

COLEÇÃO

Investigação e Proteção na Era Digital

VOLUME 07

Internet segura

Guia prático para proteger você e sua família



07

HIGOR VINICIUS NOGUEIRA JORGE

www.higorjorge.com.br

DISTRIBUIÇÃO
GRATUITA

HIGOR VINICIUS NOGUEIRA JORGE

Internet segura

Guia prático para proteger você e sua família

*Orientações essenciais para utilizar celulares, aplicativos, redes sociais
e serviços digitais com mais segurança.*

Coleção Investigação e Proteção na Era Digital
Volume 07

1ª edição
Santa Fé do Sul, SP
CodexNauta
2026

© 2026 Higor Vinicius Nogueira Jorge

Material educativo de distribuição gratuita.

Coleção Investigação e Proteção na Era Digital, volume 07.

www.higorjorge.com.br

Ficha catalográfica

Jorge, Higor Vinicius Nogueira.

Internet segura : guia prático para proteger você e sua família [recurso eletrônico] / Higor Vinicius Nogueira Jorge.

-- 1. ed. -- Santa Fé do Sul, SP : CodexNauta, 2026.

1 recurso online (47 p.) : il. -- (Coleção Investigação e Proteção na Era Digital ; 7)

Formato: PDF.

Modo de acesso: World Wide Web: <www.higorjorge.com.br>.

Inclui referências, apêndices e resumo para compartilhar.

Publicação de distribuição gratuita.

1. Segurança na internet. 2. Educação digital. 3. Privacidade. 4. Proteção de contas digitais. 5. Prevenção de golpes. 6. Família. I. Título. II. Série.

Sumário

Apresentação.....	5
Objetivos e público-alvo.....	6
1 A internet faz parte da nossa vida.....	7
2 Como proteger seu celular.....	9
3 Senhas fortes e proteção das contas.....	11
4 WhatsApp e aplicativos de mensagens.....	14
5 Redes sociais e exposição de informações.....	16
6 Compras pela internet com mais segurança.....	18
7 Pix e pagamentos digitais.....	20
8 Links e QR Codes suspeitos.....	23
9 Inteligência artificial e novos golpes.....	25
10 Como proteger crianças e pessoas idosas.....	27
11 Fui vítima de um golpe. E agora?.....	29
12 Vinte hábitos de segurança digital.....	31
Considerações finais.....	33
Apêndice A. Plano de proteção em 15 minutos.....	34
Apêndice B. Checklist de segurança do celular.....	35
Apêndice C. Dez sinais de alerta para golpes.....	36
Apêndice D. Primeiras 24 horas após um incidente.....	37
Apêndice E. Página para compartilhar com a família.....	38
Apêndice F. Resumo para compartilhar.....	39
Referências.....	42
Minicurrículo do autor.....	44
Para aprofundar o estudo.....	46
A coleção.....	47

Apresentação

O celular guarda conversas, fotografias e documentos, permite pagar contas e aproxima quem está longe. Proteger esse acesso é uma tarefa do dia a dia. Ela começa por escolhas compreensíveis: conferir quem está pedindo algo, cuidar das senhas e conhecer os caminhos de ajuda.

Muitos golpes aproveitam situações comuns. Uma pessoa está ocupada, espera uma encomenda ou recebe um pedido que parece vir de um familiar. O fraudador tenta impedir a verificação, usando urgência, medo ou uma vantagem atraente. Saber reconhecer esse momento ajuda a interromper a fraude antes do pagamento ou da entrega de dados.

No meu livro *Investigação criminal tecnológica*, examino como informações e vínculos precisam ser interpretados em seu contexto. Aqui, esse cuidado se traduz em uma orientação simples: nome, foto e aparência conhecida não bastam para confirmar quem está fazendo um pedido (Jorge, 2027).

Esta cartilha foi escrita para quem utiliza a internet sem precisar conhecer seus detalhes técnicos. Os capítulos explicam os cuidados e mostram como aplicá-los. Ao final, há instrumentos para conferir o celular, organizar a proteção da família e agir diante de um incidente.

Higor Vinicius Nogueira Jorge
www.higorjorge.com.br

Objetivos e público-alvo

Este guia se destina a pessoas de todas as idades, famílias, estudantes e usuários de serviços digitais. Pode ser utilizado em casa, em palestras e em atividades de educação digital. Nenhuma experiência em informática é necessária.

A proposta é ajudar você a reconhecer pedidos suspeitos, proteger o celular e as contas, comprar com mais cuidado e procurar ajuda pelos canais adequados. As orientações também mostram como apoiar crianças e pessoas idosas sem constrangimento ou perda desnecessária de autonomia.

Como aproveitar a leitura

Comece pelos capítulos sobre celular e senhas. Se houver um incidente em andamento, procure diretamente o capítulo 11 e o Apêndice D. A comunicação ao banco, quando houver fraude financeira, deve ser imediata. Não espere terminar a leitura ou registrar a ocorrência para pedir atendimento à instituição.

O plano de 15 minutos é um ponto de partida. Use o checklist para registrar o que foi conferido e o que ainda precisa de atenção. Não escreva senhas, códigos de recuperação ou dados bancários nos formulários.

A página para familiares pode ser impressa. O Apêndice F traz uma versão resumida, em duas páginas, para compartilhar. O resumo ajuda a lembrar os cuidados, enquanto a cartilha completa explica as situações e as providências.

CAPÍTULO 1

A internet faz parte da nossa vida

1.1 Reconhecer o momento de conferir

A segurança digital envolve o aparelho e as decisões tomadas durante o uso. Um telefone atualizado pode receber uma mensagem falsa. Uma conta protegida pode ser imitada por outro perfil. Por isso, as configurações de segurança precisam caminhar com a verificação dos pedidos recebidos.

O golpista pode conhecer seu nome, uma compra recente ou informações de sua família. Esses dados podem ter sido publicados, obtidos de terceiros ou expostos em algum incidente. Conhecer um detalhe verdadeiro não demonstra que o contato é legítimo.

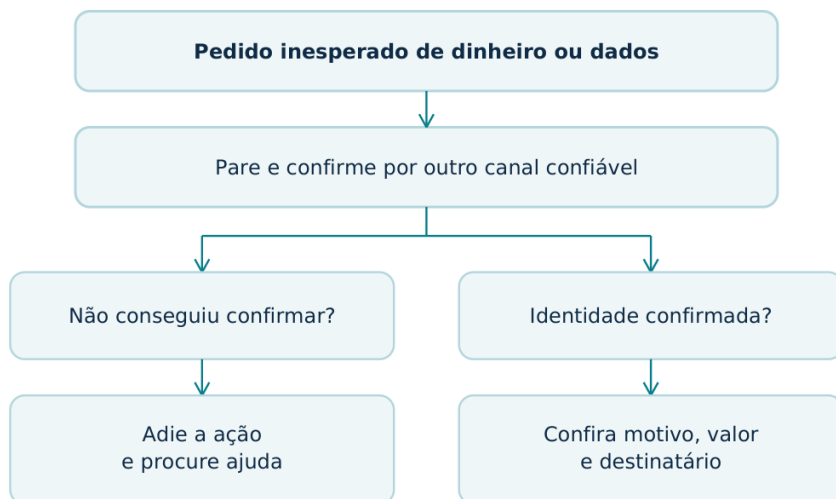
Exemplo hipotético. Uma mensagem informa que uma encomenda está retida e exige pagamento imediato. Como você realmente espera um pacote, a cobrança parece fazer sentido. Confira a situação no aplicativo ou no site oficial que já utiliza, sem abrir o endereço enviado na mensagem.

Um pedido para agir em segredo, manter uma chamada ou não consultar ninguém merece atenção. Interromper o contato e verificar por outro caminho permite decidir com mais segurança. A pressa de quem pede não precisa se tornar a sua pressa.

Cair em um golpe não define a inteligência de ninguém. Se algo acontecer, procure ajuda e preserve as informações disponíveis. A vergonha pode atrasar as medidas que reduzem o prejuízo (CERT.br, 2026a; 2026b).

1.2 Confirmar por um caminho que você escolheu

Para confirmar uma cobrança, abra por conta própria o aplicativo já instalado ou use um canal obtido anteriormente em fonte confiável. Para confirmar um pedido familiar, procure a pessoa por outro meio e esclareça o que está acontecendo. Continuar a conversa suspeita não é uma verificação independente.

Figura 1. Como conferir um pedido inesperado

Fonte: elaboração própria. Mesmo depois de confirmar a identidade, confira o motivo, o destinatário e o valor antes de autorizar um pagamento.

Se não conseguir confirmar, adie a ação. Não envie uma pequena quantia para “testar” a conta e não informe um código para provar que você é a pessoa certa. A confirmação deve acontecer antes da entrega de dinheiro ou informações.

CAPÍTULO 2

Como proteger seu celular

2.1 Bloqueio e atualizações fazem diferença

Configure uma senha de desbloqueio que outras pessoas não consigam deduzir. Evite datas conhecidas e sequências simples. Se usar biometria, mantenha também uma boa senha de reserva, pois o aparelho pode solicitá-la em diferentes situações.

Ative o bloqueio automático após um período curto de inatividade. Reduza o conteúdo de mensagens que aparece na tela bloqueada. Assim, quem estiver perto terá menos acesso a conversas e códigos recebidos, mesmo sem desbloquear o telefone.

Instale as atualizações do sistema e dos aplicativos pelos recursos oficiais. Elas corrigem falhas e podem trazer proteções adicionais. Não instale uma suposta atualização enviada por desconhecido, por mensagem ou por uma janela que anuncia infecção urgente.

Exemplo hipotético. Um aviso no navegador afirma que há vários vírus e pede um aplicativo de limpeza. Feche a página sem seguir suas instruções. Confira o aparelho pelos recursos do próprio sistema ou procure assistência de confiança. A mensagem, por si só, não é um diagnóstico.

Ao emprestar o celular, limite o acesso à tarefa necessária, utilizando os recursos disponíveis no aparelho. Evite entregar o telefone desbloqueado para que alguém “resolva tudo”, especialmente quando há bancos, documentos e contas pessoais acessíveis (CERT.br, 2022b; 2024).

2.2 Prepare o aparelho antes de precisar de ajuda

Baixe aplicativos pela loja oficial e confira o desenvolvedor. A presença na loja reduz alguns riscos, mas não dispensa a verificação. Autorize apenas permissões que façam sentido para a função utilizada. Um pedido de acesso a contatos, câmera ou localização deve ter finalidade compreensível.

Ative os recursos oficiais de localização e bloqueio remoto disponíveis para seu modelo. Saiba como acessá-los por outro dispositivo. Guarde o identificador do aparelho, chamado IMEI, fora do celular, junto à documentação de compra. Esses cuidados ajudam em caso de perda ou furto.

Faça cópias de segurança, também chamadas backups, das informações importantes. Confira se as cópias estão sendo realizadas e se você consegue recuperar algum arquivo de teste. Não dependa de uma única cópia guardada no próprio aparelho que deseja proteger.

Na prática. Reserve um momento para revisar aplicativos que não utiliza, permissões e opções de segurança. Se o telefone deixou de receber correções, planeje sua substituição conforme suas possibilidades e reduza seu uso em atividades sensíveis.

Em caso de furto, priorize sua integridade física. Uma localização no mapa não autoriza nem torna seguro tentar recuperar o aparelho por conta própria. Procure a polícia e siga as medidas de proteção das contas descritas no capítulo 11 (CERT.br, 2022b; 2023a; 2024).

CAPÍTULO 3

Senhas fortes e proteção das contas

3.1 Cada conta precisa de sua própria senha

Usar a mesma senha em vários serviços facilita o trabalho de quem a descobre em um deles. A exposição de uma conta pouco importante pode abrir caminho para o e-mail, uma loja ou outro serviço em que a senha foi repetida.

Crie senhas longas e diferentes. Evite informações pessoais, frases famosas e pequenas variações previsíveis de uma senha antiga. Um gerenciador de senhas pode ajudar a criar e guardar combinações, desde que seja obtido de fonte confiável e protegido por uma senha principal forte.

Se você prefere anotar, guarde o registro em local físico protegido, sem deixá-lo junto ao celular ou exposto em fotografias e mensagens. O importante é não manter senhas em locais facilmente acessíveis e não compartilhá-las para conseguir atendimento.

Exemplo hipotético. A senha de uma loja foi exposta e era a mesma do e-mail. Troque-a nos serviços em que foi reutilizada, começando pelas contas que permitem recuperar outras. Faça isso pelos aplicativos ou endereços oficiais, em um dispositivo confiável.

Dê atenção especial ao e-mail principal e à conta do sistema do telefone. Quem obtém esses acessos pode tentar redefinir outras senhas. Mantenha os meios de recuperação atualizados e não aprove solicitações de acesso que você não iniciou (CERT.br, 2022a).

3.2 Acrescente proteção ao acesso

A verificação em duas etapas acrescenta uma confirmação ao acesso à conta. Dependendo do serviço, pode utilizar um aplicativo autenticador, uma chave de segurança ou outro recurso. Ative uma opção adequada às suas condições e aprenda como recuperar o acesso se perder o celular.

Quando houver alternativas disponíveis, prefira métodos mais resistentes a golpes e ao uso indevido da linha telefônica. Códigos recebidos por mensagem exigem cuidado especial. Eles não devem ser repassados a quem liga ou escreve, mesmo quando a pessoa afirma trabalhar para o serviço.

Um pedido de aprovação no telefone também merece atenção. Se você não está tentando entrar na conta, recuse a solicitação e confira a segurança pelo canal oficial. Não aprove várias notificações apenas para fazê-las parar.

Exemplo hipotético. Alguém pede o código que acabou de chegar, dizendo que o enviou por engano. Esse código pode autorizar o acesso à sua conta. Não o informe. Interrompa a conversa e confira eventuais alertas diretamente no serviço.

Proteja os códigos de recuperação fornecidos ao configurar a segurança. Guarde-os de forma segura, com possibilidade de consulta se o aparelho ficar indisponível. Não os inclua nos checklists desta cartilha nem os envie a um suposto atendente (CERT.br, 2022a; 2026b).

3.3 Confira quem continua conectado

Muitos serviços mantêm o acesso depois que a senha é digitada. Por isso, trocar a senha pode não encerrar automaticamente todas as sessões existentes. Consulte a área de segurança, revise aparelhos conectados e encerre os acessos desconhecidos pelos recursos disponíveis.

Confira o telefone e o e-mail cadastrados para recuperação. Um endereço antigo, ao qual você não tem mais acesso, pode dificultar a retomada da conta. Ao trocar de número, revise os serviços em que ele era utilizado antes de abandonar a linha.

Se o serviço oferecer chaves de acesso, conhecidas como passkeys, consulte suas instruções oficiais. Elas utilizam mecanismos criptográficos ligados ao serviço para autenticar o acesso, sem exigir que você entregue uma senha digitada a uma página. Ainda assim, a segurança do aparelho e a recuperação da conta continuam importantes (Apple, 2024).

Orientação prática. Faça uma lista das contas essenciais e registre apenas quais precisam de revisão. Não anote suas credenciais nessa lista. Comece pelo e-mail principal, pela conta do sistema do celular e pelos serviços financeiros.

Desconfie de quem promete recuperar uma conta mediante pagamento antecipado e exige códigos ou acesso remoto. Utilize o procedimento oficial do serviço. Uma invasão pode ser seguida de outro golpe contra a pessoa que tenta recuperar seu acesso (CERT.br, 2022a; 2026a).

CAPÍTULO 4

WhatsApp e aplicativos de mensagens

4.1 Foto e nome não confirmam quem está falando

Uma pessoa pode copiar sua fotografia e criar um perfil para pedir dinheiro aos seus contatos. Também pode utilizar uma conta que foi comprometida. A mensagem parecer vir de alguém conhecido não basta para confirmar um pedido inesperado.

Se um contato anuncia novo número, confirme por um meio que já utilizava. Para um pedido urgente de dinheiro, procure falar diretamente com a pessoa e esclareça a situação. Se ela não puder atender, a dificuldade de confirmação é motivo para adiar o pagamento.

Exemplo hipotético. Uma mensagem com a foto de sua filha diz que o telefone quebrou e pede uma transferência para terceiro. Ligue para o número habitual ou fale com outro familiar de confiança. Não use apenas o contato recém-apresentado para confirmar a história.

Evite repassar códigos recebidos por mensagem, aceitar convites suspeitos ou permitir que outra pessoa cadastre sua conta em um aparelho. A proteção precisa alcançar tanto a entrada inicial quanto os dispositivos que continuam conectados.

A família pode combinar que pedidos de pagamento serão confirmados antes de qualquer transferência. A combinação deve incluir a possibilidade de esperar. Uma palavra combinada pode ajudar, mas não deve ser o único critério, pois pode ser descoberta ou revelada em uma conversa (CERT.br, 2026b).

4.2 Revise a privacidade e os dispositivos conectados

Nas configurações do aplicativo, procure as opções de privacidade, verificação adicional e aparelhos conectados. Os nomes dos menus podem mudar. Use a ajuda oficial para localizar os recursos e evite instruções recebidas de desconhecidos para “consertar” a conta.

Restrinja a exibição de informações pessoais conforme suas necessidades. Também confira quem pode adicioná-lo a grupos. Participar de um grupo não significa que todos os integrantes ou administradores foram identificados de forma confiável.

No uso de computadores compartilhados, tenha cuidado com sessões que ficam abertas. Encerre a sessão quando terminar e confira depois os dispositivos autorizados. Não leia um código apresentado por outra pessoa para vincular sua conta sem compreender o que está autorizando.

Exemplo hipotético. Uma pessoa oferece uma promoção e pede que você aponte a câmera para um código a fim de “validar o cadastro”. Se isso envolver vincular sua conta ou autorizar acesso, o efeito pode ser diferente do anunciado. Não prossiga por pressão ou promessa de vantagem.

Ao perceber uso indevido, utilize a recuperação oficial e avise seus contatos por outro canal. Denuncie a conta ou a mensagem na plataforma. Preserve o material disponível sem continuar conversando com o fraudador para obter novas informações (CERT.br, 2022a; 2026a; 2026b).

CAPÍTULO 5

Redes sociais e exposição de informações

5.1 Publique considerando quem poderá ver

Uma publicação pode revelar mais do que o assunto principal. Uma fotografia pode mostrar endereço, uniforme escolar, documentos, telas de trabalho ou hábitos da família. Depois de compartilhada, ela pode ser copiada e circular fora do público originalmente escolhido.

Antes de publicar, examine o fundo da imagem e o contexto. Evite divulgar documentos, passagens com códigos legíveis e informações que facilitem acessar contas ou acompanhar sua rotina. Considere publicar registros de viagem depois de retornar, em vez de anunciar continuamente a ausência de casa.

Exemplo hipotético. Uma fotografia de matrícula escolar mostra nome completo, escola e horário de saída. Esses detalhes podem ser utilizados para criar uma mensagem que pareça vir da instituição. É possível compartilhar a conquista sem expor o documento.

As opções de perfil privado ajudam a limitar o público, mas não impedem que alguém copie o conteúdo. Revise seguidores, marcações e visibilidade de publicações antigas. Peça autorização antes de divulgar imagens ou informações de outras pessoas.

A exposição nunca justifica violência ou fraude. O cuidado serve para reduzir informações disponíveis a quem pretende abusar delas, preservando o direito de utilizar a internet e de buscar ajuda quando necessário (CERT.br, 2023d; 2023e).

5.2 Desconfie também de perfis bem apresentados

Número de seguidores, comentários positivos e aparência profissional podem ser manipulados. Um perfil antigo também pode mudar de controle. Antes de comprar, doar ou entregar dados, procure uma confirmação ligada à instituição ou à pessoa por outro caminho confiável.

Tenha cuidado com testes, sorteios e formulários que pedem informações sem finalidade clara. Nome de familiares, telefone e dados sobre hábitos podem ser usados em novas abordagens. A curiosidade sobre um resultado não precisa custar a exposição de sua vida pessoal.

Exemplo hipotético. Um perfil imita uma loja e anuncia que você ganhou um prêmio, mas exige pagamento de frete e fotografia de documento. Confira a promoção no site ou no aplicativo oficial da empresa. Não envie material para o perfil apenas porque ele utiliza a marca conhecida.

Para denunciar uma publicação, use os recursos da própria plataforma. Evite divulgar novamente o endereço do golpe ou dados de vítimas ao tentar alertar outras pessoas. Um aviso pode explicar o mecanismo sem ampliar a exposição.

Se alguém se passa por você, reúna as informações já disponíveis e avise seus contatos. Não procure invadir a conta falsa, negociar com seu responsável ou realizar uma investigação particular. O caminho é proteger seus acessos, denunciar e procurar as autoridades quando cabível (CERT.br, 2023e; 2026a).

CAPÍTULO 6

Compras pela internet com mais segurança

6.1 Confira a loja antes do pagamento

Compare preço, condições de entrega e identificação do fornecedor. Uma oferta muito diferente das demais exige verificação adicional. Desconfie quando o desconto depende de pagamento imediato e não há tempo para conferir a loja.

Acesse o comércio pelo endereço que conhece ou pelo aplicativo oficial. Resultados de busca e anúncios podem levar a páginas falsas. O cadeado e o uso de HTTPS indicam proteção da conexão, mas não demonstram, sozinhos, que a loja é confiável.

Pesquise referências em mais de uma fonte. Confira se o endereço, o contato e os dados do fornecedor são coerentes. A simples presença de um CNPJ ou de avaliações no próprio site não resolve a verificação, pois informações verdadeiras podem ter sido copiadas.

Exemplo hipotético. Um anúncio vende um eletrodoméstico muito abaixo do preço comum e aceita apenas transferência para uma pessoa física sem relação esclarecida com a loja. Não pague enquanto a diferença não for explicada por um canal confiável.

Leia as regras de entrega e atendimento. Guarde a oferta, o pedido e os comprovantes da compra. Esses registros ajudam a esclarecer problemas, mas não substituem a escolha cuidadosa do fornecedor nem garantem recuperação de valores em caso de fraude (CERT.br, 2023c; 2026b).

6.2 Mantenha a compra no ambiente oficial

Quando comprar por uma plataforma, converse e pague pelos recursos previstos nela. Um pedido para sair do ambiente e obter desconto pode eliminar proteções disponíveis e dificultar a identificação do que ocorreu. Confira as condições aplicáveis antes de autorizar o pagamento.

Desconfie de cobranças adicionais recebidas por outro canal, como uma suposta taxa para liberar a entrega. Consulte o pedido no aplicativo oficial e fale com o atendimento que você mesmo localizou. Não use apenas o telefone ou o endereço indicado na cobrança suspeita.

Se utilizar cartão virtual, conheça suas opções de limite, bloqueio e uso recorrente. Não presuma que o recurso impeça qualquer fraude. Continue conferindo as compras e notificações. Nunca envie fotografia do cartão para concluir um atendimento.

Exemplo hipotético. Depois da compra, chega mensagem dizendo que o pagamento falhou e deve ser repetido por Pix. Confira primeiro o pedido e o extrato. Fazer novo pagamento sem essa verificação pode gerar prejuízo adicional.

Atraso, defeito e divergência comercial devem ser tratados pelos canais de atendimento e de proteção ao consumidor pertinentes. Nem todo problema de compra constitui golpe. Quando houver sinais de fraude, comunique também a instituição financeira e procure o registro policial adequado (CERT.br, 2023b; 2023c; 2026a).

CAPÍTULO 7

Pix e pagamentos digitais

7.1 Confira a operação antes de autorizar

Antes de confirmar um pagamento, leia o valor e os dados do destinatário na tela do aplicativo. Verifique se correspondem à compra ou à pessoa que você pretende pagar. Não ignore uma divergência porque o interlocutor explica que a conta é “do financeiro” ou “de um parente”.

Se a operação foi motivada por um pedido inesperado, confirme também a história. Um nome correto no aplicativo identifica o recebedor apresentado na transação, mas não demonstra que a cobrança é devida ou que o contato é legítimo.

Ajuste os limites de pagamento e transferência às suas necessidades. Ative notificações e confira movimentações. Para operações financeiras, prefira o próprio aparelho atualizado e uma conexão de confiança. Uma rede pública com nome conhecido pode ser imitada; não presuma que o nome da rede comprova sua origem.

Exemplo hipotético. Uma pessoa oferece ajuda para aumentar seu limite e pede acesso à tela enquanto você entra no banco. Interrompa o atendimento e procure a instituição por um canal oficial. Não instale aplicativos indicados durante uma chamada recebida nem autorize acesso remoto ao aparelho.

Proteções do sistema financeiro ajudam a reduzir riscos, mas não dispensam a conferência do contexto e dos dados de cada operação (CERT.br, 2023b; 2026b).

7.2 O banco não precisa de uma transferência de teste

Um falso atendente pode alegar compra suspeita, invasão de conta ou necessidade de “proteger” seu saldo. A abordagem procura levar você a transferir dinheiro, entregar códigos ou instalar um programa. Encerre o contato e abra o atendimento do banco por conta própria.

Não transfira valores para uma suposta conta segura indicada pelo interlocutor. Também não faça operações menores para cancelar uma maior ou testar um sistema. Uma orientação recebida pode estar disfarçando o próprio pagamento do golpe.

Ao vender algo, confira o crédito no aplicativo ou no extrato. Uma imagem de comprovante pode ser falsa. Observe se o valor foi efetivamente recebido, sem confundir agendamento ou documento enviado pelo comprador com dinheiro disponível.

Exemplo hipotético. Alguém afirma ter enviado Pix por engano e pede devolução para outra conta. Primeiro confirme o crédito no seu banco e procure orientação da instituição. Se houver devolução cabível, utilize a função vinculada à transação original, conforme as instruções oficiais. Não faça um novo Pix para a conta indicada pelo desconhecido.

Evite ceder sua conta para receber ou repassar valores de terceiros que você não compreende. Uma promessa de comissão pode envolver movimentações fraudulentas e expor você a prejuízos e à necessidade de esclarecer o uso da conta (CERT.br, 2023b; 2026b; 2026c).

7.3 Se houve fraude financeira, procure o banco imediatamente

Ao identificar uma operação fraudulenta, entre em contato imediatamente com a instituição financeira por seus canais oficiais. Descreva o ocorrido, identifique as transações e peça a contestação e a análise dos mecanismos cabíveis de bloqueio ou recuperação. Anote o protocolo.

No Pix, o Mecanismo Especial de Devolução, chamado MED, é uma ferramenta destinada a ajudar vítimas de fraude a tentar recuperar valores. Utilize a contestação disponível no aplicativo ou o atendimento oficial da instituição. A recuperação depende da análise do caso e da disponibilidade de recursos, e pode não ocorrer integralmente.

O MED não é um estorno garantido nem a solução para qualquer problema de compra. Desacordos comerciais e um Pix enviado por erro, sem fraude, têm

tratamento diferente. Informe os fatos com precisão, sem alterar a descrição para tentar enquadrar a situação no mecanismo.

Na prática. Não espere reunir todos os documentos ou registrar a ocorrência para comunicar a fraude ao banco. Guarde comprovantes e registre também o fato perante a polícia. São providências com funções distintas.

Se o atendimento não resolver a questão, procure a ouvidoria e os canais de reclamação pertinentes, inclusive órgãos de proteção ao consumidor. Uma reclamação também não constitui promessa de restituição (Banco Central do Brasil, [2026?]; CERT.br, 2026a).

CAPÍTULO 8

Links e QR Codes suspeitos

8.1 Não use o próprio aviso para conferir o aviso

Uma mensagem pode informar bloqueio de conta, dívida, entrega pendente ou benefício a receber. O endereço incluído nela pode levar a uma página que imita a instituição. A verificação deve começar fora da mensagem, pelo aplicativo ou pelo endereço oficial que você já conhece.

Não é preciso abrir um link suspeito para descobrir se ele é perigoso. Se a informação pode ser conferida de outra forma, use esse caminho. Um botão com o nome de uma empresa pode apontar para outro destino, e um endereço encurtado pode ocultar sua origem.

Exemplo hipotético. Um aviso diz que você deve regularizar um documento hoje para evitar multa. Em vez de abrir o endereço recebido, consulte o serviço diretamente pelo portal oficial. Não telefone para um número fornecido no próprio aviso como única forma de confirmação.

Tenha o mesmo cuidado com anexos e convites para instalar programas. Um arquivo apresentado como boleto, fotografia ou atualização pode produzir efeitos diferentes dos anunciados. Se não esperava o material, confirme sua origem antes de qualquer abertura.

Se já abriu uma página, pare e avalie o que ocorreu: informou senha, baixou arquivo, instalou aplicativo ou autorizou algo? Essa diferença ajuda a orientar a resposta do capítulo 11. Apenas ter visto uma página não comprova que houve invasão (CERT.br, 2026a; 2026b).

8.2 Um código pode levar a uma página ou a um pagamento

O QR Code facilita acessar informações e iniciar pagamentos. O desenho, porém, não permite saber se o destino é legítimo. A confiança precisa estar na origem do código e na conferência do que o aplicativo apresenta antes da autorização.

Em locais públicos, observe sinais de substituição, como um adesivo sobre outro. Se houver dúvida, não leia o código para “testar”. Fale com o estabelecimento e procure uma forma de acesso ou pagamento confirmada por ele.

Ao pagar por QR Code de origem confiável, confira os dados exibidos no aplicativo financeiro. Leia valor e recebedor. Se não corresponderem à operação, interrompa e esclareça a diferença antes de autorizar. A aparência do cartaz não substitui essa conferência.

Exemplo hipotético. Uma placa de estacionamento contém um código que leva a uma cobrança em nome estranho ao serviço. Não conclua a operação apenas porque o código está fixado no local. Procure um canal oficial do responsável pelo estacionamento.

Lembre-se também de que códigos podem servir para vincular dispositivos ou autorizar acesso a contas. Leia a finalidade apresentada na tela. Não utilize o código de outra pessoa durante uma chamada de suposto suporte sem compreender o efeito da autorização (CERT.br, 2026b).

CAPÍTULO 9

Inteligência artificial e novos golpes

9.1 Uma voz conhecida também precisa de confirmação

Ferramentas de inteligência artificial podem produzir textos convincentes e manipular vozes, imagens e vídeos. Uma gravação pode imitar um familiar ou apresentar uma pessoa conhecida fazendo uma oferta que ela nunca realizou. O conteúdo também pode misturar partes verdadeiras e falsas.

Não dependa apenas de erros visuais ou de uma voz estranha para identificar fraude. Se houver pedido de dinheiro, segredo, código ou ação urgente, confirme por outro meio. Uma chamada de vídeo, isoladamente, também não elimina a necessidade de verificar o contexto.

Exemplo hipotético. Um áudio com voz semelhante à de um parente relata uma emergência e exige transferência imediata. Interrompa o pagamento e procure o familiar por outro canal, ou fale com alguém que possa esclarecer a situação. Se houver risco real à integridade de alguém, busque também ajuda emergencial adequada.

Uma palavra combinada em família pode ser apoio adicional, mas não substitui a conferência. Evite usar como resposta uma informação que já aparece em redes sociais. Não revele o combinado a um contato cuja identidade ainda é incerta.

A prevenção não exige dominar a tecnologia usada na falsificação. Ela depende de conservar a possibilidade de verificar antes de entregar dinheiro, dados ou acesso (CERT.br, 2026b; 2026c).

9.2 Proteja seus dados ao conversar com uma IA

Ao utilizar um serviço de inteligência artificial, considere quais informações está enviando e quais ações está autorizando. Evite inserir senhas, dados completos de cartão, documentos pessoais e informações íntimas da família sem necessidade e sem compreender o tratamento oferecido.

Prefira descrever situações com informações genéricas quando a identificação não for necessária. Revise as opções de privacidade e as permissões. Uma configuração de histórico não deve ser interpretada, sozinha, como garantia de sigilo de tudo o que foi enviado.

A ferramenta pode apresentar respostas incorretas e fontes inexistentes. Confira informações importantes diretamente em fontes confiáveis, sobretudo antes de decisões sobre dinheiro, direitos ou saúde. Uma redação segura e bem organizada não comprova que o conteúdo está correto.

Exemplo hipotético. Uma resposta indica um endereço de atendimento para resolver uma dívida. Confirme o canal no site oficial da instituição antes de fornecer qualquer dado. Não utilize o contato apenas porque foi apresentado pela ferramenta.

Se uma aplicação puder agir em seu nome, limite as permissões e revise o que será feito antes de autorizar pagamentos, publicações ou exclusões. O uso de IA deve continuar sob seu controle, com atenção ao conteúdo e às consequências da ação (CERT.br, 2026c).

CAPÍTULO 10

Como proteger crianças e pessoas idosas

10.1 Ensine a pedir ajuda sem medo

Com crianças e adolescentes, combine regras compreensíveis sobre contatos, compras, publicações e pedidos de ajuda. Explique por que certas configurações são necessárias e ajuste o acompanhamento à idade e às necessidades. O controle parental pode ajudar, mas não substitui a conversa.

Mostre que uma pessoa desconhecida pode apresentar nome, idade e fotografia que não correspondem à realidade. Oriente a interromper pedidos de segredo, dinheiro, imagens íntimas ou encontro sem conhecimento dos responsáveis. Reforce que contar um problema não é motivo para humilhação.

Exemplo hipotético. Um participante de jogo oferece vantagem e pede conversa fora da plataforma. O responsável pode ouvir o relato, conferir o contexto com a criança e utilizar as opções de proteção e denúncia. Não é necessário provocar o contato ou fingir ser a criança para investigar por conta própria.

Tenha cuidado também com o que os adultos publicam sobre os filhos. Escola, horários, documentos e imagens da intimidade merecem proteção. Considere a dignidade e a privacidade de quem ainda está aprendendo a decidir sobre sua exposição.

Se houver violência ou ameaça, acolha e procure os serviços de proteção e as autoridades competentes. Não reproduza nem redistribua imagens de abuso sexual de crianças e adolescentes. Preserve as demais informações disponíveis de modo seguro, sem investigar o material por conta própria (CERT.br, 2022b; 2023d; 2023e).

10.2 Ajude preservando a autonomia

Apoiar uma pessoa idosa exige conhecer suas dificuldades concretas, sem presumir incapacidade pela idade. Letras pequenas, excesso de avisos e interfaces confusas podem atrapalhar qualquer usuário. Ajustes de acessibilidade e uma explicação tranquila tornam o uso mais compreensível.

Ofereça ajuda para revisar notificações, contatos oficiais, limites financeiros e formas de recuperação. Sempre que possível, deixe a própria pessoa executar a ação, explicando cada etapa. Não concentre senhas e decisões nas mãos de alguém apenas porque se apresentou como quem entende de tecnologia.

Exemplo hipotético. Uma pessoa recebe ligação sobre uma cobrança e pede ajuda ao filho. Ele pode orientá-la a encerrar a chamada e abrir o atendimento do banco por um canal conhecido, sem ridicularizar a dúvida nem assumir permanentemente o controle da conta.

Combine que pedidos urgentes de dinheiro serão conferidos e que qualquer familiar poderá pedir uma segunda opinião. Escolha pessoas de confiança e mantenha mais de uma forma de contato. Ninguém precisa decidir sozinho sob pressão.

Se houver prejuízo, a prioridade é proteger a pessoa e agir rapidamente. Evite cobranças e acusações que dificultem o relato. O apoio deve facilitar a comunicação com banco, plataforma e polícia, conforme a situação, sem prometer recuperação de valores (CERT.br, 2026a; 2026b).

CAPÍTULO 11

Fui vítima de um golpe. E agora?

11.1 Interrompa o dano e procure o canal correto

Pare de enviar dinheiro, códigos e documentos. Interrompa o contato suspeito. Não negocie uma suposta liberação de valores e não pague a quem promete recuperar tudo mediante nova transferência. Utilize outro dispositivo confiável se houver suspeita de controle indevido do seu aparelho.

Se houve pagamento ou acesso bancário exposto, comunique imediatamente a instituição financeira. Peça a contestação e as medidas cabíveis para proteger contas e cartões. No Pix, solicite a análise pelo MED quando pertinente. Guarde protocolos, mas não espere ter toda a documentação para pedir atendimento.

Se informou uma senha, altere-a no canal oficial e nas contas em que foi reutilizada. Revise meios de recuperação, verificação em duas etapas e sessões abertas. Se perdeu o acesso, siga a recuperação oficial. Avise contatos quando alguém puder estar usando sua identidade.

Se o celular foi furtado. Em local seguro, procure bloquear acessos financeiros e comunicar a operadora para desativar a linha e solicitar bloqueio do aparelho. Utilize os recursos oficiais de bloqueio remoto disponíveis. O bloqueio do IMEI não encerra automaticamente contas e acessos pela internet.

Registre a ocorrência policial pelo meio adequado ao caso. Em situação de risco físico, priorize a segurança e a ajuda imediata. Não vá ao local apontado no mapa para confrontar quem está com o telefone (Banco Central do Brasil, [2026?]; CERT.br, 2024; 2026a).

11.2 Guarde o que já está disponível e acompanhe

Conserve mensagens, comprovantes, nomes de perfis, números utilizados e protocolos que já estejam disponíveis. Registre datas, horários e a sequência do ocorrido. Não retorne ao endereço suspeito nem continue conversando com o fraudador apenas para conseguir mais informações.

Mantenha os arquivos de origem disponíveis e guarde cópias de forma protegida. Uma captura de tela pode ajudar a explicar a situação, mas não esclarece sozinha todos os fatos. Evite editar o material ou publicá-lo com dados de vítimas e terceiros. A investigação e a análise técnica cabem aos profissionais competentes.

Se instalou um aplicativo suspeito ou permitiu acesso remoto, interrompa o uso do aparelho para operações sensíveis e procure assistência confiável. Pode ser necessário restaurar o sistema, o que apaga dados. Antes disso, obtenha orientação sobre preservação das informações e recuperação de cópias seguras, sem atrasar a proteção das contas.

Acompanhamento. Revise extratos, cartões e alertas de acesso nos dias seguintes. Conteste operações que não reconhece e acompanhe os protocolos. A ausência de nova cobrança imediata não garante que os efeitos terminaram.

Procure a plataforma, os órgãos de proteção ao consumidor e orientação jurídica quando necessários. Se o caso envolver imagens de abuso sexual de crianças ou adolescentes, não as copie nem redistribua; procure as autoridades e os serviços de proteção (CERT.br, 2026a; Jorge, 2027).

CAPÍTULO 12

Vinte hábitos de segurança digital

12.1 Cuidados com contas e aparelhos

Os hábitos abaixo reúnem medidas desenvolvidas nos capítulos anteriores. Adote-os conforme suas necessidades e revise o que ainda não conseguiu configurar.

1. Bloqueie a tela com senha difícil de deduzir e mantenha uma senha de reserva adequada à biometria.
2. Instale atualizações pelos recursos oficiais do sistema e dos aplicativos.
3. Confira o desenvolvedor antes de instalar um aplicativo e revise as permissões concedidas.
4. Use senhas diferentes para as contas, com atenção especial ao e-mail principal.
5. Ative a verificação adicional disponível e guarde meios de recuperação em local seguro.
6. Recuse pedidos de aprovação de acesso que você não iniciou.
7. Revise dispositivos conectados e encerre sessões desconhecidas ou que não utiliza mais.
8. Faça cópias de segurança e confira se consegue recuperar as informações importantes.
9. Prepare formas de bloqueio remoto e mantenha a identificação do celular fora dele.
10. Reduza o conteúdo sensível exibido na tela bloqueada e evite guardar senhas em mensagens ou fotografias.

Não é necessário fazer tudo de uma vez. Comece pelas contas essenciais e reserve tempo para concluir as demais medidas (CERT.br, 2022a; 2022b; 2023a; 2024).

12.2 Cuidados com pedidos e pagamentos

11. Confirme pedidos inesperados por um canal escolhido por você, sem depender do contato suspeito.
12. Não entregue senhas, códigos de acesso ou de recuperação a quem entra em contato.
13. Confira valor, recebedor e motivo antes de autorizar um pagamento.
14. Ajuste limites financeiros e acompanhe movimentações e notificações.
15. Mantenha compras e pagamentos no ambiente oficial utilizado para a contratação.
16. Não abra links, arquivos ou QR Codes suspeitos para descobrir se são perigosos.
17. Examine o que aparece nas fotografias e preserve informações da rotina familiar.
18. Verifique pedidos mesmo quando utilizem voz, imagem ou nome de alguém conhecido.
19. Combine formas de pedir ajuda, respeitando a autonomia e a privacidade de cada pessoa.
20. Ao perceber incidente, interrompa o dano, comunique os canais competentes e acompanhe as providências.

O objetivo é conservar a possibilidade de conferir antes de agir e de buscar ajuda quando necessário. Nenhum hábito impede todos os incidentes, mas a combinação de cuidados reduz oportunidades para o golpe e facilita uma resposta mais rápida (CERT.br, 2023b; 2023c; 2023d; 2026a; 2026b; 2026c).

Considerações finais

A proteção digital deve caber na rotina. Uma senha bem escolhida, uma conta com recuperação preparada e uma pausa antes de uma transferência são decisões que podem ser repetidas sem conhecimento técnico especializado.

A família pode ajudar tornando a dúvida um assunto permitido. Quando uma pessoa sabe que pode consultar outra sem ser ridicularizada, fica mais fácil interromper um pedido suspeito. Esse apoio também precisa respeitar a privacidade e a autonomia de quem utiliza os serviços.

Os aplicativos mudam, e algumas configurações podem ter nomes diferentes dos utilizados por quem oferece ajuda. Procure as orientações oficiais e compreenda o efeito da ação antes de confirmar. Uma autorização para conectar outro aparelho ou controlar a tela pode ter consequências maiores do que a promessa apresentada.

Se ocorrer um incidente, concentre-se nas providências possíveis. Comunique rapidamente a instituição financeira quando houver fraude, proteja os acessos e registre o fato pelos canais adequados. Guardar as informações disponíveis e acompanhar os protocolos ajuda a organizar a resposta.

Os materiais seguintes transformam a leitura em conferências práticas. Use-os para começar, identificar pendências e combinar como pedir ajuda. A segurança se fortalece quando os cuidados passam a fazer parte do uso cotidiano da internet.

APÊNDICE A

Plano de proteção em 15 minutos

Este é um começo, não uma revisão completa. Se uma configuração exigir mais tempo, conclua-a com calma e re programe as demais. Não faça este roteiro se houver incidente em andamento: procure o capítulo 11.

Minutos 0 a 3

Confira senha de bloqueio, bloqueio automático e exposição de mensagens na tela. Identifique atualizações pendentes e programe a instalação pelo sistema oficial.

Minutos 3 a 6

Revise o e-mail principal e a conta do sistema do telefone. Confira se conhece a senha e se os meios de recuperação estão atualizados.

Minutos 6 a 9

Confira a verificação adicional da conta prioritária. Se ainda não estiver ativa, inicie a configuração oficial e proteja os códigos de recuperação.

Minutos 9 a 12

Localize o contato oficial do banco fora de mensagens recebidas. Revise limites e alertas financeiros. Não faça uma transferência para testar.

Minutos 12 a 15

Combine como a família confirmará pedidos de dinheiro e pedirá ajuda. Anote uma pendência concreta e uma data para resolvê-la.

Minha próxima providência e data

Fonte: instrumento próprio, com base nos capítulos 2, 3, 7 e 10. Não registre senhas ou códigos nesta página.

APÊNDICE B

Checklist de segurança do celular

Marque apenas o que conferiu. Se precisar de ajuda, utilize os recursos oficiais ou uma pessoa de confiança, preservando suas credenciais.

- ☐ A senha de bloqueio não é uma data ou sequência previsível.
- ☐ O bloqueio automático está configurado.
- ☐ Mensagens sensíveis não ficam expostas na tela bloqueada.
- ☐ As atualizações são obtidas pelos recursos oficiais.
- ☐ Os aplicativos instalados e seus desenvolvedores foram revistos.
- ☐ As permissões correspondem às funções utilizadas.
- ☐ A conta principal tem meios de recuperação atualizados.
- ☐ A verificação adicional foi conferida nas contas essenciais.
- ☐ Os dispositivos conectados foram revisados.
- ☐ Há cópia de segurança dos dados importantes.
- ☐ Um arquivo de teste pôde ser recuperado da cópia.
- ☐ Os recursos de bloqueio remoto foram preparados.
- ☐ O IMEI e a documentação estão guardados fora do celular.
- ☐ Os contatos oficiais de atendimento podem ser obtidos sem o aparelho.

Pendência, ajuda necessária e data da próxima revisão

Fonte: capítulos 2 e 3. Checklist de apoio, sem garantia de ausência de risco. Não anote senhas, códigos ou números de cartão.

APÊNDICE C

Dez sinais de alerta para golpes

Um sinal isolado não comprova fraude. Se houver dúvida, interrompa a ação e confira por um canal independente.

1. Pressão para pagar ou decidir imediatamente.
2. Pedido para guardar segredo ou não consultar ninguém.
3. Solicitação de senha, código ou aprovação de acesso.
4. Indicação de uma “conta segura” para transferir dinheiro.
5. Pedido para instalar programa ou permitir controle da tela.
6. Novo número de familiar acompanhado de pedido financeiro.
7. Recebedor ou valor diferente do que você esperava pagar.
8. Cobrança fora da plataforma ou por canal não confirmado.
9. Oferta excepcional condicionada à entrega urgente de dados.
10. Promessa de recuperar um prejuízo mediante novo pagamento.

O que fazer: Pare o pagamento ou a entrega de informações. Encerre o contato suspeito e procure o canal oficial por conta própria. Se não conseguir confirmar, adie a ação. Não abra um endereço suspeito para testá-lo.

Fonte: capítulos 1, 4, 6, 7 e 9. Exemplos de sinais, sem lista exaustiva de mecanismos de fraude.

APÊNDICE D

Primeiras 24 horas após um incidente

Não espere completar 24 horas para agir. Algumas providências são imediatas e podem ser divididas com uma pessoa de confiança.

Interrompa o dano

Pare de enviar dinheiro, códigos e documentos. Se houver suspeita de controle do aparelho, use outro dispositivo confiável para buscar atendimento.

Avise a instituição financeira

Em fraude financeira, comunique o banco imediatamente. Peça contestação, proteção dos acessos e análise dos mecanismos cabíveis de recuperação. Guarde o protocolo. Não há garantia de restituição.

Proteja contas e linha

Revise senhas expostas, meios de recuperação e sessões. Se o telefone foi furtado, comunique a operadora e solicite as medidas de bloqueio. Não tente recuperá-lo pessoalmente.

Registre e acompanhe

Guarde o material já disponível, registre a ocorrência policial e utilize a denúncia da plataforma. Anote providências, protocolos e pendências. Não volte a contatar o golpista para buscar provas.

Providência prioritária, responsável e protocolo

Fonte: capítulo 11. Não copie nem redistribua imagens de abuso sexual de crianças e adolescentes; procure as autoridades e os serviços de proteção.

APÊNDICE E

Página para compartilhar com a família

Antes de pagar ou informar dados

Confirme quem está pedindo e por quê. Use um contato ou aplicativo que você escolheu por outro caminho confiável. Foto, nome e voz conhecidos não bastam.

Não entregue códigos. Não transfira para uma suposta conta de proteção. Não instale programas nem permita controle da tela por orientação de uma ligação recebida.

Para manter os acessos protegidos

Use senhas diferentes, verificação adicional e meios de recuperação preparados. Atualize o celular, bloqueie a tela e mantenha cópias de segurança.

Para pedir ajuda

Combine que toda pessoa da família pode interromper um pedido e consultar alguém, sem vergonha. Crianças e pessoas idosas precisam de apoio respeitoso, com cuidado à privacidade e à autonomia.

Se algo acontecer

Interrompa o contato suspeito. Em fraude financeira, fale com o banco imediatamente. Proteja as contas, guarde as informações disponíveis e registre o fato. Não pague a quem promete recuperar tudo.

Pessoas de confiança para procurar

Fonte: síntese da cartilha. Não registre senhas nesta página. A versão resumida está no Apêndice F.

APÊNDICE F

Resumo para compartilhar

Confira antes de agir

Um pedido inesperado precisa de confirmação

Foto, nome, voz e vídeo podem ser imitados. Se alguém pedir dinheiro, código ou segredo, interrompa a ação e confirme por outro canal confiável. Procure a pessoa pelo número habitual ou abra o aplicativo oficial por conta própria. Não use apenas o contato indicado na mensagem suspeita.

Se não conseguir confirmar, espere. Não envie uma pequena quantia para testar. Uma emergência alegada não obriga você a decidir durante a ligação.

Cuide do celular e das contas

Bloqueie a tela e reduza mensagens sensíveis exibidas com o telefone bloqueado. Atualize o sistema e os aplicativos pelos recursos oficiais. Confira o desenvolvedor e as permissões antes de instalar um programa.

Use senhas longas e diferentes. Ative a verificação adicional disponível e prepare meios de recuperação. Recuse aprovações de acesso que você não iniciou. Revise aparelhos conectados e mantenha cópias de segurança que possam ser recuperadas.

Confira compras e pagamentos

Verifique valor, recebedor e motivo antes de autorizar. Mantenha a negociação e o pagamento no ambiente oficial. Desconfie de cobrança fora da plataforma. O cadeado do navegador não comprova que uma loja é honesta.

Não transfira para uma suposta conta de proteção e não permita controle da tela durante uma ligação recebida. Não abra links ou QR Codes suspeitos para descobrir se são perigosos.

Combine como pedir ajuda

Crianças, pessoas idosas e qualquer familiar devem poder tirar dúvidas sem humilhação. Respeite a privacidade e a autonomia. Não publique documentos, horários e imagens que exponham a intimidade da família.

Pessoa de confiança e canal para consultar

Síntese dos capítulos 1 a 10. Não anote senhas ou códigos nesta folha. A cartilha completa explica os cuidados e oferece instrumentos de conferência.

Se algo aconteceu, procure ajuda

Interrompa o dano e organize as providências

Um incidente pode acontecer com qualquer pessoa. Agir rapidamente e procurar o canal adequado ajuda a reduzir os efeitos. Não espere concluir todos os passos para comunicar uma fraude financeira ao banco.

1. Pare a ação suspeita

Interrompa o contato. Não envie novos valores, senhas, códigos ou documentos. Não pague a quem promete recuperar tudo mediante outra transferência. Se houver suspeita de controle do aparelho, use outro dispositivo confiável para buscar atendimento.

2. Fale com a instituição financeira imediatamente

Use o aplicativo ou um canal oficial que você escolheu por outro caminho confiável. Informe as operações e peça a contestação e as medidas cabíveis de proteção e recuperação. No Pix, solicite a análise pelo Mecanismo Especial de Devolução, o MED, quando pertinente.

A devolução não é garantida. Ela depende da análise do caso e da disponibilidade de recursos. O MED não resolve qualquer desacordo comercial nem todo Pix enviado por engano, sem fraude. Guarde o protocolo e acompanhe o atendimento.

3. Proteja os acessos

Se informou uma senha, troque-a no canal oficial e nas contas em que foi repetida. Revise recuperação, verificação adicional e sessões abertas. Se perdeu a conta, use a recuperação oficial e avise seus contatos por outro meio.

Se o celular foi furtado, priorize sua segurança. Procure bloquear acessos financeiros, comunicar a operadora e utilizar os recursos oficiais de bloqueio remoto. Não tente recuperar o aparelho pessoalmente.

4. Guarde as informações e acompanhe

Conserve mensagens, comprovantes, datas e protocolos já disponíveis. Não volte ao endereço suspeito nem continue conversando com o fraudador para obter material. Registre a ocorrência policial pelo meio adequado e utilize os recursos de denúncia da plataforma.

Se houver violência contra criança ou adolescente, acolha e procure os serviços de proteção e as autoridades. Não copie nem redistribua imagens de abuso sexual. Busque orientação sobre a preservação adequada das informações disponíveis.

Atendimento, protocolo e próxima providência

Fonte: capítulos 7 e 11 e referências do Volume 07, especialmente CERT.br e Banco Central do Brasil. Material gratuito para compartilhar. Cartilha completa e canais do autor: www.higorjorge.com.br.

Referências

APPLE. **Sobre a segurança das chaves de acesso**. [S. l.]: Apple, 30 set. 2024. Disponível em: <https://support.apple.com/pt-br/102195>. Acesso em: 12 out. 2026.

BANCO CENTRAL DO BRASIL. **Segurança no Pix**. Brasília, DF: Banco Central do Brasil, [2026?]. Versão eletrônica corrente, sem data editorial identificada. Disponível em: <https://www.bcb.gov.br/estabilidadefinanceira/pix-seguranca>. Acesso em: 13 ago. 2026.

CERT.br. **Autenticação**. [S. l.]: NIC.br, nov. 2022a. Fascículo da Cartilha de Segurança para Internet. Disponível em: <https://cartilha.cert.br/fasciculos/autenticacao/fasciculo-autenticacao.pdf>. Acesso em: 18 ago. 2026.

CERT.br. **Backup**. [S. l.]: NIC.br, maio 2023a. Fascículo da Cartilha de Segurança para Internet. Disponível em: <https://cartilha.cert.br/fasciculos/backup/fasciculo-backup.pdf>. Acesso em: 29 set. 2026.

CERT.br. **Banco via internet**. [S. l.]: NIC.br, abr. 2023b. Fascículo da Cartilha de Segurança para Internet. Disponível em: <https://cartilha.cert.br/fasciculos/banco-via-internet/fasciculo-banco-via-internet.pdf>. Acesso em: 18 jun. 2026.

CERT.br. **Celulares e tablets**. [S. l.]: NIC.br, out. 2022b. Fascículo da Cartilha de Segurança para Internet. Disponível em: <https://cartilha.cert.br/fasciculos/celulares-e-tablets/fasciculo-celulares-e-tablets.pdf>. Acesso em: 14 ago. 2026.

CERT.br. **Comércio via internet**. [S. l.]: NIC.br, nov. 2023c. Fascículo da Cartilha de Segurança para Internet. Disponível em: <https://cartilha.cert.br/fasciculos/comercio-via-internet/fasciculo-comercio-via-internet.pdf>. Acesso em: 19 set. 2026.

CERT.br. **Furto de celular**. [S. l.]: NIC.br, nov. 2024. Fascículo da Cartilha de Segurança para Internet. Disponível em: <https://cartilha.cert.br/fasciculos/furto-de-celular/fasciculo-furto-de-celular.pdf>. Acesso em: 14 out. 2026.

CERT.br. **Golpes: caiu? Veja o que fazer**. [S. l.]: NIC.br, maio 2026a. Fascículo da Cartilha de Segurança para Internet. Disponível em: <https://cartilha.cert.br/fasciculos/golpes-o-que-fazer/fasciculo-golpes-o-que-fazer.pdf>. Acesso em: 26 jun. 2026.

CERT.br. **Golpes: evite fraudes.** [S. l.]: NIC.br, mar. 2026b. Fascículo da Cartilha de Segurança para Internet. Disponível em: <https://cartilha.cert.br/fasciculos/golpes-evite-fraudes/fasciculo-golpes-evite-fraudes.pdf>. Acesso em: 9 ago. 2026.

CERT.br. **Inteligência artificial.** [S. l.]: NIC.br, set. 2026c. Fascículo da Cartilha de Segurança para Internet. Disponível em: <https://cartilha.cert.br/fasciculos/ia/fasciculo-ia.pdf>. Acesso em: 4 out. 2026.

CERT.br. **Privacidade.** [S. l.]: NIC.br, ago. 2023d. Fascículo da Cartilha de Segurança para Internet. Disponível em: <https://cartilha.cert.br/fasciculos/privacidade/fasciculo-privacidade.pdf>. Acesso em: 3 jul. 2026.

CERT.br. **Redes sociais.** [S. l.]: NIC.br, fev. 2023e. Fascículo da Cartilha de Segurança para Internet. Disponível em: <https://cartilha.cert.br/fasciculos/redes-sociais/fasciculo-redes-sociais.pdf>. Acesso em: 25 jul. 2026.

JORGE, Higor Vinicius Nogueira. **Investigação criminal tecnológica: fundamentos, método e limites na era dos vestígios informacionais.** 1. ed. Salvador: Juspodivm, 2027. ISBN 9788544277386.

Minicurrículo do autor

HIGOR VINICIUS NOGUEIRA JORGE

Delegado de Polícia da Polícia Civil do Estado de São Paulo, professor, escritor e pesquisador nas áreas de Direito, tecnologia, investigação criminal e inteligência cibernética. Autor e coordenador de mais de 80 obras jurídicas publicadas, integra o Conselho de Direito Digital, Transformação e Novas Tecnologias da Editora Juspodivm.

Mestre em Educação pela Universidade Estadual de Mato Grosso do Sul (UEMS) e graduado em Direito pelo Centro Universitário Toledo de Araçatuba (UniToledo/SP), é professor concursado da Academia de Polícia Dr. Coriolano Nogueira Cobra (Acadepol/SP). Possui pós-graduações em Polícia Comunitária (Unisul), Repressão e Prevenção à Corrupção (Faculdade Estácio), VANTs e Drones: Legislação, Planejamento e Aplicações (Uniminas), Cybercrime e Cybersecurity: Prevenção e Investigação de Crimes Digitais (Uniminas) e Investigação Digital (WB Educação).

Sua atuação acadêmica compreende o ensino, a pesquisa e a produção de conhecimento nas áreas de investigação criminal tecnológica, direito digital, crimes cibernéticos, inteligência cibernética, prova digital e aplicação de novas tecnologias à segurança pública. Além de sua atividade docente na Acadepol/SP, ministra aulas de inteligência cibernética no âmbito do Ministério da Justiça e Segurança Pública (MJSP). Também atuou em cursos de pós-graduação e programas de formação especializada de instituições como a Escola Brasileira de Direito (EBRADI), o Complexo de Ensino Renato Saraiva (CERS), a Escola Superior de Advocacia da OAB-SP (ESA-OAB/SP), a Escola da Magistratura do Estado do Rio de Janeiro (EMERJ), a Escola Mineira de Direito (EMD), o Damásio Educacional, a Verbo Jurídico, o MeuCurso, a WB Educação e a Associação dos Diplomados da Escola Superior de Guerra (ADESG, Campinas).

Em 2015, desenvolveu a disciplina Investigação Criminal Tecnológica, concebida como uma proposta teórico-metodológica voltada à aplicação sistemática, juridicamente fundamentada e tecnicamente controlada de recursos tecnológicos à investigação criminal. Diferentemente da investigação

de crimes cibernéticos, cujo objeto está relacionado às infrações penais praticadas no ambiente digital ou mediante o emprego de tecnologias, a Investigação Criminal Tecnológica possui abrangência transversal, aplicando-se à apuração de delitos de qualquer natureza. Sua abordagem compreende a identificação, a preservação, a obtenção, o tratamento, a correlação, a interpretação e a apresentação de vestígios informacionais relevantes à persecução penal, com observância das garantias fundamentais, dos requisitos de validade probatória e da cadeia de custódia.

Integra a Associação Internacional de Informática Forense (ASIIF) e a Associação Internacional de Investigação de Crimes de Alta Tecnologia (HTCIA). É titular da Cadeira nº 30 da Academia de Ciências, Artes e Letras dos Delegados de Polícia do Estado de São Paulo e Diretor de Relações Institucionais da Associação dos Delegados de Polícia do Estado de São Paulo (ADPESP), na gestão 2024-2026.

Entre 2017 e 2026, recebeu, em dez edições consecutivas, reconhecimento na categoria Jurídica do levantamento Melhores Delegados de Polícia do Brasil, promovido pelo Portal Nacional dos Delegados e pela Revista da Defesa Social.

Para aprofundar o estudo

Investigação criminal tecnológica

Fundamentos, método e limites na era dos vestígios informacionais

Higor Vinicius Nogueira Jorge. Salvador: Editora Juspodivm, 1ª edição, ano editorial 2027. ISBN 9788544277386.

O livro apresenta a Investigação Criminal Tecnológica como disciplina de abrangência transversal, aplicável à apuração de crimes de qualquer natureza. Desenvolve o vestígio informacional juridicamente relevante como objeto de estudo, o método em sete fases (identificação, preservação, obtenção, tratamento, correlação, interpretação e apresentação) e o Controle de Viés Investigativo, além de examinar prova digital, fontes abertas, inteligência artificial, inteligência criminal, drones, fraudes, dados em nuvem, cooperação jurídica internacional e governança.

Esta cartilha é um material educativo gratuito, escrito para aproximar esses fundamentos da prática. O livro é uma publicação comercial da Editora Juspodivm, indicada a quem deseja aprofundar o estudo.

Conheça o livro no site da editora: editorajuspodivm.com.br

A coleção

A Coleção Investigação e Proteção na Era Digital reúne oito cartilhas gratuitas sobre investigação criminal, prova digital, uso responsável da tecnologia e proteção de pessoas e famílias no ambiente digital. Todos os volumes estão disponíveis em www.higorjorge.com.br, em formato PDF.

- Vol. 01** **Investigação Criminal Tecnológica.** Fundamentos, métodos e aplicações práticas
- Vol. 02** **Provas digitais e cadeia de custódia.** Da coleta à valoração jurídica
- Vol. 03** **Inteligência artificial na investigação criminal.** Aplicações, limites e boas práticas
- Vol. 04** **Golpes digitais e fraudes eletrônicas.** Prevenção, identificação e investigação
- Vol. 05** **Investigação de crimes na internet.** Dados, registros, sigilos e medidas judiciais
- Vol. 06** **Raciocínio investigativo e decisão fundamentada.** Do indício ao relatório final
- Vol. 07** **Internet segura.** Guia prático para proteger você e sua família (este volume)
- Vol. 08** **Crianças e adolescentes na internet.** Guia de proteção para pais e responsáveis

Canais oficiais do autor

- Site** www.higorjorge.com.br
- YouTube** youtube.com/@direitoetecnologia
- Instagram** [@higorjorge](https://www.instagram.com/higorjorge)
- Facebook** facebook.com/professorhigorjorge