação: não confronte de cara. Crie ambiente seguro: "reparei que algo mudou; quando quiser conversar, estou aqui e não vou te julgar". Se confirmar: prints de tudo (provas), denuncie na escola e na plataforma, e nos casos graves registre BO e denuncie em denuncie.org.br/safernet.

5.2 Grooming online (aliciamento)

Grooming é o processo pelo qual um adulto se aproxima de uma criança para criar laço de confiança com objetivo de abuso. No mundo digital, pode acontecer em **jogos online** (Roblox, Fortnite, Minecraft, Free Fire) e em **plataformas de chat** (Discord, Snapchat).

O padrão observado pelas polícias:

1. Aproximação no jogo: aliciador finge ser criança ou adolescente; oferece Robux/V-Bucks/skins como isca digital ("eu te mando se você adicionar lá no Discord").
2. Migração de plataforma: leva a criança do jogo (com moderação) para Discord/Snapchat/WhatsApp (sem moderação).
3. Isolamento: pede "segredo entre nós"; faz a criança sentir-se especial; cria conflito com pais ("eles não vão entender").
4. Sexualização gradual: conversas inocentes evoluem para perguntas íntimas; pedido de foto "comum"; depois íntima.
5. Chantagem (sextortion): uma vez obtida a primeira foto, ameaça expor para forçar mais material ou encontro presencial.

> ■ **PERIGO — A pesquisa que assustou pesquisadores em 2025**
>
> Segundo a WeProtect Global Alliance e o US Department of Homeland Security (Online Enticement Informational Bulletin, janeiro/2025), forças policiais documentaram períodos de aliciamento tão curtos quanto **19 segundos**. Não dias. Não horas. Dezenove *segundos* entre o primeiro contato e a primeira tentativa de obter material íntimo.
>
> A velocidade do crime exige velocidade da conversa familiar.

5.3 Sextortion juvenil

A SaferNet relata **576 atendimentos** em 2025 sobre exposição de imagens íntimas, alta de 39% sobre 2024, o tema mais frequente no Helpline. O número real é muito maior: a vergonha é a principal barreira de denúncia.

A consequência mais grave é que a sextortion está documentada como um dos principais gatilhos de suicídio adolescente. Estudo Corassa *et al.* (PLOS One, 2025) confirma a tendência ascendente; o Instituto Vita Alere reporta cerca de 3,5 crianças e adolescentes tirando a própria vida por dia no Brasil. A taxa de suicídio na faixa 10–19 anos cresceu mais de 50 vezes entre 2000 e 2022, segundo depoimento na Câmara dos Deputados.

✓ DICA RÁPIDA — A "Regra do Não Brigo": a conversa que pode salvar uma vida

Antes que aconteça qualquer coisa, faça essa conversa explícita com seu filho ou filha adolescente, verbalmente, olhando nos olhos:

"Filho, eu quero que você saiba uma coisa. Se um dia alguém na Internet tiver uma foto sua que você não queria ter mandado, ou estiver te ameaçando por causa disso, você pode vir falar comigo. Eu não vou brigar. Não importa o que aconteceu, o que você fez, que horas é. Vem falar comigo. O problema é do criminoso, não seu. A vergonha que ele quer te impor é arma dele, e eu vou te ajudar a desarmar."

Repita essa frase mais de uma vez. Em momentos calmos. Sem associar a nenhum evento. É um seguro emocional que muitas famílias só descobriram que precisavam tarde demais.

■ CHECKLIST — O que fazer ao descobrir um caso de sextortion contra seu filho

1. NÃO pague. Pagar nunca encerra. Quase sempre aumenta a chantagem.

2. NÃO apague nada. Tudo é prova: prints, mensagens, perfil do criminoso.

3. Bloqueie o criminoso imediatamente em todas as plataformas. Considere desativar a conta da vítima temporariamente.

4. Reporte na plataforma (Instagram, Discord, etc. têm processos expressos para material íntimo de menores).

5. Denuncie: SaferNet (denuncie.org.br/safernet), Disque 100, e Boletim de Ocorrência na Delegacia de Repressão a Crimes Cibernéticos do seu estado.

6. Acolha: SaferNet Helpline gratuito em new.safernet.org.br/helpline. Considere acompanhamento psicológico imediato. O CVV (188) atende 24h.

7. Não exponha a vítima a postagens públicas em redes sociais sobre o ocorrido. Reduza ainda mais a circulação.

5.4 Predadores em jogos online

O Roblox tem cerca de 144 milhões de usuários ativos diários (Q4/2025). A maioria com menos de 13 anos. Em 2025, a Procuradoria-Geral da Louisiana (EUA) entrou com ação judicial contra a empresa por exposição sistêmica de crianças a predadores; Los Angeles fez o mesmo em fevereiro de 2026. Existem inquéritos abertos na Polícia Judiciária de Portugal e processos na Justiça brasileira.

■ CHECKLIST — Regras de uso de jogos online em família

1. Para crianças menores de 13: chat em jogos online **desabilitado** ou apenas com amigos pré-aprovados pelos pais.

2. Discord só com supervisão para menores de 16; servidores apenas privados, de amigos da escola, nunca servidores públicos.

3. Console/PC com jogos online **na sala**, não no quarto. Princípio antigo, eficácia comprovada.

4. Combine: "se alguém pede para você ir para outro app, mandar foto, ou guardar segredo, você me conta na hora, e a gente não briga". É a Regra do Não Brigo aplicada a jogos.

5. Aprenda o que seus filhos jogam. Não para impedir, para conversar. Crie um Roblox seu, jogue 30 minutos. Você vai entender os riscos e ganhar credibilidade quando precisar conversar.

5.5 ECA Digital: Lei 15.211/2025

A Lei 15.211, sancionada em 17 de setembro de 2025 e em vigor desde 17 de março de 2026, é a **primeira legislação das Américas** sobre proteção integral de crianças e adolescentes em ambiente digital. Foi popularmente chamada de "Lei Felca" em referência ao influenciador que mobilizou a opinião pública em agosto de 2025 com o vídeo "Adultização".

O que a lei garante à sua família:

1. Verificação de idade real: plataformas devem verificar a idade do usuário (gov.br, estimativa por IA, documento), fim da autodeclaração "tenho +18".
2. Vinculação a responsável: conta de menor de 16 anos deve estar vinculada à conta de um responsável.
3. Controle parental nativo: plataformas devem oferecer gratuitamente, em destaque, ferramenta de controle parental.
4. Remoção em 24 horas: conteúdo violador deve ser removido em até 24 horas após denúncia de vítima, responsável, MP ou entidade, sem necessidade de ordem judicial.
5. Proibição de publicidade comportamental para menores: nada de anúncios baseados em rastreamento de comportamento.
6. "Influenciadores mirins": exigência de autorização judicial prévia dos responsáveis para monetização de conteúdo com crianças.
7. Fiscalização ANPD: multas até 10% do faturamento ou R$ 50 milhões por infração.
8. Aplica-se a empresas estrangeiras com filial no Brasil, com responsabilidade solidária.

> **■ SAIBA MAIS — Como exercer seus direitos sob o ECA Digital**
>
> **Conteúdo nocivo contra seu filho:** denuncie na plataforma (Instagram, TikTok, YouTube, Roblox têm canal específico para menores). Tem que ser removido em 24h.
>
> Se a plataforma não remover em 24h: registre denúncia na ANPD (`gov.br/anpd` → Peticionamento) e na SaferNet (`denuncie.org.br/safernet`).
>
> Para conteúdo de abuso sexual: denúncia **imediata** à Polícia Federal (denúncia anônima funciona).
>
> Para "influenciador mirim" sem autorização: denuncie ao Ministério Público da Infância e Juventude do seu estado.

5.6 Ferramentas de controle parental que funcionam

Controle parental **não substitui diálogo**, mas é uma camada essencial, especialmente para crianças menores de 13 anos. A maioria das pessoas não usa essas ferramentas simplesmente porque ninguém mostrou como instalar. Abaixo, o passo a passo de cada uma delas.

1. Google Family Link, Android (gratuito)

O que faz: controla tempo de tela, aprova ou bloqueia cada app que a criança quer instalar, define horários (ex: bloqueio total após 21h), mostra localização do celular dela e gera relatórios semanais de uso.

■ CHECKLIST — Como instalar o Google Family Link, passo a passo

1. No **seu celular (Android ou iPhone)**, baixe o app **"Google Family Link"** na loja oficial (Play Store ou App Store).

2. Abra o app e toque em "Começar". Faça login com sua conta Google (a mesma do seu Gmail).

3. Selecione "Pai ou responsável" e depois "Adicionar uma criança". Se a criança ainda não tem conta Google, o app cria uma para ela. Se já tem, pede o e-mail e senha dela.

4. O app gera um código de 9 letras. Vá ao **celular da criança**, baixe o "Family Link" também (versão "filho"), abra e digite o código.

5. Aceite as permissões pedidas no celular da criança (localização, gerenciamento de apps, tempo de tela). Sem essas permissões, o controle não funciona.

6. No seu celular, configure os limites: tempo de tela diário (ex: 2 horas em dias úteis, 4 no fim de semana), horário de "soneca" (ex: 21h às 7h, celular trava sozinho), classificação etária de apps e jogos (Play Store filtra automaticamente).

Dica: ative "Aprovar instalação de apps". Toda vez que a criança tentar instalar algo, você recebe notificação para aprovar ou negar pelo seu celular.

2. Tempo de Uso + Compartilhamento Familiar, iPhone e iPad (gratuito)

O que faz: nativo da Apple, sem precisar baixar nada. Limite de tempo por app (ex: máximo 30 min de TikTok por dia), bloqueio de compras na App Store, restrição de conteúdo adulto, "Tempo Longe da Tela" para horário de dormir e dever de casa, e localização integrada via "Buscar".

■ CHECKLIST — Como configurar Tempo de Uso, passo a passo

1. No **seu iPhone**, vá em **Ajustes** → **"Família"** (ou "Compartilhamento Familiar" em iOS mais antigo).

2. Toque em "Adicionar Membro" → "Criar Conta para Criança". Insira nome, idade e crie um Apple ID para a criança (ou use o existente).

3. Aceite os termos de "Pedir Para Comprar". Toda compra da criança na App Store agora exige sua autorização.

4. Ainda em "Família", toque no nome da criança → "Tempo de Uso". Ative "Tempo de Uso" e defina:

— **Tempo Longe da Tela:** horário em que o celular fica praticamente bloqueado (ex: 21h às 7h).

— **Limites de Apps:** defina tempos máximos por categoria (Redes Sociais: 1h; Jogos: 30min; etc).

— **Restrições de Conteúdo:** bloqueia sites adultos, conteúdo explícito em música, filmes adultos.

5. Defina uma **senha de Tempo de Uso** de 4 dígitos só sua, diferente da senha do iPhone. Sem ela, a criança pode desativar tudo.

Dica: ative "Compartilhar Localização" no Compartilhamento Familiar. Você vê onde a criança está em tempo real via app "Buscar", sem instalar nada extra.

3. Microsoft Family Safety, Windows e Xbox (gratuito)

O que faz: controla horários de uso do PC, lista sites visitados, bloqueia sites e jogos por idade, mostra tempo gasto em cada aplicativo. Funciona também no Xbox da criança.

■ CHECKLIST — Como configurar Microsoft Family Safety, passo a passo

1. Acesse **family.microsoft.com** no navegador (ou baixe o app "Family Safety" no celular).

2. Faça login com sua conta Microsoft (do Outlook, Hotmail, ou Windows). Clique em "Criar Grupo Familiar" → "Adicionar membro" → "Criança".

3. Cria-se uma conta Microsoft para a criança (ou usa a existente). Ela vai logar no Windows do PC dela com essa conta.

4. No painel da família, ative os controles:

— **Tempo de tela:** defina horários permitidos por dia (ex: 1h por dia em dias úteis, 3h no fim de semana).

— **Filtro de conteúdo:** bloqueia sites adultos, força "Pesquisa Segura" no Bing e Google, exige sua aprovação para instalar novos apps.

— **Atividade:** relatório semanal por e-mail mostrando o que a criança visitou, jogou e instalou.

5. No PC da criança, faça login com a conta dela. O controle entra em vigor automaticamente.

Dica: se a criança usa Xbox, ela já entra com a mesma conta Microsoft. Os controles de jogo (limite de idade, tempo) são aplicados automaticamente lá.

4. Qustodio, multiplataforma (pago)

O que faz: o mais completo do mercado para quem tem família com dispositivos mistos (Android + iPhone + PC + Mac). Monitora mensagens, ligações, redes sociais, tempo por app, e localização. Custa cerca de US$ 50 a US$ 100 por ano (de 5 a 10 dispositivos).

■ CHECKLIST — Como configurar Qustodio, passo a passo

1. Acesse **qustodio.com** e crie a conta gratuita (funciona para 1 dispositivo, depois é paga).

2. Baixe o app no **seu** celular (o "Qustodio Parental Control").

3. No celular ou PC da criança, baixe o app "Qustodio Kids". Ele pede permissões intensas (acessibilidade, administrador de dispositivo). Sem elas, o monitoramento não funciona, é a natureza do produto.

4. Vincule o dispositivo da criança à sua conta usando o código gerado.

5. No painel do Qustodio (no app ou no site), você define:

— Categorias bloqueadas (pornografia, jogos de azar, drogas, violência).

— Tempo de tela total e por app.

— Localização em tempo real e histórico (últimos 7 dias).

— "SOS Pânico": botão no celular da criança que envia alerta para você com localização exata.

Atenção: Qustodio é mais invasivo que os outros. Use só com transparência, conte para a criança que está monitorando e por quê. Espionar escondido vira controle abusivo, não proteção.

5. NextDNS e Cloudflare 1.1.1.1 for Families, filtro de rede (gratuitos)

O que faz: a defesa mais subestimada e ao mesmo tempo mais eficaz. Configura uma vez no roteador da sua casa, e **todos** os dispositivos conectados ao Wi-Fi ganham bloqueio automático de sites adultos, malware, golpes e rastreadores. Funciona em qualquer aparelho: celular, TV, console, tablet do vovô.

■ CHECKLIST — Como configurar Cloudflare 1.1.1.1 for Families (mais simples), passo a passo

1. Acesse o roteador Wi-Fi da sua casa pelo navegador. Geralmente é **192.168.0.1** ou **192.168.1.1** (digite no navegador). Login e senha estão em uma etiqueta atrás do roteador.

2. Procure a opção "DNS" (geralmente em "Configurações Avançadas" ou "Internet" ou "WAN").

3. Troque o DNS automático para **manual** e digite:

— **DNS Primário:** 1.1.1.3

— **DNS Secundário:** 1.0.0.3

(Esses endereços bloqueiam malware E conteúdo adulto. Para bloquear só malware, use 1.1.1.2 e 1.0.0.2.)

4. Salve e reinicie o roteador. Pronto, sua casa inteira agora filtra automaticamente.

Para Android e iPhone, sem mexer no roteador: baixe o app oficial "1.1.1.1: Faster Internet" da Cloudflare na loja do seu sistema, ative "1.1.1.1 for Families" dentro dele e pronto, o filtro vale só para esse celular, onde quer que esteja.

NextDNS (mais avançado): em **nextdns.io**, crie conta gratuita (300 mil consultas por mês), configure categorias específicas (TikTok depois das 22h? Roblox bloqueado no horário escolar?), e copie os DNS gerados para o seu roteador ou celular. Mais customizável, mas exige um pouco mais de cuidado.

■ SAIBA MAIS — O que vem aí: Projeto Shield (lançamento previsto para setembro de 2026)

As ferramentas acima são, hoje, o estado da arte do controle parental disponível no Brasil. Mas todas têm uma limitação comum: foram desenhadas fora do país, sem considerar o cenário específico das famílias brasileiras.

É por isso que **Wanderley J. Abreu Jr. e Felipe Neto** estão se unindo para construir o **Projeto Shield**: um ecossistema de segurança pensado de raiz para a família brasileira, com previsão de lançamento em setembro de 2026.

Esta edição do livro precede esse lançamento. Mais informações serão disponibilizadas na versão dinâmica em **stormnexus.com.br/familia**. Por enquanto, fique com as cinco ferramentas acima e saiba que há algo a caminho, feito por brasileiros, para brasileiros.

CAPÍTULO 06

Protegendo os idosos da família

Por que eles são alvos e como conversar sem ofender

82% dos idosos paulistas já sofreram tentativa de golpe digital (pesquisa Seade TIC, 2025). **68% acreditam ser "praticamente impossível" se proteger**. O Disque 100 registrou mais de 72 mil casos de violência contra idosos em 2024. Em São Paulo, denúncias de golpes financeiros contra idosos no Grande ABC cresceram **108% em três anos**.

6.1 Por que idosos são alvo preferencial

Existem **fatores estruturais** que tornam idosos especialmente vulneráveis a golpes digitais, e nenhum deles é "burrice", como erroneamente se diz:

- **Cultura de respeito à autoridade.** Idosos cresceram em sociedade hierárquica. Quando alguém diz "sou da polícia/gerente/médico", há predisposição cultural a obedecer.
- **Solidão.** Ligações longas e atenção dedicada de "um gerente" preenchem lacuna emocional que pode ser exatamente o que falta no dia.
- **Medo de errar no aparelho.** Hesitam em pedir ajuda para não "atrapalhar" os filhos. Tentam resolver sozinhos seguindo instruções de estranhos.
- **Vulnerabilidade financeira.** Aposentadoria é um ativo conhecido, fixo, mensal, exatamente o que golpistas procuram.
- **Menor familiaridade com sinais de fraude.** Não cresceram lendo "ATENÇÃO: GOLPE". Para muitos, o medo de parecerem desconfiados é maior do que o medo de serem enganados.

ATENÇÃO — O ponto cego dos próprios filhos

Pesquisa do Diário do Grande ABC (novembro/2025) revela um dado desconfortável: **57,5% das violências patrimoniais contra idosos no Grande ABC em 2025 foram cometidas pelos próprios filhos**. Empréstimos consignados sem consentimento, transferências "para resolver depois", apropriação indevida.

Este livro é sobre golpes externos, mas vale o alerta: cuidar do idoso da família passa também por garantir que **nenhum familiar** tenha acesso unilateral ao dinheiro dele sem transparência. Considere conta-conjunta com co-titularidade, ou procuração específica registrada em cartório.

6.2 Os 7 golpes mais comuns contra idosos no Brasil

#	Golpe	Como funciona
1	Falso parente em apuros	WhatsApp "filho/neto" pedindo Pix urgente por boleto/aluguel/problema. Pode usar voz clonada por IA.
2	Falsa central do banco	Ligação se passando por gerente, induzindo "transferência de segurança" para conta do próprio criminoso. Dura até 4 horas.
3	Empréstimo consignado fraudulento	Ligação oferecendo "revisão de aposentadoria" para baixar app. O app pega senha do INSS e contrata consignado em nome do idoso. 57.824 queixas no Procon em 2024.
4	Falso médico/hospital	"Seu filho deu entrada na UTI, pague R$ 5.000 de caução agora". Variante: falso seguro saúde "para liberar internação".
5	Falso advogado/herança	"Sua família recebeu herança no exterior. Pague taxa de R$ 2.000 para liberar". Pode envolver "advogado" que cobra honorário antecipado.
6	Falso recadastramento do INSS	"Prova de vida foi suspensa, baixe esse app para recadastrar". O app é trojan. O INSS faz prova de vida automaticamente ou na agência.
7	Falso motoboy de cartão	"Seu cartão foi clonado, vamos enviar motoboy para destruir". O motoboy busca o cartão real para uso.

6.3 Método 5 etapas para conversar com idosos sobre tecnologia

A conversa errada destrói confiança e empurra o idoso a esconder erros • o que é exatamente o que o golpista quer. Siga este método testado:

1. **NÃO RIDICULARIZE.** Jamais diga "como você caiu nisso, pai?". A vergonha é o principal aliado do criminoso (Diário do Grande ABC). Em vez disso: "Pai, isso aconteceu com muita gente. Você não é o primeiro nem o último. Vamos ver juntos o que fazer agora?"

2. **COMBINE PALAVRA-CÓDIGO FAMILIAR.** Em uma reunião de família, pessoal, jamais por WhatsApp, combinem uma palavra ou frase única para emergências. "Se alguém te ligar pedindo Pix, mesmo com a minha voz, pergunte a palavra. Se a pessoa não souber, é golpe."

3. **CONFIGURE LIMITES BAIXOS.** No app do banco, configure limites de Pix baixos (R$ 200/dia, R$ 50 em horário noturno). Para Pix acima do limite, exige liberação manual. Isso compra tempo precioso.

4. **CADASTRE UM "CONTATO DE CONFIANÇA".** Alguns bancos (Bradesco, Caixa, Itaú) já permitem que um familiar seja cadastrado como contato de emergência, para receber alertas de transações incomuns. Pergunte ao gerente do seu pai/mãe.

5. **REUNIÃO MENSAL DE "ATUALIZAÇÃO DE GOLPES".** Toda primeira sexta do mês, almoço/jantar em família, e revisem juntos os 2-3 golpes que estão circulando. Isso vacina cognitivamente e cria espaço para o idoso contar coisas que talvez não conte de outra forma.

6.4 Kit prático para configurar o celular de um idoso

■ CHECKLIST — Checklist de blindagem do celular do idoso

1. PIN no chip (SIM): 4 dígitos exigidos a cada reinicialização. Em Android: Ajustes → Segurança → Configurar bloqueio do SIM. No iPhone: Ajustes → Celular → PIN do SIM.

2. WhatsApp com 2FA: Configurações → Conta → Confirmação em duas etapas. Anote o PIN no gerenciador de senhas da família.

3. Foto do WhatsApp para "Meus contatos". Idem para Stories.

4. Limite de Pix baixo: R$ 200-500/dia configurado no app do banco.

5. Notificações de transação: ativar SMS e push do banco para qualquer transação, ainda que pequena.

6. App do banco oficial, não site mobile.

7. App "antigolpes" gratuito (PSafe Quantum, NextDNS, Truecaller) para bloquear ligações de golpe.

8. Lista impressa com telefones de emergência colada perto do aparelho: filhos, banco (do verso do cartão), Disque 100, 190.

9. Configure um "contato de confiança" no celular (Ajustes → Saúde no iPhone, "SOS" em Androids) que possa ser acionado por gesto em emergência.

■ ATENÇÃO — O que NUNCA fazer pelo seu pai/mãe

1. Não use o login do idoso "para resolver mais rápido". Isso pode caracterizar apropriação indevida em caso de auditoria do banco, além de remover a oportunidade de ele aprender.

2. Não compartilhe a senha do banco do idoso por WhatsApp, e-mail ou anotação visível. Use gerenciador de senhas com cofre familiar.

3. Não fale do idoso "na frente dele" como se ele não estivesse, isso reforça o sentimento de incapacidade que o golpista explora.

CAPÍTULO 07

Deepfakes e IA generativa: a nova fronteira do golpe

Quando a voz da sua mãe pode ser sintetizada em 15 segundos

Em fevereiro de 2024, um funcionário de uma multinacional em Hong Kong participou de uma videoconferência com seu CFO e três colegas. Ao final da reunião, o CFO autorizou que ele transferisse **US$ 25 milhões** para uma "conta de pagamento de fornecedor". Todos os participantes eram **deepfakes**. O CFO e os colegas estavam ocupados em suas mesas, alheios. Foi a maior fraude por deepfake já documentada.

■ CASO REAL — Anatomia técnica do golpe: Hong Kong, fevereiro de 2024

Reconhecimento (OSINT pré-ataque): os criminosos passaram semanas coletando vídeos públicos do CFO e diretores em entrevistas a canais financeiros, vídeos corporativos no YouTube e LinkedIn, e conferências gravadas. O volume era mais que suficiente: deepfake corporativo de alta qualidade exige entre 5 e 15 minutos de imagem frontal e áudio limpo por pessoa.

Treinamento dos modelos: 4 deepfakes simultâneos foram preparados, um por executivo, em pipeline de Generative Adversarial Networks (GANs) combinadas a modelos de voz neural (TTS com condicionamento por embedding de locutor). Custo estimado de produção: entre US$ 5 mil e US$ 15 mil em GPUs de aluguel.

Vetor inicial: o funcionário recebeu e-mail do "CFO" (spear phishing) marcando reunião emergencial. O e-mail veio de domínio recém-registrado, visualmente idêntico ao corporativo (typosquatting com caractere Unicode no lugar de "l" minúsculo).

Execução em tempo real: a videoconferência usou plataforma corporativa legítima, mas com os "participantes" sendo deepfakes gerados em tempo real por meio de software como DeepFaceLive ou derivados. Os movimentos eram limitados (rosto frontal, sem virar a cabeça em ângulos extremos, limitação técnica dos modelos da época).

Pressão social: os "executivos" pediram urgência, confidencialidade ("não comente com ninguém antes da divulgação pública"), e aprovaram a transação verbalmente. O funcionário, desconfiado a princípio, validou-se vendo "o próprio rosto do CFO" e seguiu o protocolo de aprovação por hierarquia.

Lavagem instantânea: os US$ 25 milhões foram fragmentados em mais de uma dezena de transferências para contas em diferentes jurisdições asiáticas em questão de minutos.

Defesas que teriam impedido: (1) *verificação por canal alternativo obrigatória* para qualquer transação acima de limiar corporativo definido, chamada de voz direta ao CFO no celular pessoal conhecido; (2) *palavra-código corporativa* pré-combinada para transações sensíveis (mesmo conceito da palavra-código familiar, aplicada ao C-level); (3) *protocolo de duas pessoas* (Two-Person Integrity), nenhuma transação acima de US$ 1 milhão sem co-aprovação humana via canal independente; (4) *treinamento em deepfake awareness* para colaboradores com poder de assinatura.

Por que isso interessa à sua família: a mesma mecânica é usada hoje em escala muito menor para clonar a voz de um filho pedindo Pix de R$ 2.000. A diferença é só o orçamento do criminoso.

Pode parecer Hong Kong, mas em 2025 o Brasil registrou crescimento de **830%** em golpes com deepfake (BioCatch). A voz do seu filho, da sua mãe ou do seu chefe pode ser clonada com qualquer áudio público de 15 segundos. E você precisa estar preparado.

7.1 Clonagem de voz: a nova ferramenta favorita do golpista

15 seg
DE ÁUDIO BASTAM PARA CLONAR
ElevenLabs, Respeecher 2025

+680%
EM DEEPFAKE DE VOZ NO MUNDO
Pindrop Report 2025 (vs 2024)

US$ 897 mi
PERDAS GLOBAIS ACUMULADAS
Surfshark, desde 2019

Plataformas como ElevenLabs, Speechify, Respeecher e até o próprio OpenAI Voice oferecem clonagem de voz com qualidade quase humana. Os criminosos coletam áudios das vítimas em **Stories do Instagram** (narração de vídeo), **mensagens de voz no WhatsApp** (vazadas em celular roubado, ou enviadas para conhecidos infectados), **entrevistas no YouTube**, podcasts, qualquer coisa.

■ PERIGO — O "golpe da ligação muda"

Em 2025, a Polícia Civil de São Paulo emitiu alerta sobre um golpe novo: o criminoso liga, fica em silêncio, e espera apenas o seu "alô".

Três segundos de "alô" já bastam para clonar sua voz e, em seguida, usar essa voz para ligar para parentes seus pedindo Pix urgente.

Defesa: se atender e o interlocutor não falar em 2 segundos, desligue. Não diga "alô?" várias vezes. Não fale "quem é?". Apenas desligue.

7.2 Como reconhecer um deepfake (limitações reais)

Seja honesto: **cada vez é mais difícil reconhecer um deepfake só pela aparência ou pelo som**. As ferramentas estão ficando boas demais. Em 2026, o brasileiro médio não vai conseguir distinguir uma voz clonada profissional de uma voz real em uma chamada curta. Por isso a defesa precisa ser **processo**, não **percepção**.

Pistas que AINDA funcionam (com cuidado):

Em vídeo: movimentos abruptos da cabeça revelam inconsistências (os modelos são treinados em fotos frontais). Peça à pessoa para virar o rosto 90° em uma chamada, deepfakes em tempo real ainda quebram.
Em vídeo: piscar de olhos irregular ou ausente em deepfakes mais antigos.
Em áudio: cadência levemente mecânica; respiração inexistente ou em lugar estranho; pausa estranha antes de responder pergunta inesperada (o modelo precisa "pensar").
Em ambos: contexto que não bate. Por que a pessoa está te ligando agora? Por que do número que não é o dela? Por que com pressa?

> **✓ DICA RÁPIDA — A defesa que funciona contra QUALQUER deepfake**
>
> **Verificação por canal alternativo é a única defesa robusta.**
>
> Se receber uma chamada urgente pedindo Pix, autorização, código, qualquer coisa, **desligue**. Ligue de volta no número que você tem na sua agenda. Se a pessoa atender e confirmar, era real. Se não atender ou estranhar, era golpe.
>
> Demora 30 segundos. Salva R$ 50.000.
>
> **Complemento:** palavra-código familiar combinada antes. Em qualquer chamada com emergência financeira, pergunte a palavra. Quem está do outro lado de verdade saberá; deepfake nunca.

7.3 Imagens íntimas falsas: deepfake sexual não consensual

Talvez o uso mais perverso da IA generativa. Adolescentes têm sido alvo em escolas brasileiras: colegas pegam fotos públicas do Instagram, geram nudes falsas com apps de "remoção de roupa" baseados em IA, distribuem em grupos de WhatsApp. O impacto psicológico é devastador, mesmo sendo "falso".

> **■ SAIBA MAIS — Resposta legal e prática**
>
> **Legal:** a Lei 14.811/2024 e o Código Penal punem a produção e a distribuição de imagens íntimas (verdadeiras ou falsas) sem consentimento. O ECA Digital aumenta penas no caso de menores. A LGPD considera imagem facial dado biométrico sensível.
>
> **Prático:** denuncie na escola (responsabilidade institucional), na plataforma de origem (Discord, Instagram, WhatsApp têm canais), no MP da Infância e Juventude e na Delegacia de Repressão a Crimes Cibernéticos. Guarde prints como prova.
>
> **Emocional:** a vítima precisa entender que **não é dela a culpa, nem mesmo a foto**. É integralmente do agressor. Apoio psicológico é tão essencial quanto a denúncia.

7.4 Defesas familiares contra IA generativa

■ CHECKLIST — Plano antifraude com IA: para toda a família

1. Reduza áudio público. Perfis fechados; pouca narração em Stories; podcasts de membros da família com link só para quem segue.

2. Combine palavra-código com a família estendida. Não só pais e filhos, avós, tios, primos. Quanto mais gente cobre, mais blindado o golpe.

3. Regra das 24 horas. Nenhum Pix urgente baseado em mensagem ou ligação de "emergência" deve ser feito sem ligação de volta para o número conhecido. Se realmente é urgente, é urgente para esperar 1 minuto.

4. Conversa explícita com os adolescentes sobre nudes falsas. Não como "isso pode acontecer", como "isso vai acontecer com alguém da sua escola. Quando acontecer, conte comigo".

5. Para empresários e profissionais com perfil público: considere palavra-código também com sua equipe e seus fornecedores grandes. Hong Kong não foi exceção: é o futuro.

7.5 Casos brasileiros que ilustram o risco

William Bonner, **Drauzio Varella**, **Felipe Neto**, governadores e ministros já tiveram suas imagens e vozes clonadas em 2024-2025 para promover "indenizações do governo", investimentos em cripto fraudulentos e medicamentos milagrosos. Nenhuma das pessoas envolvidas autorizou seu uso. As plataformas (Meta, YouTube) demoraram dias a semanas para remover.

■ ATENÇÃO — A regra geral para qualquer "celebridade" recomendando produto

Se você ver uma "live de William Bonner" recomendando investimento, ou um "vídeo do Drauzio" recomendando remédio milagroso, ou um "áudio do presidente" oferecendo benefício, assuma que é fraude até prova em contrário.

Confirme em **fontes oficiais** (Globo, programa do Drauzio, site do governo). Se for real, está lá também. Se não está, é fake.

CAPÍTULO 08

Segurança básica em casa: Wi-Fi, senhas e 2FA

A infraestrutura invisível que protege sua família

O roteador da sua casa é a porta de entrada para todos os ataques que chegam pela Internet. Suas senhas são as chaves do reino digital. E o 2FA, autenticação de dois fatores, é o cadeado a mais que separa um golpe de uma tragédia.

8.1 Roteador Wi-Fi

Quase ninguém pensa no roteador. Ele é instalado pelo técnico, fica piscando luzinhas no canto da sala, e some da vida da família. Mas um roteador mal configurado é como uma porta da frente sem fechadura.

■ SAIBA MAIS — Como acessar o painel do seu roteador

1. Abra um navegador (Chrome, Safari, Edge) no celular ou computador **conectado ao Wi-Fi de casa**.

2. Na barra de endereço, digite `192.168.0.1` e aperte Enter. Se não abrir nada, tente `192.168.1.1`. Se ainda não funcionar, tente `192.168.15.1` (comum em roteadores brasileiros).

3. Vai aparecer uma tela de login. Os mais comuns são: `admin/admin`, `admin/password`, `admin/(em branco)`. Se não funcionar, olhe a **etiqueta atrás do roteador**, geralmente vem o login e senha de fábrica impressos lá.

4. Pronto, você está dentro do painel. Agora vem a parte importante.

Importante: cada marca de roteador (TP-Link, Intelbras, D-Link, Mercusys, Tenda, ASUS, Huawei, Multilaser, e os modelos das operadoras Vivo, Claro, Oi) tem um painel diferente, com nomes diferentes para as mesmas opções. Mas todos têm essas funções, só muda onde estão escondidas. Use os termos abaixo como guia, procure menus parecidos no seu painel.

■ CHECKLIST — 1. Trocar a senha do painel de administração

Por que: a senha admin/admin é conhecida por todo criminoso. Quem invadir sua rede pode reconfigurar tudo, redirecionar você para sites falsos, espionar tráfego.

Onde procurar no painel: menus chamados "**Administração**", "**Sistema**", "**Gerenciamento**", "**Configurações Avançadas**" ou "**Senha do Roteador**".

O que fazer: procure um campo "Senha atual" e "Nova senha". Coloque uma senha forte de 14+ caracteres (use seu gerenciador de senhas para gerar e guardar). Salve e faça login novamente com a nova senha.

■ CHECKLIST — 2. Ativar criptografia WPA3 (ou WPA2-AES no mínimo)

Por que: WPA3 é o padrão moderno (2018). WPA2 ainda é seguro se usar o modo AES. WEP e WPA antigos podem ser quebrados em segundos por qualquer ferramenta gratuita disponível na Internet.

Onde procurar no painel: menus chamados "**Wireless**", "**Wi-Fi**", "**Rede sem fio**", "**Segurança da rede**" ou "**Modo de segurança**".

O que fazer: procure a opção "**Modo de segurança**" ou "**Encryption**". Selecione "**WPA3-Personal**" se disponível, ou "**WPA2-PSK (AES)**" como segunda opção. Evite "WPA/WPA2 misto", "WPA-PSK (TKIP)" ou qualquer opção com a palavra "WEP". Salve.

Se o seu roteador é antigo demais para ter WPA3, considere trocar: roteadores sem WPA3 geralmente também não recebem mais atualizações de segurança.

■ CHECKLIST — 3. Trocar a senha do Wi-Fi (a que os visitantes pedem)

Por que: a senha de fábrica vem em uma etiqueta atrás do roteador. Qualquer pessoa que já entrou na sua casa (faxineiro, encanador, amigo da escola do seu filho) pode ter anotado e usar de fora.

Onde procurar no painel: mesma seção da criptografia ("Wireless", "Wi-Fi", "Rede sem fio"). Procure "**Senha da rede**", "**Wi-Fi password**", "**Pre-Shared Key**" ou "**WPA Key**".

O que fazer: coloque uma senha de 14+ caracteres aleatórios (use o gerenciador de senhas). Salve. **Atenção:** todos os dispositivos da casa vão perder conexão e você precisa reconectar cada um com a nova senha, celular, TV, console, etc.

■ CHECKLIST — 4. Desativar o WPS

Por que: o WPS (Wi-Fi Protected Setup) é aquele botão que conecta aparelhos sem digitar senha. Ele tem falha de segurança conhecida há mais de uma década. Roubar a senha do Wi-Fi via WPS leva cerca de 10 horas com ferramenta gratuita.

Onde procurar no painel: menus chamados "**WPS**", "**Conexão Wi-Fi simplificada**", "**Configuração rápida**" ou "**QSS**" (em roteadores TP-Link antigos).

O que fazer: procure a chave "**WPS**" ou "Habilitar WPS" e marque **Desativado** ou desmarque a caixa. Salve.

■ CHECKLIST — 5. Atualizar o firmware do roteador

Por que: firmware é o sistema operacional do roteador. Atualizações corrigem falhas de segurança descobertas depois da venda. Roteador sem atualização há 3 anos é um campo aberto.

Onde procurar no painel: menus chamados "**Atualização de firmware**", "**Firmware Upgrade**", "**Sistema → Atualização**" ou "**Manutenção → Firmware**".

O que fazer: a maioria dos painéis modernos tem botão "**Verificar atualizações**" que baixa e instala sozinho. Se não tiver, anote o modelo do roteador (etiqueta atrás), vá ao site oficial da marca, baixe a versão mais recente e suba pelo painel.

Repita a cada 3 meses. Vale o lembrete na agenda.

■ CHECKLIST — 6. Criar rede de visitantes (Guest Network)

Por que: quando você dá senha do Wi-Fi para um amigo, ele entra na mesma rede onde estão suas câmeras, computador com imposto de renda, smart TV. Se o celular dele estiver infectado, sua rede também está. Visitantes precisam de uma rede separada, isolada.

Onde procurar no painel: menus chamados "**Rede de visitantes**", "**Guest Network**", "**Wi-Fi para convidados**" ou "**Rede secundária**".

O que fazer: ative a opção. Dê um nome diferente (ex: "Visitantes-CasaSilva"), defina senha própria (também gerada pelo gerenciador), **ative o isolamento** ("Isolamento de cliente" ou "AP isolation"). Pronto: visitantes acessam só a Internet, sem ver os outros aparelhos da casa.

■ ATENÇÃO — E se eu não conseguir achar essas opções?

Cada marca esconde os menus de jeito diferente. Se você não achar, faça uma busca no Google ou YouTube com o **modelo exato do seu roteador** (anotado na etiqueta atrás) + a opção que você quer mudar. Exemplo: `"TP-Link Archer C20 desativar WPS"` ou `"Intelbras WiFiber 121 AC alterar senha admin"`.

Há vídeo no YouTube para praticamente qualquer modelo vendido no Brasil, em português, mostrando exatamente onde clicar.

E quando tudo mais falhar: peça ajuda de um adolescente da família. Eles geralmente ficam felizes em demonstrar que sabem mais do que você sobre alguma coisa.

8.2 IoT doméstico: a Internet das Ameaças

Câmeras IP, smart TVs, assistentes de voz, geladeiras inteligentes, lâmpadas Wi-Fi: cada dispositivo IoT em sua casa é uma porta extra. Câmeras Wi-Fi baratas de origem desconhecida são particularmente preocupantes, várias famílias brasileiras tiveram imagens internas de suas casas vazadas em fóruns clandestinos.

Regras para qualquer IoT em casa:

1. Troque a senha-padrão. Se o aparelho não permite, devolva.
2. Mantenha firmware atualizado. Se o fabricante não atualiza há mais de 2 anos, considere descartar.
3. Ponha em rede de visitantes (isolada).
4. Aponte câmeras só para áreas comuns. Nunca para quartos ou banheiros.
5. Em smart TV: desative microfone se não usar comando de voz; revise permissões de apps; não use a conta principal do Google/Apple, crie uma dedicada.
6. Em assistentes de voz (Alexa, Google Home): revise gravações mensalmente; desative compras por voz.

8.3 Wi-Fi público e VPN

Wi-Fi de cafeteria, hotel, aeroporto, shopping é território de **ninguém**. Pode estar sob controle de criminoso fazendo **man-in-the-middle**, interceptando tudo que passa.

■ CHECKLIST — Regras de Wi-Fi público

1. Sempre que possível, use **4G/5G** em vez de Wi-Fi grátis. Seu plano de dados é mais seguro que a maioria das redes públicas.

2. Se usar Wi-Fi público, ative **VPN** imediatamente. Recomendadas (pagas, com política no-log auditada): Mullvad, ProtonVPN, NordVPN. Custam menos de R$ 30/mês por toda a família.

3. NUNCA acesse banco em Wi-Fi público sem VPN. Se for emergência, use 4G.

4. Evite VPNs grátis, vivem do que coletam dos usuários. "Se o produto é grátis, o produto é você."

5. VPN **não substitui antivírus** nem protege contra phishing. É camada complementar.

8.4 Senhas e gerenciadores de senha

A senha "Familia2025!" é fraca, vai vazar em algum banco de dados, e todas as outras contas que usam ela também serão comprometidas. A única solução real é usar **senhas únicas, longas e aleatórias por serviço**. Como você não vai decorar 150 senhas únicas, usa um gerenciador.

Gerenciadores recomendados para famílias:

Gerenciador	Tipo	Por que recomendamos
Bitwarden	Gratuito + Premium	Open source, plano gratuito generoso, cofre familiar a US$ 40/ano. Recomendado pelo NIST.
1Password Families	Pago (~R$ 25/mês)	Melhor UX para famílias, cofres compartilhados, monitoramento de vazamentos.
KeePass	Gratuito	Open source, 100% offline. Para quem prefere não confiar em nuvem.
Proton Pass	Gratuito + Premium	Da equipe ProtonMail; suíça; inclui aliases de e-mail e 2FA.

✓ DICA RÁPIDA — Regras de senha em 2026

1. Mínimo 14 caracteres. Geradas aleatoriamente pelo gerenciador.

2. Uma senha única por serviço. Sem exceção.

3. NÃO use o gerenciador do navegador (Chrome, Safari) como única defesa, extensões maliciosas podem roubar.

4. Senha-mestra do gerenciador: longa (20+ caracteres), memorizada, jamais escrita. É a única que você precisa lembrar.

5. Cofre familiar compartilhado: para senhas que **devem** ser acessíveis a múltiplos membros (Netflix, banco conjunto, Wi-Fi da casa).

8.5 Autenticação de dois fatores (2FA)

Senha forte sozinha não basta. Bases vazam, dados são roubados, e às vezes você mesmo cai num phishing bem feito. O 2FA é a segunda camada, uma confirmação independente de que é você mesmo entrando.

Hierarquia de segurança do 2FA (do melhor para o pior):

Tipo	Segurança	Quando usar
Chave física FIDO2 (YubiKey, etc.)	Máxima	E-mail principal, conta Google/Apple, banco. Custa R$ 200-400.
Passkey	Muito alta	Use quando disponível, Apple, Google, Microsoft, alguns bancos.
App autenticador (Google, Authy)	Alta	Para todos os serviços onde 2FA por app está disponível.
Notificação push do app oficial	Alta	Bancos brasileiros oferecem (Itaú, Nubank, Bradesco).
Token físico (calculadora do banco)	Média-alta	Modelo antigo, mas seguro. Banco do Brasil ainda oferece.
E-mail	Média	Aceitável se o e-mail tem 2FA forte. Não use se e-mail é vulnerável.
SMS	BAIXA	**Último recurso.** Vulnerável a SIM swap. Tirar do meio sempre que possível.

8.6 Passkeys: o fim da senha?

Passkey é a tecnologia que está substituindo gradualmente as senhas em 2025-2026. Em vez de digitar senha + 2FA, você usa biometria (Face ID, Touch ID, leitor de impressão digital) do seu próprio dispositivo. A chave privada nunca sai do aparelho, então é **resistente a phishing por design**.

Apple, Google e Microsoft já suportam passkeys nativamente. Em 2026, os principais bancos brasileiros começaram a oferecer (Nubank, Itaú, Bradesco). Quando seu serviço favorito perguntar "deseja usar passkey?", a resposta é sim.

CAPÍTULO 09

Proteção financeira digital: Pix, MED e cartão virtual

Configurações que limitam o prejuízo e as primeiras 24h após um golpe

Quando o golpe acontece, segundos contam. A diferença entre perder R$ 200 e perder R$ 20.000 está nas **configurações que você fez antes** e nas **ações que você faz nos primeiros minutos depois**.

9.1 Pix seguro: configuração obrigatória

■ CHECKLIST — Setup mínimo do Pix em qualquer banco

1. Limites por horário. Configure: R$ 1.000/dia em horário comercial, R$ 200 das 22h às 6h. Para Pix acima do limite, exige liberação manual com 30 minutos de espera (regra do BCB).

2. Limites por destinatário. Para chaves não cadastradas, estabeleça limite de R$ 500/transação.

3. Cadastre na agenda destinatários frequentes (família, aluguel, escola). Sai do "primeiro Pix" e tem limite separado.

4. Ative todas as notificações push e SMS de qualquer Pix, mesmo de pequeno valor.

5. Ative o botão de contestação MED no app (obrigatório em todos os bancos desde 1º de outubro de 2025).

6. Para idosos: limites ainda menores (R$ 200/dia padrão).

9.2 MED 2.0: Mecanismo Especial de Devolução

A **Resolução BCB 493**, em vigor desde 2 de fevereiro de 2026, criou o MED 2.0, versão expandida do mecanismo que permite tentar recuperar dinheiro perdido em golpe via Pix. As principais melhorias:

1. Prazo de **80 dias corridos** para abrir contestação (antes era 7 dias).
2. Banco recebedor tem **11 dias** para análise robusta (antes era 7 dias).
3. Monitoramento de saldo por **90 dias** após contestação.
4. Rastreio do "caminho do dinheiro" em até **5 transferências sucessivas** (o golpista costuma "lavar" o Pix em cadeias rápidas).
5. Botão de contestação no app disponível desde 1º de outubro de 2025 em todos os bancos.

■ SAIBA MAIS — O que o MED cobre e o que NÃO cobre

COBRE: Pix feito sob coação, engano (falsa central, WhatsApp clonado), invasão de conta, ou falha operacional do banco.

NÃO COBRE: Pix por erro de digitação de chave (você errou a chave); desacordo comercial (comprou algo e o produto não veio como esperado, isso é Procon, não MED); Pix consciente a terceiro que de boa-fé recebeu sem saber da origem fraudulenta.

IMPORTANTE: abra a contestação MED nas primeiras 24-48 horas. Quanto mais cedo, maior a chance de recuperar, o dinheiro pode estar bloqueado em alguma das 5 contas seguintes.

9.3 Cartões virtuais e cartões pré-pagos

Para compras online em sites desconhecidos, **cartão de crédito virtual** é o seu melhor amigo. Bancos brasileiros oferecem geração de cartões virtuais com:

• Validade curta (24 horas a 30 dias);
• Valor pré-definido (só dá para gastar até o limite que você definiu);
• Possibilidade de descartar a qualquer momento.

Se o site vazar seus dados ou cobrar valor diferente, o prejuízo está contido. Bancos como Nubank, Itaú, Bradesco, C6 e Inter oferecem gratuitamente.

9.4 As primeiras 24 horas após um golpe

Caiu em golpe. Respire fundo. As próximas 24 horas vão definir o tamanho do prejuízo. Faça **nesta ordem exata**:

[1] PRIMEIRA HORA, BANCO
Ligue para o canal de fraude do seu banco (geralmente no verso do cartão). Acione bloqueio cautelar BCB (até 72h). Abra contestação MED no app.

[2] PRIMEIRA HORA, BO ONLINE
Registre Boletim de Ocorrência no site da Delegacia Virtual do seu estado. SP: `delegaciaeletronica.policiacivil.sp.gov.br`. RJ: `delegaciavirtual.policiacivil.rj.gov.br`.

[3] PRIMEIRAS 6H, TROCAR SENHAS
Comece pelo e-mail principal (que controla todas as outras). Depois: banco, WhatsApp, Instagram, Facebook, e-commerce. Tudo via gerenciador, todas novas e únicas.

[4] PRIMEIRAS 12H, AVISAR CONTATOS
Mande mensagem para os contatos mais próximos: "Caí em golpe X. Meu WhatsApp pode estar sendo usado por golpista. Não façam Pix nem cliquem em links que eu pareça mandar até nova confirmação."

[5] PRIMEIRAS 24H, BLOQUEAR CRÉDITO
Acesse o **Registrato BCB** (`registrato.bcb.gov.br`) e veja se há contas/Pix abertos em seu nome que você não reconheça. Solicite congelamento preventivo no Serasa e Boa Vista.

[6] 24-48H, DENÚNCIAS COMPLEMENTARES
ANPD se houve vazamento de dados; Procon se foi e-commerce; SaferNet se envolveu menor de idade. Mantenha tudo documentado.

[7] 24-72H, ACOMPANHAMENTO PSICOLÓGICO
Vergonha e culpa são reações comuns e perigosas. Não enfrente sozinho. Converse com pessoa próxima. Em casos graves, CVV 188 (24h).

[8] 7 DIAS, ACOMPANHE A CONTESTAÇÃO
Banco tem 11 dias para resposta sobre o MED. Cobre. Se negarem, recorra junto ao BCB pelo **Fale Conosco BCB**: `bcb.gov.br/acessoinformacao`.

CAPÍTULO 10

LGPD para famílias e vazamentos de dados

O que fazer quando seus dados estão na dark web

Em abril de 2026, o pacote chamado "MORGUE", com **251 milhões de registros** de CPFs brasileiros, supostamente extraídos do Gov.br, foi vendido na dark web por US$ 500 em bitcoin. Em 2021, o vazamento "Fim do Mundo" já havia exposto 223 milhões de CPFs. Provavelmente todos os adultos brasileiros têm **vários** dados vazados circulando. A questão não é "se", é "o que fazer com isso".

10.1 O que é dado pessoal, pela LGPD

A Lei Geral de Proteção de Dados (LGPD, Lei 13.709/2018) considera **dado pessoal** qualquer informação que identifique você diretamente (CPF, nome, endereço) ou indiretamente (IP, biometria, localização, hábitos de consumo).

Dados **sensíveis** (art. 5º, II) são uma categoria especial, saúde, religião, opinião política, vida sexual, biometria, dado genético, origem racial. Esses têm proteção reforçada.

10.2 Seus 6 direitos básicos como titular

O art. 18 da LGPD garante a você, gratuitamente:

1. **Confirmação:** saber se a empresa tem dados seus.
2. **Acesso:** ver quais dados ela tem.
3. **Correção:** corrigir dados errados.
4. **Anonimização ou eliminação:** apagar ou tornar anônimo.
5. **Portabilidade:** levar seus dados para outra empresa.
6. **Revogação do consentimento:** "não quero mais que vocês usem meus dados".

> ■ **SAIBA MAIS — Como exercer seus direitos**
>
> **1.** Toda empresa séria tem um **Encarregado de Dados (DPO)**, com contato obrigatório na política de privacidade. Comece por aí: mande e-mail com seu pedido específico.
>
> **2.** A empresa tem **15 dias** para responder (LGPD art. 19).
>
> **3.** Não responderam ou negaram indevidamente? Faça denúncia à **ANPD**: `gov.br/anpd` → Peticionamento. É gratuito e online.
>
> **4.** Para casos graves (vazamento massivo, dados expostos sem consentimento), considere ação judicial. Procure Defensoria Pública ou advogado especializado em LGPD.

10.3 Como saber se seus dados vazaram

■ CHECKLIST — Ferramentas gratuitas de verificação

Have I Been Pwned (`haveibeenpwned.com`): digite seu e-mail ou telefone e veja em quais vazamentos conhecidos você está. Em inglês mas simples de usar.

Serasa Premium, Dark Web: o serviço pago (R$ 19,90/mês) inclui monitoramento contínuo de CPF, e-mail e cartão na dark web.

Registrato BCB (`registrato.bcb.gov.br`): mostra todas as contas, Pix e empréstimos em seu nome. Detecta uso fraudulento do seu CPF no sistema financeiro.

Sintegra/Receita Federal: para verificar CNPJs abertos em seu nome (alguns golpistas usam CPF para abrir MEI fantasma).

10.4 O que fazer se seus dados vazaram

Após confirmar vazamento (de e-mail ou senha em *Have I Been Pwned*, por exemplo):

1. Troque a senha imediatamente nesse serviço, e em qualquer outro onde você usou a mesma senha (motivo número 1 para gerenciador).
2. Ative 2FA no serviço.
3. Configure alertas de movimentação no banco e cartão.
4. Considere **congelamento preventivo de crédito** no Serasa e Boa Vista. Impede que terceiros peçam crédito em seu nome.
5. Monitore Registrato BCB mensalmente nos meses seguintes.

■ PERIGO — A fake news da "indenização automática de R$ 15 mil"

Após cada grande vazamento, circulam mensagens prometendo "indenização garantida de R$ 15 mil pela LGPD", basta pagar taxa de R$ 59,90, R$ 197,00 ou "honorário advocatício antecipado".

É golpe. A LGPD prevê indenização proporcional a dano **específico e comprovado**, jamais valor fixo automático. Não existe processo coletivo nessas condições.

Se você foi vítima de dano real (cartão clonado, conta aberta em seu nome), procure advogado de confiança ou Defensoria Pública. Nunca pague taxa antecipada a "escritório" que aparece em WhatsApp ou Instagram.

10.5 Casos brasileiros emblemáticos

Vazamento "Fim do Mundo" (janeiro de 2021): a maior exposição já documentada no país, 223 milhões de CPFs e dados associados. Cinco anos depois, esses dados ainda alimentam golpes diariamente. Atribuído à Serasa Experian, que foi notificada pelo Procon-SP e Senacon.

MORGUE (abril/2026): 251 milhões de registros vendidos por US$ 500 em bitcoin. Preço 80 vezes menor que o vazamento de 2021, sinal de que dados pessoais brasileiros viraram **commodity barata**.

Multas ANPD 2023-2025: a Autoridade aplicou cerca de R$ 98 milhões em multas. Valor ainda tímido frente à escala, mas crescente.

CAPÍTULO 11

Plano de Emergência Digital Familiar, 30 dias

Uma tarefa por dia para blindar sua família por completo

Se você implementar **uma única ação por dia** deste plano, no final do mês sua família estará mais protegida que 99% das famílias brasileiras. Imprima esta seção. Cole na geladeira. Risque conforme completa.

Dia	Categoria	Tarefa do dia (~15-30 min)
1	SENHAS	Instale Bitwarden (gratuito) em todos os celulares da família. Crie senha-mestra forte.
2	BANCO	Ative 2FA por app no seu banco principal. Tire SMS do meio.
3	PIX	Configure limites de Pix: R$ 1.000/dia comercial, R$ 200 noturno. Cadastre destinatários frequentes.
4	WHATSAPP	Ative Confirmação em Duas Etapas. Configure foto/visto por último para "Meus Contatos".
5	FAMÍLIA	Convoque reunião familiar. Defina PALAVRA-CÓDIGO única. Ensine a todos, incluindo avós.
6	CHIP	Ative PIN do SIM em todos os celulares da família.
7	WI-FI	Troque senha do roteador. Crie rede de visitantes separada.
8	INSTAGRAM	Toda a família: conta privada, 2FA, foto para contatos. Reveja seguidores estranhos.
9	FACEBOOK	Reveja apps conectados, "ver como público", remova reconhecimento facial.
10	GOOGLE	Em myaccount.google.com: 2FA, revisar apps com acesso, atividade recente.
11	E-MAIL	Troque senha do e-mail principal. Configure recuperação por chave física ou backup codes.
12	VAZAMENTOS	Verifique cada membro da família em haveibeenpwned.com. Troque senhas vazadas.
13	BACKUP	Configure backup 3-2-1 das fotos da família (Google Drive ou iCloud + HD externo).
14	IDOSOS	Sente com seu pai/mãe. Reconfigure WhatsApp, banco, foto de perfil. Combine palavra-código.
15	CRIANÇAS	Instale Family Link ou Tempo de Uso. Defina limites e bloqueios apropriados à idade.

Dia	Categoria	Tarefa do dia (~15-30 min)
16	CONVERSA	Faça a "Regra do Não Brigo" com adolescentes da família.
17	JOGOS	Reveja contatos do Discord/Roblox/Fortnite dos seus filhos. Desabilite chat com estranhos.
18	CARTÃO	Ative cartão virtual no app do banco. Use a partir de agora para compras online.
19	MED-Pix	Localize o botão de contestação MED no seu app. Saiba como usar antes de precisar.
20	DNS	Configure NextDNS ou Cloudflare 1.1.1.1 for Families na rede de casa.
21	NAVEGADOR	Instale uBlock Origin e Privacy Badger. Remova extensões que você não usa.
22	NOTIFICAÇÕES	Ative todas as notificações de transação no banco, mesmo de R$ 1.
23	REGISTRATO	Consulte registrato.bcb.gov.br. Veja se há contas/Pix em seu nome que não reconhece.
24	TVS E IoT	Reveja smart TV, Alexa/Google Home: senhas, gravações, apps instalados.
25	IMPRESSO	Imprima telefones de emergência (banco, 100, 180, 190, SaferNet). Cole na geladeira.
26	TESTE	Faça um simulado: peça a um parente para tentar um "golpe do parente" por WhatsApp.
27	IDOSO+2	Volte com seu pai/mãe. Revise se as configurações ainda estão. Reforce regras.
28	KIT EMERGÊNCIA	Documente em PDF: senha-mestra (não a senha), contatos, conta dos serviços críticos. Guarde com pessoa de confiança.
29	AVALIAÇÃO	Em família: o que aprenderam? Onde ainda há vulnerabilidades? Que dúvidas restaram?
30	CICLO	Marque na agenda: próxima revisão em 90 dias. Defina responsável familiar pela "manutenção digital".

✓ DICA RÁPIDA — Depois dos 30 dias: manutenção contínua

Mensal: Reunião familiar de 30 min para falar dos golpes do mês. Revisar privacidade de uma rede social por vez.

Trimestral: Revisar firmware do roteador. Auditar apps instalados no celular. Revisar permissões de acessibilidade.

Semestral: Verificar Have I Been Pwned. Consultar Registrato BCB. Atualizar palavra-código familiar se houver suspeita.

Anual: Revisar tudo deste livro. Atualizar a edição mais recente (golpes evoluem; este livro evolui).

CAPÍTULO 12

Casos reais brasileiros que você precisa conhecer

O que aconteceu, e o que aprendemos com cada caso

Estatísticas convencem a razão. Casos reais convencem o instinto. Aqui estão 6 casos brasileiros recentes que ilustram como cada golpe acontece na vida real, e quais lições eles nos deixam.

Aposentada em Santo André (SP), março de 2024

Falsa central, R$ 25 mil

Uma aposentada de 79 anos recebeu ligação de "gerente do banco" às 14h. A conversa, com transferências graduais "para conta segura", durou 4 horas. Quando desligou, o saldo havia caído R$ 25 mil. O Diário do Grande ABC relatou o caso como parte da alta de 108% em golpes contra idosos no ABC em 3 anos.

Lição: nenhum banco mantém cliente por horas ao telefone. Quando começa a passar de 5 minutos, é fraude. Combine com idosos da família a regra de "desligar e ligar de volta no número do cartão".

Mulher em Acadiana (EUA), janeiro de 2025

Deepfake romance, US$ 60 mil

A vítima passou meses em relacionamento por mensagens com "Elon Musk", incluindo chamadas FaceTime com deepfake. O criminoso pediu sucessivos depósitos para "liberar fundos congelados". A vítima perdeu economias de uma vida.

Lição: celebridades não namoram via DM. Reversão de imagem em Google Images detecta foto roubada em segundos. Deepfake já consegue enganar em videochamada, mas pedidos de dinheiro são sempre red flag.

Funcionário em Hong Kong, fevereiro de 2024

Deepfake corporativo, US$ 25 milhões

Em uma videoconferência supostamente com o CFO e três colegas, o funcionário autorizou transferência de US$ 25 milhões. Todos os participantes eram deepfakes. Maior fraude por deepfake já documentada no mundo.

Lição: palavra-código também em empresas. Para transações incomuns, exija confirmação por canal alternativo, mesmo de superiores hierárquicos.

Operação Grandoreiro (PF + Interpol), março de 2024

Trojan bancário brasileiro, US$ 120 milhões em prejuízo global

Polícia Federal e Polícia Nacional da Espanha prenderam 5 operadores da quadrilha Grandoreiro, um trojan que mirou 1.700 bancos em 45 países. Apesar das prisões, o malware continuou evoluindo com novas variantes em 2025. A Kaspersky descreve o Grandoreiro como o trojan bancário brasileiro de maior longevidade.

Lição: **nunca instale app de banco fora da loja oficial**. Se receber SMS ou e-mail pedindo para "atualizar o app", ignore. Vá direto à Play Store ou App Store.

Vazamento MORGUE, abril de 2026

251 milhões de CPFs, US$ 500 em bitcoin

Um ator anônimo colocou à venda na dark web pacote com 251 milhões de registros incluindo CPFs, nomes completos, datas de nascimento e endereços. O preço, apenas US$ 500 em bitcoin, chocou pesquisadores de segurança: oito vezes a população do Brasil em registros, ao preço de uma camiseta de futebol.

Lição: **seus dados pessoais já vazaram em alguma medida**. A defesa é assumir isso e blindar as camadas seguintes: 2FA forte, monitoramento Registrato BCB, congelamento preventivo de crédito.

Roblox, ações judiciais Louisiana (ago/2025) e Los Angeles (fev/2026)

Exposição sistêmica de crianças a predadores

As Procuradorias-Gerais da Louisiana e de Los Angeles entraram com ações judiciais contra a Roblox Corporation por alegada falha em proteger menores de predadores na plataforma de 144 milhões de usuários ativos diários. O Brasil registra 19% das contas globais de Roblox.

Lição: **plataformas globais não vão proteger seu filho por você**. Controle parental, supervisão ativa, conversas honestas e o ECA Digital agora dão respaldo legal a famílias que exigem mais.

✓ DICA RÁPIDA — O fio condutor

Em **todos** esses casos, Hong Kong com R$ 130 milhões ou aposentada em Santo André com R$ 25 mil, a defesa que teria funcionado é a mesma: **pausa e verificação por canal alternativo**.

Não importa se você é um adolescente caindo em sextortion, ou um CFO autorizando transferência milionária: a pressa do golpe é o que dá certo para o criminoso. A pausa de 30 segundos é o que mata o golpe.

Treine sua família para essa pausa. É o investimento mais barato e mais rentável que você pode fazer.

CAPÍTULO 13

Glossário de Termos

O vocabulário da guerra digital, explicado em uma linha

Esta seção é seu dicionário rápido. Toda vez que um termo técnico apareceu no livro e você ficou em dúvida, volte aqui. Ordem alfabética.

2FA / MFA	Autenticação de Dois ou Múltiplos Fatores. Confirmação extra além da senha (código, biometria, chave física).
AdBlocker	Extensão de navegador que bloqueia anúncios e rastreadores. Exemplos: uBlock Origin, Privacy Badger.
Algoritmo	Sequência lógica de instruções que um programa executa. Em redes sociais, decide o que você vê.
Antivírus	Software que detecta e remove malware. Hoje considerado defesa básica, não suficiente sozinho.
ANPD	Autoridade Nacional de Proteção de Dados. Fiscaliza o cumprimento da LGPD no Brasil.
Antifraude	Sistema que detecta padrões suspeitos de transação (Pix, cartão) e bloqueia preventivamente.
Backup	Cópia de segurança de arquivos. A regra 3-2-1: 3 cópias, em 2 mídias diferentes, com 1 fora do local.
BCB	Banco Central do Brasil. Regula sistema financeiro, Pix, contestações MED e portabilidade bancária.
Biometria	Identificação por características corporais únicas: digital, rosto, íris, voz. Não é infalível.
Bot	Programa automatizado. Em redes sociais, finge ser humano para amplificar mensagens ou aplicar golpes.
Botnet	Rede de dispositivos infectados controlados remotamente por um criminoso, sem o dono saber.
Brute force	Ataque por força bruta: testar milhares de senhas até acertar. Defesa: senha longa e 2FA.
Cavalo de Troia	Sinônimo de trojan. Programa que se disfarça de legítimo e abre porta para roubo após instalação.
Captcha	Teste "Não sou robô". Confirma que há um humano operando, não um bot automatizado.
CDC	Código de Defesa do Consumidor (Lei 8.078/1990). Garante direitos em compras e serviços digitais.
CERT.br	Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. Aceita denúncias de fraude.
Certificado SSL/TLS	Cadeado verde no navegador. Indica que a conexão com o site é cifrada, não que o site é honesto.
Cibersegurança	Disciplina técnica de proteção de sistemas, redes e dados contra ataques digitais.
Clickjacking	Botão invisível sobreposto a outro. Você acha que clicou em uma coisa, mas clicou em outra.

Cloud	Computação em nuvem. Serviços remotos como Google Drive, iCloud, Dropbox. Conveniente, mas centraliza riscos.
Cookies	Pequenos arquivos que sites guardam no seu navegador. Necessários para login, mas também rastreiam você.
CPF na nota	Hábito brasileiro de fornecer CPF em compras. Cada uso amplia sua exposição em vazamentos.
Criptografia	Embaralhamento matemático de dados que só pode ser lido por quem tem a chave correta.
CVV	Código de verificação do cartão (3 dígitos atrás). Nunca compartilhe por telefone ou SMS.
Dark web	Parte da Internet acessível só por navegador Tor. Onde dados vazados, drogas e armas são negociados.
Deepfake	Vídeo ou áudio gerado por IA imitando rosto ou voz reais. Bastam 15 segundos de áudio para clonar uma voz.
DNS	Domain Name System. Traduz "banco.com.br" em número de IP. Ataques de DNS levam a sites falsos.
Doxxing	Expor publicamente dados pessoais (endereço, telefone, família) de alguém com intenção de prejudicar.
ECA Digital	Lei 15.211/2025 (em vigor desde 17/03/2026). Estende o Estatuto da Criança e do Adolescente ao ambiente digital.
Engenharia social	Manipulação psicológica para induzir a vítima a entregar dados ou fazer ações fora do comum. Base de quase todo golpe.
eSIM	Chip digital embutido no celular, sem cartão físico. Presente em iPhones e Androids mais novos.
Febraban	Federação Brasileira de Bancos. Divulga estatísticas oficiais de fraude bancária no país.
FIDO2 (chave física)	Padrão de chave de segurança em USB ou NFC (ex: YubiKey). Substitui senha. Resistente a phishing por design.
Firewall	Barreira entre sua rede e a Internet. Filtra conexões suspeitas. Roteadores domésticos já trazem um básico.
FOMO	*Fear Of Missing Out*. Medo de ficar de fora. Gatilho psicológico usado por jogos e redes para manter você grudado.
Gestor de senhas	App que armazena suas senhas de forma cifrada. Bitwarden, 1Password, KeePass, Proton Pass. Senha mestra é única que você decora.
Golpe do amor	Romance scam. Criminoso constrói relacionamento online por semanas/meses antes de pedir dinheiro.
Golpe do falso parente	Variação do WhatsApp clonado. "Mãe, troquei de número, salva aí" antes de pedir Pix urgente.
Grooming	Aliciamento gradual de criança ou adolescente por adulto. Ganho de confiança antes do abuso. Acontece em jogos e chats.
Hacker	Pessoa com profundo conhecimento técnico. Pode ser ético (defensivo) ou criminoso. O termo correto para o segundo é *cracker*.
Hash	Impressão digital matemática de um arquivo ou senha. Mudou um bit, mudou o hash. Usado para verificar integridade.
Have I Been Pwned	Site (haveibeenpwned.com) onde você consulta se seu e-mail apareceu em vazamentos públicos. Grátis.

IA generativa	Inteligência Artificial que cria conteúdo: texto, imagem, voz, vídeo. ChatGPT, Midjourney, ElevenLabs.
IoT	Internet of Things. Dispositivos conectados: câmeras, lâmpadas, TVs, geladeiras. Principal vetor doméstico hoje.
IP	Endereço numérico que identifica seu dispositivo na Internet. Pode revelar sua cidade aproximada.
LGPD	Lei Geral de Proteção de Dados (Lei 13.709/2018). Define direitos dos cidadãos sobre seus dados pessoais.
Login social	"Entrar com Google/Facebook/Apple". Conveniente, mas concentra todo seu acesso em um único ponto de falha.
Malware	Termo guarda-chuva para programa malicioso: vírus, trojan, spyware, ransomware. Significa *software malicioso*.
MED-Pix	Mecanismo Especial de Devolução do Pix (Resolução BCB 493). Permite contestar Pix de fraude em até 80 dias.
Metadados	Dados sobre os dados: hora da foto, localização GPS, modelo do celular. Vazam mais que o conteúdo em si.
MORGUE	Vazamento brasileiro de abril/2026 com 251 milhões de CPFs à venda na dark web por US$ 500 em bitcoin.
NextDNS / Cloudflare 1.1.1.1	DNS familiar com filtros de conteúdo. Bloqueia sites adultos, phishing e malware na rede toda da casa.
NFC	*Near Field Communication*. Tecnologia de pagamento por aproximação. Maquininha, celular, cartão sem contato.
OSINT	*Open Source Intelligence*. Coleta de dados públicos (redes sociais, sites) para reconhecimento antes de ataque.
Painel gov.br	Painel de Fraudes Bancárias Digitais lançado pelo governo federal em dezembro/2025. Dados oficiais consolidados.
Passkey	Chave criptográfica que substitui senha. Usa biometria do dispositivo. A chave privada nunca sai do aparelho.
Phishing	Mensagem (e-mail, SMS, WhatsApp) que se passa por instituição legítima para roubar dados. "Pesca" digital.
Pix	Sistema de pagamento instantâneo do BCB. Praticamente irreversível, salvo via MED em casos de fraude.
Procon	Órgão estadual de defesa do consumidor. Aceita reclamações de fraude em compras e serviços.
Projeto Shield	Ecossistema de segurança digital para a família brasileira. Parceria Wanderley J. Abreu Jr. (Storm) + Felipe Neto; lançamento previsto para setembro/2026.
Ransomware	Vírus que criptografa todos os arquivos do computador e exige pagamento (geralmente em bitcoin) para liberá-los.
Recuperação por SMS	Método de recuperação de senha por código enviado por SMS. Vulnerável a SIM swap. Evite quando possível.
Registrato	Sistema do BCB (registrato.bcb.gov.br) onde você consulta todas as contas e empréstimos em seu CPF.
RFID Blocker	Carteira ou capa que bloqueia leitura por rádio de cartões NFC/RFID. Útil em transporte público lotado.
SaferNet	ONG brasileira que recebe denúncias de crimes digitais contra crianças. (safernet.org.br).

Scareware	Pop-up que assusta a vítima com falsa infecção ("seu PC tem 47 vírus!") para vender produto falso ou instalar malware.
Senha mestra	A única senha que você precisa decorar quando usa gestor de senhas. Longa, forte, exclusiva.
Sextortion	Chantagem usando material íntimo (real ou falso) da vítima. Crescente entre adolescentes; gatilho frequente de suicídio.
SIM PIN	Senha de 4-8 dígitos pedida pelo chip a cada reinicialização. Inutiliza o chip se o celular for roubado.
SIM swap	Golpe em que criminoso transfere seu número telefônico para um chip dele. Captura SMS de recuperação de senha.
Smishing	Phishing por SMS. Tipicamente: "Sua encomenda está retida, clique aqui para regularizar".
Spear phishing	Phishing personalizado com dados reais da vítima (nome, CPF, endereço) para parecer legítimo.
Spoofing	Falsificação de identidade técnica: número de telefone, e-mail remetente ou IP de origem.
Stalkerware	App de espionagem instalado no celular da vítima, frequentemente sem consentimento, em contexto de violência doméstica.
Tempo de Uso (iOS) / Family Link (Android)	Controles parentais nativos do sistema operacional. Limitam tempo de tela e aplicativos por idade.
Tor	Navegador especial que oculta sua identidade rebatendo a conexão por várias máquinas. Acesso à dark web.
Trojan	Programa que se disfarça de legítimo (falso app de banco) e, quando instalado, abre porta para roubo de dados.
Two-Person Integrity	Política corporativa: nenhuma transação grande sem co-aprovação humana por canal independente.
Typosquatting	Domínio falso com erro intencional (goog1e.com, bradescco.com.br) para enganar quem digita rápido.
uBlock Origin	Extensão de navegador gratuita e open-source. Bloqueia anúncios e rastreadores. Mais eficaz que AdBlock Plus.
Vazamento	Exposição não autorizada de dados pessoais. Pode ser por ataque, falha técnica ou venda interna.
VPN	*Virtual Private Network*. Cria túnel cifrado para sua navegação. Útil em Wi-Fi público; não anonimiza totalmente.
Vishing	Phishing por voz (ligação telefônica). Falsa central, falso gerente, falso parente. Forma mais antiga e ainda muito eficaz.
WPA3	Padrão atual de criptografia Wi-Fi (2018). Mais seguro que WPA2 e infinitamente mais seguro que WEP/WPA.
YubiKey	Marca mais conhecida de chave física FIDO2. Custa entre R$ 200 e R$ 600. Resistente a phishing por design.
Zero Trust	Modelo de segurança que parte do princípio "não confiar em ninguém por padrão". Cada acesso é verificado.

Recursos

Canais oficiais de denúncia, ajuda e informação

Imprima esta página. Cole na geladeira. Salve uma foto no celular de cada pessoa da família. Numa crise, segundos contam, e ter os contatos certos à mão pode salvar dinheiro, dignidade ou uma vida.

Canal	Para que serve	Como acessar
SaferNet Brasil, Denúncia	Crimes contra crianças online, abuso sexual, exposição íntima	denuncie.org.br/safernet (anônimo)
SaferNet Helpline	Ajuda gratuita para vítimas de crimes online	new.safernet.org.br/helpline
Disque 100	Violência contra crianças, adolescentes, idosos, LGBT+	Ligar 100 (24h)
Disque 180	Violência contra mulher	Ligar 180 (24h, gratuito)
CVV, Centro Valorização da Vida	Apoio em crise emocional / risco de suicídio	Ligar 188 (24h, gratuito)
CERT.br	Reportar phishing, malware, spam, incidentes	cert.br/contato
SaferNet, Cybercrimes	Denúncia de crimes cibernéticos em geral	new.safernet.org.br/denuncie
gov.br, Cartilhas de segurança	Material educativo oficial	gov.br/seguranca-cibernetica
ANPD, Autoridade Nacional	Vazamento de dados, abusos LGPD	gov.br/anpd → Peticionamento
Procon estadual	Problemas de consumo (e-commerce fake, cobrança indevida)	Procon do seu estado
Polícia Federal	Crimes federais, vazamentos massivos, exploração infantil	gov.br/pf → Delegacia Virtual
Delegacias de cibercrime (estaduais)	BO online de estelionato eletrônico, invasão de conta	Site da Polícia Civil do seu estado
Registrato BCB	Ver contas, Pix e empréstimos abertos em seu CPF	registrato.bcb.gov.br
Fale Conosco BCB	Reclamações contra bancos (MED negado etc.)	bcb.gov.br/acessoinformacao
Have I Been Pwned	Verificar se e-mail/telefone foi vazado	haveibeenpwned.com
No More Ransom	Decryptors gratuitos para ransomware	nomoreransom.org
Black Ice Security	Atualizações deste livro, materiais educativos complementares	blackice-security.com.br
Grupo Storm	Site institucional do autor	stormnexus.com.br

Sobre o autor

A trajetória de Storm

Wanderley J. Abreu Jr., conhecido no mundo da segurança digital como **Storm**, nasceu em 17 de janeiro de 1978, no Rio de Janeiro. Ex-hacker e empresário, é fundador do **Grupo Storm** e da **Black Ice Security**, com mais de três décadas de atuação em cibersegurança, criptografia e proteção de infraestruturas críticas.

A invasão à NASA: aos 17 anos

Aos 17 anos, Storm invadiu sistemas da **NASA**. O episódio poderia tê-lo levado a sérias complicações internacionais, mas, em vez de processo, recebeu um convite oficial. Foi recebido no **Goddard Space Flight Center (GSFC)**, em Maryland, para demonstrar as vulnerabilidades encontradas e participar de programas de fortalecimento. Voltou ao Brasil com um diploma de especialista em segurança digital concedido pela própria agência.

Na mesma época, a partir do acesso obtido nos sistemas da NASA, Storm alcançou o **Blue Mountain**, então um dos supercomputadores mais poderosos do mundo, instalado no **Laboratório Nacional de Los Alamos**, no Novo México. O caso ampliou ainda mais o reconhecimento de sua capacidade técnica e consolidou sua trajetória internacional em segurança digital.

Anos depois, integrou a equipe de comunicação do projeto **Mars 2020**, que pousou o rover Perseverance em Marte em fevereiro de 2021, e contribuiu para sistemas do **Telescópio Espacial James Webb**.

Agência Espacial Europeia e OTAN

Trabalhou para a **Agência Espacial Europeia (ESA)** no projeto **Galileo**, o sistema europeu de navegação por satélite, e desenvolveu criptografia multinível para tropas da **OTAN no Afeganistão**, em operações de comunicação segura em zona de conflito.

Operação Catedral-Rio: a outra missão

No Brasil, aos 20 anos, fez história ao trabalhar voluntariamente com o **Ministério Público do Rio de Janeiro** na **Operação Catedral-Rio**, a primeira grande operação contra pedofilia online realizada no Brasil. Trabalhando nas madrugadas ao lado do então promotor Romero Lyra, Storm criou personas online para infiltrar redes de criminosos e identificou **mais de 200 pedófilos**, gerando provas materiais que mudaram a jurisprudência brasileira sobre crimes sexuais contra crianças em ambiente digital.

Sua atuação na Operação Catedral é citada como uma das forças que motivaram a alteração das leis brasileiras sobre publicação digital de material de abuso. O biógrafo Alessandro Greco registra que, dos 230 pedófilos indiciados pela operação, "quatro ou cinco foram condenados" diante das brechas legais da época, e foi justamente esse caso que forçou a lei brasileira a evoluir.

Formação e empresas

Estudou Engenharia Mecatrônica e Sistemas da Informação na **PUC-Rio** e fez especialização em Segurança de Computadores e Criptografia pelo **MIT**. Aos 25 anos, havia criado e vendido sua primeira empresa, a **Storm Development**.

Hoje comanda o **Grupo Storm**, um ecossistema de empresas focadas em desenvolvimento de sistemas de alto desempenho, DevSec, streaming global e cibersegurança corporativa, atuando para governos, instituições financeiras e organizações internacionais.

Honrarias

• **Medalha Tiradentes**, da Assembleia Legislativa do Rio de Janeiro (Alerj), março de 2021.
• **Medalha Pedro Ernesto**, da Câmara Municipal do Rio de Janeiro, outubro de 2021.
• **Medalha Cinquentenário das Forças de Paz do Brasil**, da Associação Brasileira das Forças Internacionais de Paz da ONU (ABFIPONU), maio de 2022.

Biografia

Sua trajetória foi narrada no livro ***"Storm: A história do hacker brasileiro que invadiu a Nasa, desbaratou crimes na rede e inovou no empreendedorismo digital"***, escrito pelo jornalista **Alessandro Greco** e publicado em novembro de 2022 pela **Companhia das Letras** (selo Objetiva).

> *"A trajetória de Storm sintetiza a tensão entre luz e sombra do universo hacker. O mesmo conhecimento que poderia ter causado um incidente internacional foi usado para proteger crianças e para construir um dos maiores ecossistemas de cibersegurança do Hemisfério Sul."*
>
> **Alessandro Greco**, biógrafo (Companhia das Letras, 2022)

■ SAIBA MAIS — Por que escrever este livro agora

"Passei a vida no lado técnico da história. Mas há um lado da guerra que nenhum firewall corporativo resolve: o lado de casa. O lado em que sua mãe recebe um áudio do neto pedindo Pix de R$ 2 mil e a voz é exatamente a do seu filho, porque um algoritmo clonou em 15 segundos."

"Este livro é o manual que eu queria ter dado para a minha família há dez anos. É a tradução, para o português direto e a realidade brasileira, daquilo que aprendi protegendo sistemas para NASA, ESA, OTAN e MP-RJ, agora aplicado àquilo que mais importa: a sua casa."

Storm, Rio de Janeiro, maio de 2026

Você é o próximo alvo.
Sua família, também.

Um manual de defesa para as famílias brasileiras no Brasil de 2026.

OS NÚMEROS DA GUERRA DIGITAL NO BRASIL

R$ 10,1 bi	1 a cada 3s	+220%
PERDIDOS EM 2024	**TENTATIVA DE FRAUDE**	**CRESCIMENTO MALWARE**
Febraban	*gov.br 2024*	*BioCatch 1º sem. 2025*

WhatsApp clonado. Falsa central. Deepfake de voz. Predadores em jogos. Golpes contra idosos. Vazamentos massivos. A guerra digital invadiu a sua casa.

Este livro é o seu manual de defesa.

Você vai aprender a configurar 2FA no banco em 5 minutos, conversar com seu filho sobre grooming online, blindar seu pai da falsa central, identificar um deepfake de voz no WhatsApp e acionar o MED-Pix nas primeiras 24 horas.

> *A segurança da sua família não é mais um problema técnico.*
> *É um problema de família. E como todo problema de família,*
> *se resolve com conversa, regra e exemplo.*
>
> **— STORM**

AUTOR

WANDERLEY J. ABREU JR.

"STORM" NASA • ESA • OTAN • MP-RJ (Catedral-Rio, 1998)
Storm Nexus • Black Ice Security • Grupo Storm

PUBLICAÇÃO

Storm Nexus — Black Ice Security

stormnexus.com.br • blackice-security.com.br • Rio de Janeiro • Maio de 2026

IDENTIFICADOR DIGITAL

BIS-2026-FAM-001

Educativo • Uso livre

PROTEGER • EDUCAR • DEFENDER