ALERTA
SITE SUSPEITO

DOMÍNIO
RECÉM CRIADO

IP
LOCALIZADO

VÍNCULOS
EVIDENCIADOS

CURSO

OSINT

INVESTIGAÇÃO DE GOLPES DIGITAIS

INVESTIGAÇÃO DIGITAL
DO ZERO, DIRETO AO PONTO.

APRENDA A INVESTIGAR
SITES E PERFIS SUSPEITOS

DESCUBRA GOLPES ANTES
QUE SEJA TARDE DEMAIS

PROTEJA SEU NEGÓCIO,
SUA FAMÍLIA E SEUS CLIENTES

FERRAMENTAS REAIS.
ESTRATÉGIAS PRÁTICAS.
RESULTADOS REAIS.

LOCALIZAÇÃO:
177.54.146.93

RISCO: ALTO

CONHECIMENTO É A SUA
MELHOR DEFESA

NÃO SEJA MAIS UMA VÍTIMA.
SEJA O INVESTIGADOR.

donodosite.com

Bem-vindo à investigação digital

Você não precisa ser hacker, policial ou “entender de computador” para descobrir se um site, uma loja ou uma mensagem é golpe. Precisa apenas saber onde olhar — e é exatamente isso que este curso ensina, do zero, com as mesmas ferramentas gratuitas que usamos nos laudos profissionais do donodosite.com.

MÓDULO 1

Entenda o golpista

Como o golpe nasce, os gatilhos psicológicos e os sinais em WhatsApp, e-mail, sites e redes sociais.

MÓDULO 2

Domine as ferramentas OSINT

WHOIS, PIX, DNS, certificado SSL, geolocalização de IP, metadados de imagem, busca reversa, reputação e CNPJ — explicadas de forma simples.

MÓDULO 3

Proteja sua família

Investigação aplicada a compras, redes sociais, golpe do falso parente e proteção de crianças e adolescentes.

PARA QUEM É ESTE CURSO

- Pais e mães que querem proteger filhos e idosos dos golpes mais comuns.
- Pequenos empreendedores que vendem e compram online e não podem cair em fraude.
- Qualquer pessoa cansada de ter medo de clicar, pagar ou confiar na internet.

O que é OSINT?

OSINT (Open Source Intelligence, ou “inteligência de fontes abertas”) é a arte de reunir e cruzar informações que já são públicas — registros de domínio, DNS, certificados, fotos, avaliações — para chegar a uma conclusão. É como ser um detetive que só usa pistas deixadas à vista de todos. Nenhuma invasão, nenhuma senha, nenhum mistério: só observação inteligente.

PODE — COLETA PASSIVA

- Consultar registro do domínio (WHOIS/RDAP).
- Ver DNS, certificado SSL e localização do IP.
- Ler avaliações, reclamações e histórico do site.
- Analisar fotos e metadados públicos.
- Decodificar um código PIX que recebeu.

NÃO PODE — INVASÃO

- Invadir contas, sistemas ou redes alheias.
- Tentar adivinhar ou roubar senhas.
- Explorar falhas de segurança do servidor.
- Se passar por outra pessoa para enganar.
- Expor ou vazar dados pessoais de terceiros.

A REGRA DE OURO DO INVESTIGADOR

Investigue para se proteger e decidir com segurança — não para perseguir, expor ou acusar ninguém. Toda informação deste curso vem de fontes públicas e abertas. Use-a para responder uma única pergunta: “posso confiar neste site, nesta loja ou nesta mensagem?”. O resultado é um juízo de risco, não uma sentença: na dúvida, não pague e não clique.

MÓDULO

1

Entenda o golpista

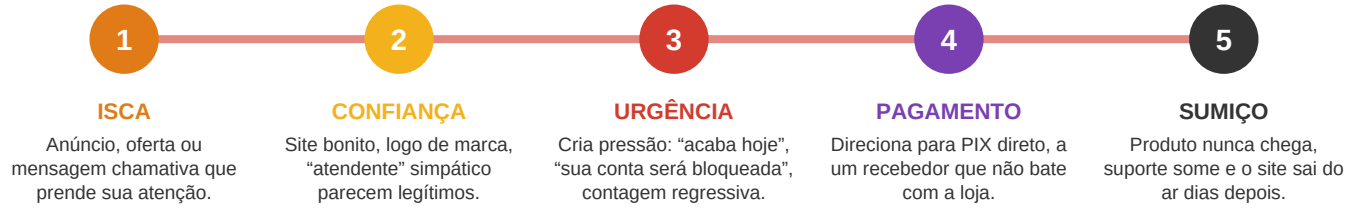
Antes de investigar, é preciso pensar como o criminoso pensa. Conheça a engenharia por trás do golpe.

O que você vai aprender neste módulo

- A anatomia de um golpe, do primeiro contato ao sumiço
- Os 8 gatilhos psicológicos que derrubam qualquer um
- Sinais de golpe no WhatsApp, no e-mail e nos sites
- Perfis e anúncios falsos nas redes sociais

A anatomia de um golpe

Quase todo golpe segue o mesmo roteiro. Quando você reconhece as etapas, consegue interromper a armadilha antes da parte que dói: o pagamento. Veja a linha do tempo de um golpe típico.



ONDE O INVESTIGADOR QUEBRA O GOLPE

- Na CONFIANÇA: o WHOIS revela um site nascido há poucos dias, derrubando a "tradição".
- No PAGAMENTO: o Decodificador PIX mostra que o dinheiro vai para um CPF estranho.
- No SUMIÇO: reputação, Reclame Aqui e Wayback Machine expõem o histórico real.

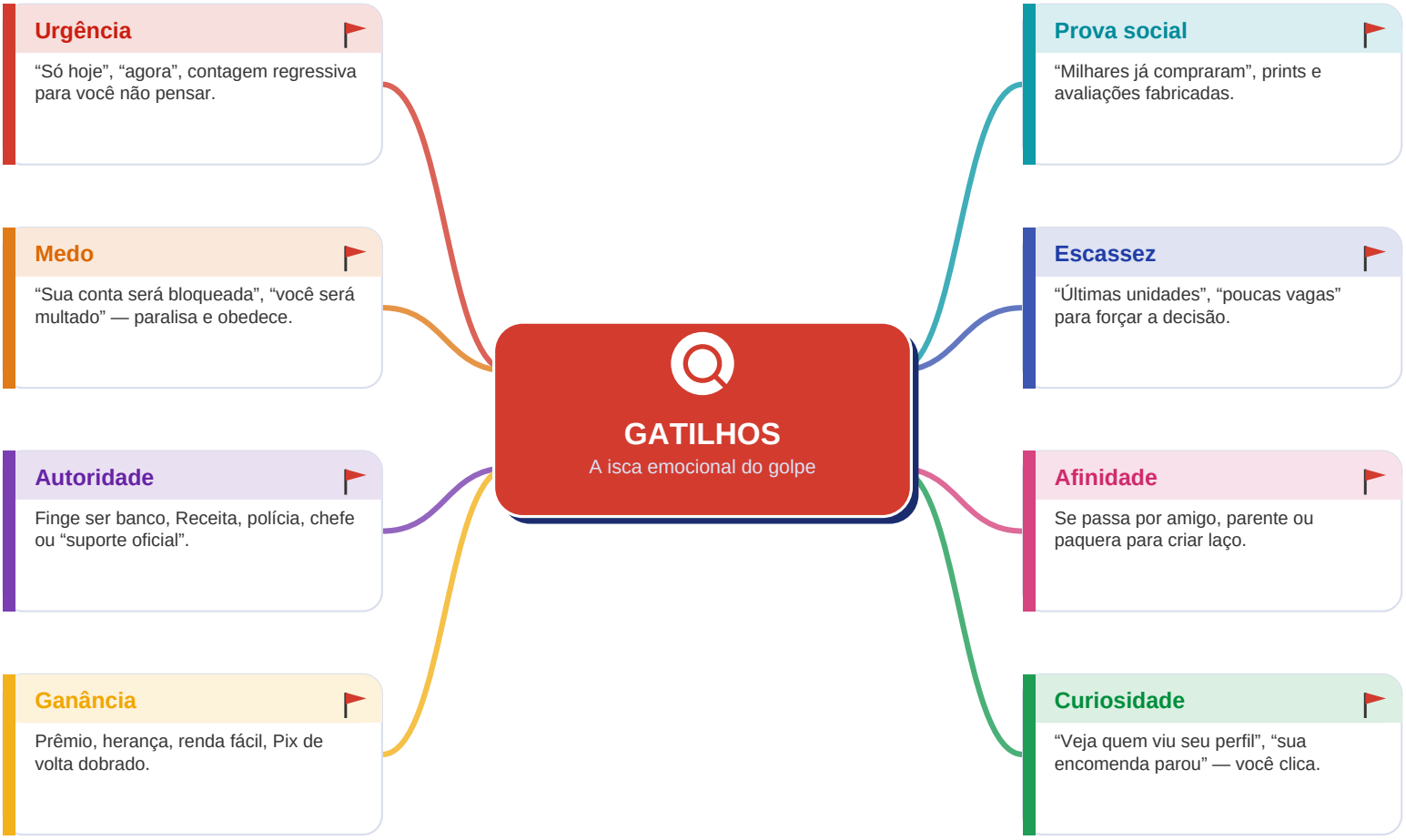
Lição: o golpe depende de você decidir no impulso. Investigar quebra o roteiro porque troca a emoção pela informação.

PARA LEMBRAR

O golpe vive da pressa. Sua única obrigação antes de pagar é desacelerar — dois minutos de checagem valem mais do que qualquer promoção "imperdível".

Os 8 gatilhos que derrubam qualquer um

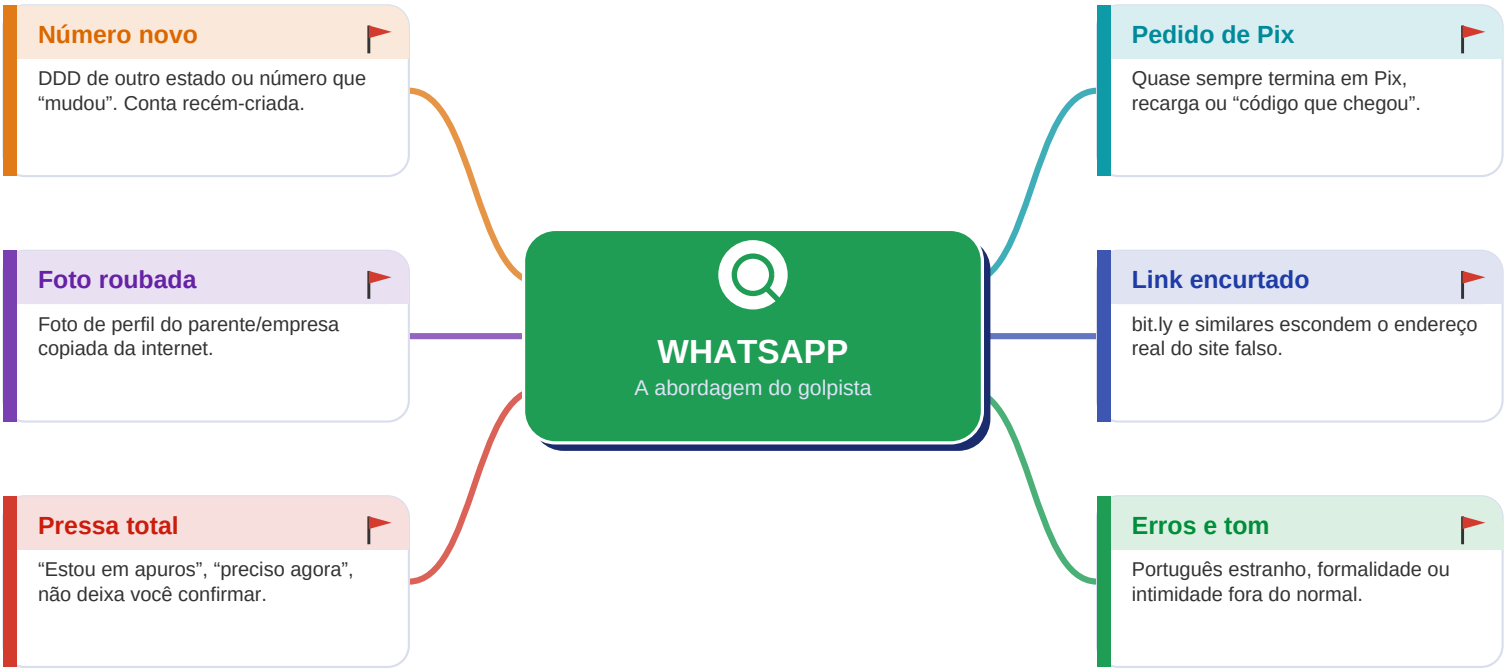
O golpista não ataca o computador — ataca a emoção. Estes são os botões que ele aperta. Reconhecê-los é o primeiro antivírus, e ele roda na sua cabeça.



Antídoto: sempre que sentir urgência, medo ou euforia, PARE. Emoção forte é o sinal de que alguém quer que você aja sem pensar. Respire e investigue.

Os sinais de golpe no WhatsApp

O WhatsApp é o palco favorito do golpista: íntimo, rápido e cheio de confiança. Conheça os elementos que se repetem em quase toda abordagem.



EXEMPLO REAL — "OI MÃE, MUDEI DE NÚMERO"

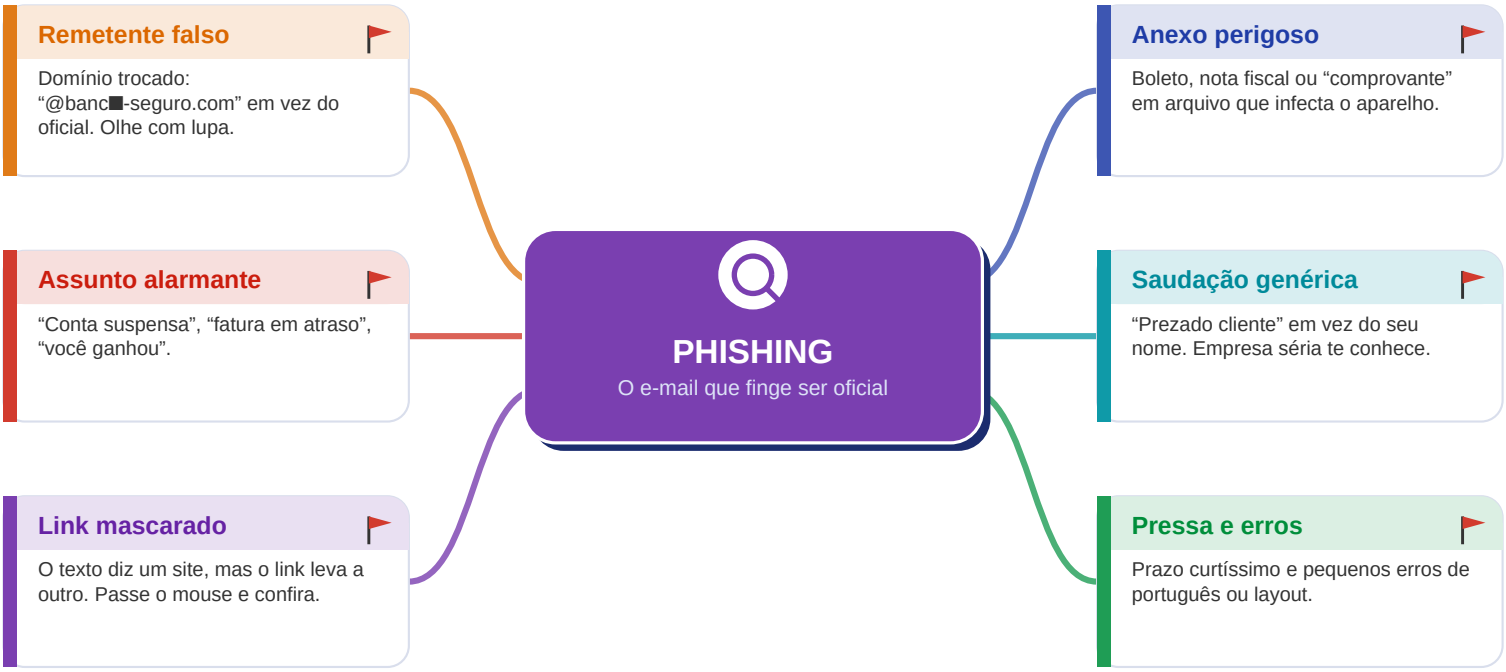
Uma mensagem de número desconhecido se diz seu filho com o "celular novo" e pede um Pix urgente.

Sinais: número de outro DDD, foto de perfil genérica, pressa e o pedido sempre cai em Pix.

Defesa: ligue para o número antigo e combine uma palavra-código de família (veja o Módulo 3).

Phishing: o golpe que chega por e-mail

Phishing é o e-mail “pescador”: imita um remetente confiável para você morder a isca e clicar. Aprenda a desmontá-lo sem nem precisar abrir o link.



EXEMPLO REAL — “SUA NOTA FISCAL ELETRÔNICA”

Um e-mail “da Receita” pede que você baixe a NF-e em anexo ou clique para “regularizar” o CPF.

O endereço do remetente não é gov.br, o link aponta para um domínio estranho e há pressa.

Defesa: nunca clique. Acesse o site oficial digitando você mesmo o endereço no navegador.

Como reconhecer um site falso

A loja fantasma existe só para receber o seu Pix e desaparecer. A boa notícia: cada sinal abaixo tem uma ferramenta OSINT que o comprova — e você vai dominá-las no Módulo 2.



NO DONODOSITE.COM VOCÊ FAZ ISSO DE GRAÇA

- Consulta WHOIS: descubra a idade real e o dono do domínio da loja.
- Decodificador PIX: veja para quem (nome e CPF/CNPJ) o seu dinheiro iria de verdade.

Perfis e anúncios falsos nas redes

Instagram, Facebook e Marketplace viraram caça aos incautos. Golpistas clonam lojas, criam perfis “oficiais” e impulsionam anúncios que somem em horas. Veja os sinais e como verificar.

Conta recente

Perfil criado há pouco, poucas publicações e seguidores comprados.

@ levemente diferente

“@loja.oficial.br” imitando a marca real. Compare letra por letra.

Sem selo / sem histórico

Sem verificação e sem postagens antigas de clientes reais.

Só chama no direct

Foge dos canais oficiais e leva a conversa para WhatsApp/Pix.

COMO VERIFICAR UM PERFIL

- Veja a data de criação da conta (transparência da página).
- Cheque o link da bio no WHOIS — domínio novo é alerta.
- Faça busca reversa da foto de perfil (Módulo 2).
- Procure o nome + “golpe” / “reclamação” no Google.

ANÚNCIO SUSPEITO?

- Preço muito abaixo do mercado para item desejado.
- Frase de urgência: “restam poucas unidades hoje”.
- Pagamento só por Pix antecipado, sem cartão.
- Comentários desativados ou cheios de elogios iguais.

MÓDULO

2

O kit de ferramentas OSINT

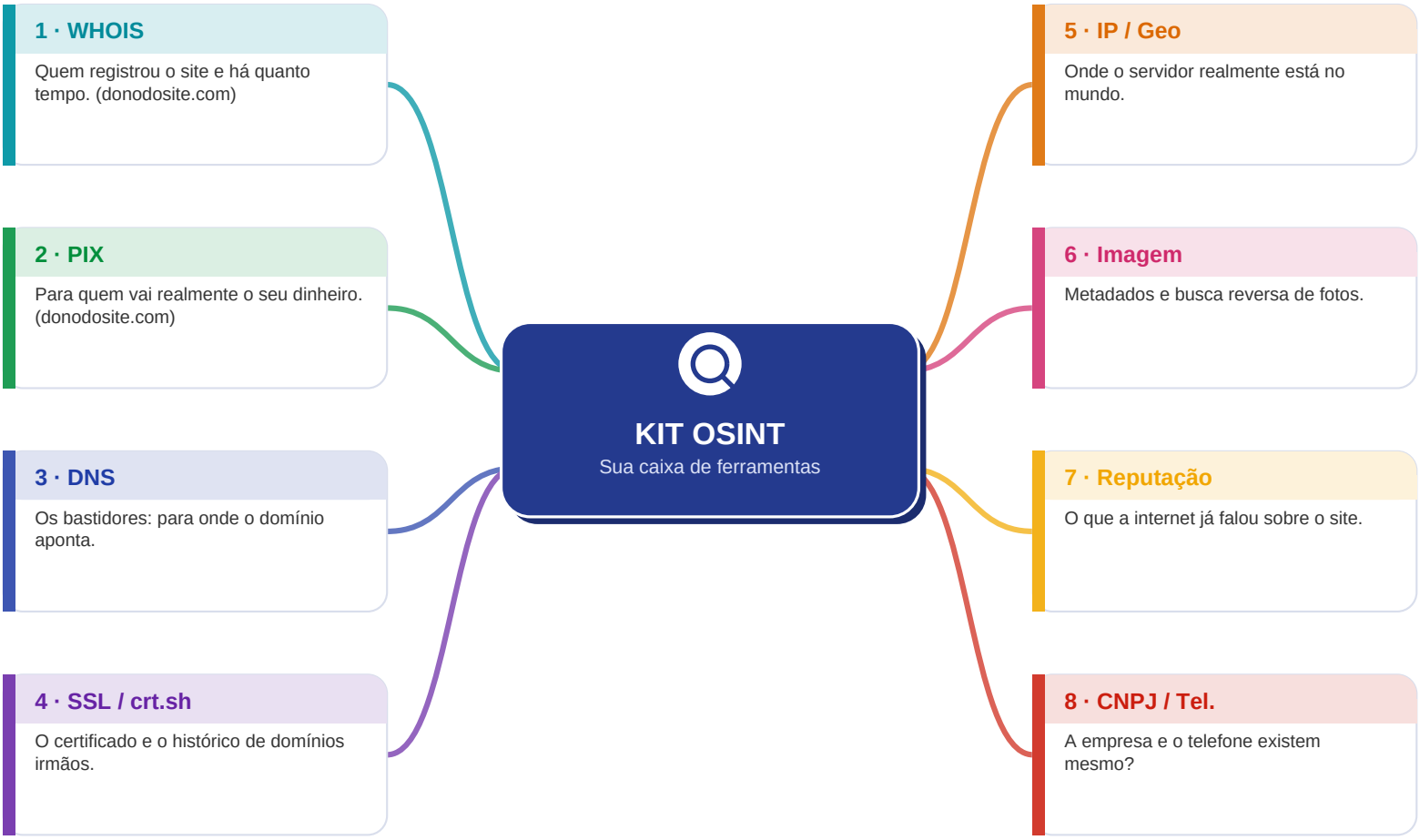
O coração do curso: as ferramentas gratuitas que transformam você em investigador. Simples, no navegador, sem instalar nada.

O que você vai aprender neste módulo

- WHOIS e Decodificador PIX — direto no donodosite.com
- DNS, certificado SSL e geolocalização de IP
- Metadados de imagem e busca reversa de fotos
- Reputação, Wayback Machine, CNPJ e telefone

Seu kit de ferramentas OSINT

Oito ferramentas, oito perguntas. Cada uma responde uma parte da investigação. Você não precisa usar todas sempre — mas, juntas, elas montam o retrato completo de um site ou contato suspeito.



Nas próximas páginas, cada ferramenta ganha uma explicação simples: o que é, o que revela, os sinais de alerta e um exemplo real.

1. Consulta WHOIS

O QUE É

Todo domínio tem um registro público — uma “certidão de nascimento”. A consulta WHOIS (ou RDAP, sua versão moderna) revela quando o site foi criado, quem o registrou e em qual empresa. É a primeira pergunta de qualquer investigação: há quanto tempo essa loja existe de verdade?

O QUE REVELA

- Data de criação e de expiração do domínio.
- Nome do titular (ou aviso de privacidade).
- Empresa registradora e país do registro.
- Status do domínio (ativo, bloqueado, em transferência).
- Servidores de nome (para onde o site aponta).

SINAIS DE ALERTA

- Domínio criado há dias ou semanas numa loja “antiga”.
- Titular oculto por privacidade numa loja brasileira.
- Registro válido por apenas 1 ano (perfil descartável).
- Registrador e país que não combinam com a marca.

EXEMPLO REAL — A “LOJA DE 20 ANOS”

Uma loja anuncia “duas décadas de tradição” com eletrônicos a preço de banana.

No WHOIS, o domínio nasceu há 11 dias e o titular está protegido por privacidade.

Conclusão: a tradição é falsa. Risco altíssimo — não compre.

POR QUE ISSO TE PROTEGE NO DIA A DIA

Compras online: confirma se a “loja antiga” na verdade nasceu ontem.
Redes sociais: revela a idade do site que está no link da bio do perfil.
Família: ensine pais e avós a checar a idade do site antes de pagar.

NO DONODOSITE.COM VOCÊ FAZ ISSO DE GRAÇA

Abra a Consulta WHOIS no donodosite.com e cole o endereço do site.
Leia primeiro a DATA DE CRIAÇÃO — o sinal mais poderoso contra lojas-fantasma.

1. WHOIS na prática — lendo o resultado

Ao colar um domínio, você recebe uma ficha. Veja como interpretar cada linha que importa, sem se perder em termos técnicos.

CAMPO	O QUE SIGNIFICA	COMO LER
Creation Date / Registrado em	Quando o domínio nasceu.	Recente = alerta máximo.
Registrant / Titular	Quem registrou.	Oculto ou estrangeiro = desconfie.
Registrar	Empresa onde foi registrado.	Serve para denúncia (abuse).
Expiry Date / Expira em	Validade do registro.	Só 1 ano = site descartável.
Name Servers	Para onde o domínio aponta.	Revela a hospedagem/CDN.
Status	Situação atual.	“clientHold” = pode estar bloqueado.

TRADUZINDO NA PRÁTICA

Você vê: “Creation Date: 2026-06-02” e “Registrant: REDACTED FOR PRIVACY”.

Leitura: domínio com poucos dias e dono escondido — dois sinais fortes de loja-fantasma.

Some isso a “preço bom demais” e “só Pix” e a decisão é clara: não pague.

NO DONODOSITE.COM VOCÊ FAZ ISSO DE GRAÇA

Treine agora: pegue um site que você usa e veja a idade dele na Consulta WHOIS do donodosite.com.

2. Decodificador PIX

O QUE É

O código “Pix Copia e Cola” parece embaralhado, mas é um padrão aberto (BR Code / EMV) cheio de informação legível. O Decodificador traduz esse código e mostra quem vai realmente receber o seu dinheiro — antes de você confirmar. É a checagem que desmonta a loja-fantasma na hora do pagamento.

O QUE REVELA

- Nome do recebedor (e se bate com a loja).
- Cidade do recebedor.
- Chave Pix (e-mail, telefone, CPF/CNPJ, aleatória).
- Valor exato e identificador da transação.
- O intermediário de pagamento, quando houver.

SINAIS DE ALERTA

- Nome do recebedor diferente da loja anunciada.
- Loja “grande” recebendo na conta de pessoa física.
- Cidade do recebedor sem relação com a empresa.
- Valor diferente do combinado na tela.

EXEMPLO REAL — A “LOJA OFICIAL”

Você fecha a compra numa suposta loja oficial e recebe um Pix Copia e Cola para pagar.

Decodificado, o recebedor é uma pessoa física (CPF) de outra cidade — não a empresa.

Conclusão: loja séria recebe como CNPJ no próprio nome. Não pague.

POR QUE ISSO TE PROTEGE NO DIA A DIA

Compras online: garante que o dinheiro vai para a loja certa, não para um laranja.
Família: no golpe do falso parente, o recebedor nunca está no nome do seu familiar.
Todo Pix: dez segundos de checagem que evitam o prejuízo de meses.

NO DONODOSITE.COM VOCÊ FAZ ISSO DE GRAÇA

Cole o código “Pix Copia e Cola” no Decodificador PIX do donodosite.com.
Antes de confirmar qualquer pagamento, confira o NOME e o CPF/CNPJ do recebedor.

2. PIX na prática — o que há dentro do código

O BR Code é formado por “campos” numerados (padrão EMV). Você não precisa decorá-los — o donodosite.com faz a leitura — mas entender o que cada um significa te deixa no controle.

Campo 00 / 01
Versão e tipo do código (estático ou dinâmico).

Campo 26
O “coração”: chave Pix e o intermediário (br.gov.bcb.pix).

Campo 52 / 53
Categoria do recebedor e moeda (986 = Real).

Campo 58
País do recebedor (BR).

Campo 59
NOME do recebedor — confira com a loja!

Campo 60
CIDADE do recebedor.

Campo 62
Identificador da transação (referência da loja).

Campo 63
CRC: código de verificação que fecha o BR Code.

LENDO UM CÓDIGO DECODIFICADO

Resultado: Nome “J. P. SILVA”, Cidade “SAO PAULO”, Chave = CPF, Valor R$ 459,90.

A loja se chamava “MegaTech Importados”, mas quem recebe é uma pessoa física.

O nome do recebedor (campo 59) e a chave revelam a fraude em 5 segundos.

NO DONODOSITE.COM VOCÊ FAZ ISSO DE GRAÇA

Sempre que receber um Pix Copia e Cola, cole no Decodificador PIX do donodosite.com antes de pagar.

O ATALHO QUE NUNCA FALHA

O nome do recebedor (campo 59) e a chave Pix são o atalho da investigação: se não for o nome da loja, não pague — por mais bonita que seja a tela.

3. Análise de DNS

O QUE É

O DNS é a “lista telefônica” da internet: ele liga o nome do site (o domínio) ao servidor onde ele mora. Consultar o DNS mostra para onde um domínio aponta e como o e-mail dele é tratado — pistas valiosas sobre a estrutura por trás da loja.

O QUE REVELA

- Registro A/AAAA: o endereço IP do servidor.
- Registro MX: se o domínio tem e-mail profissional.
- Registro NS: a hospedagem/CDN usada (ex.: Cloudflare).
- Registros TXT/SPF: configurações de segurança de e-mail.

SINAIS DE ALERTA

- Sem registro de e-mail (MX) numa “empresa” séria.
- Estrutura escondida atrás de CDN para ocultar o servidor.
- Mesmo IP compartilhado com vários sites de golpe.
- Configuração improvisada, típica de site montado às pressas.

EXEMPLO REAL — A “EMPRESA” SEM E-MAIL

Uma “grande importadora” só atende por WhatsApp e formulário no site.

No DNS, o domínio não tem registro MX — ou seja, não existe e-mail @ daquela empresa.

Empresa real tem e-mail próprio. A ausência reforça o perfil de fachada.

POR QUE ISSO TE PROTEGE NO DIA A DIA

Compras online: uma “empresa” sem e-mail próprio (sem MX) é bandeira vermelha.
Trabalho: confirma a estrutura real de um fornecedor ou prestador novo.
Geral: separa o negócio sério da fachada montada às pressas.

ONDE USAR (GRÁTIS)

dnschecker.org · mxtoolbox.com · who.is — cole o domínio e veja os registros A, MX e NS.

4. Certificado SSL e crt.sh

O QUE É

O cadeado do navegador é o certificado SSL/TLS: ele garante que a conexão é criptografada — mas NÃO que a loja é honesta (golpista também usa cadeado). O valor investigativo está em quando o certificado foi emitido e, no site crt.sh, em descobrir outros domínios “irmãos” ligados ao mesmo dono.

O QUE REVELA

- Data de emissão do certificado (idade real do site).
- Quem emitiu (ex.: Let’s Encrypt, gratuito).
- No crt.sh: histórico de todos os certificados.
- Subdomínios e domínios irmãos do mesmo esquema.

SINAIS DE ALERTA

- Certificado emitido há poucos dias (site novo).
- Tratar o “cadeado” como prova de confiança.
- Vários domínios-clone irmãos no crt.sh.
- Certificado que não cobre o domínio que você acessou.

EXEMPLO REAL — A REDE DE CLONES

Você investiga “loja-promo-x.com” e busca o domínio no crt.sh.

Aparecem 30 domínios quase idênticos (loja-promo-y, -z...) criados no mesmo dia.

Conclusão: é uma fábrica de lojas-fantasma descartáveis. Fuja de todas.

POR QUE ISSO TE PROTEGE NO DIA A DIA

- Compras online: desfaz o mito perigoso de que “tem cadeado, então é seguro”.
- Redes sociais: encontra a rede de sites-clone por trás de um mesmo anúncio.
- Geral: uma busca revela dezenas de sites-irmãos do mesmo golpe.

ONDE USAR (GRÁTIS)

crt.sh — digite o domínio para ver o histórico de certificados e domínios irmãos. O cadeado, sozinho, não é garantia.

5. Geolocalização de IP

O QUE É

Todo servidor tem um endereço IP, e o IP tem uma localização aproximada e um "dono" (a empresa de hospedagem). Saber onde a "loja brasileira" está realmente hospedada — e em qual provedor — ajuda a medir a coerência da operação.

O QUE REVELA

- País e cidade aproximados do servidor.
- Empresa de hospedagem/provedor (ASN).
- PTR reverso: o nome técnico ligado ao IP.
- Se o site usa CDN (Cloudflare) para se ocultar.

SINAIS DE ALERTA

- "Loja do Brasil" hospedada em servidor improvável.
- Provedor offshore incompatível com o negócio.
- IP que hospeda dezenas de sites suspeitos.
- Localização que contradiz o endereço anunciado.

EXEMPLO REAL — O "ATACADO NACIONAL"

Um "atacado nacional" jura ter centro de distribuição em São Paulo.

A geolocalização do IP aponta servidor no exterior, sem qualquer estrutura no Brasil.

A incoerência entre discurso e infraestrutura reforça o risco.

POR QUE ISSO TE PROTEGE NO DIA A DIA

- Compras online: um "atacado nacional" hospedado no exterior não combina.
- Geral: mede a coerência entre o discurso da loja e a infraestrutura real.
- Denúncia: ajuda a localizar o provedor certo para reportar o abuso.

ONDE USAR (GRÁTIS)

ipinfo.io · ip-api.com — informe o domínio ou IP e veja país, cidade e provedor de hospedagem.

6. Cabeçalhos e tecnologias

O QUE É

Quando você abre um site, o servidor envia “cabeçalhos” (informações técnicas) junto com a página. Ferramentas gratuitas revelam quais tecnologias o site usa, se foi montado a partir de um modelo pronto e se há sinais de uma fábrica de lojas replicadas.

O QUE REVELA

- Servidor e tecnologias usadas no site.
- Plataforma de loja (ex.: template white-label).
- Rastreadores e gateways de pagamento embutidos.
- Pistas de que o site é cópia de um modelo.

SINAIS DE ALERTA

- Placeholders de template não preenchidos (CNPJ 00.000...).
- Mesma plataforma-clone de outros golpes conhecidos.
- Gateway de pagamento que não bate com a loja.
- Contador regressivo que reinicia sozinho (falsa escassez).

EXEMPLO REAL — O CNPJ DE MENTIRA

No rodapé, o site exibe “CNPJ 00.000.000/0000-00”.

Esse é o CNPJ de exemplo que vem nos modelos prontos — ninguém preencheu o real.

Sinal clássico de loja montada em minutos a partir de um template.

POR QUE ISSO TE PROTEGE NO DIA A DIA

- Compras online: flagra CNPJ de exemplo e dados de template não preenchidos.
- Redes sociais: identifica lojas-clone feitas com o mesmo molde pronto.
- Geral: mostra qual é o gateway de pagamento que realmente recebe.

ONDE USAR (GRÁTIS)

wappalyzer.com · builtwith.com — informe o site e veja tecnologias, plataforma e rastreadores.

7. Metadados de imagem

O QUE É

Fotos digitais carregam metadados (EXIF): data, câmera, às vezes a localização (GPS) e o software de edição. Analisar a imagem de um produto, documento ou perfil pode revelar de onde ela veio — e desmascarar fotos roubadas ou forjadas.

O QUE REVELA

- Data e hora em que a foto foi tirada.
- Câmera/telefone ou software de edição usado.
- Coordenadas GPS, quando presentes.
- Sinais de montagem (ex.: “editado no Photoshop”).

SINAIS DE ALERTA

- Foto de “produto em estoque” editada e sem origem.
- Imagem com dimensões típicas de banco de imagens.
- Metadados removidos para apagar a procedência.
- GPS que contradiz o local anunciado.

EXEMPLO REAL — O “COMPROVANTE” FORJADO

Um golpista envia o “comprovante de pagamento” como imagem para liberar o produto.

Os metadados mostram que a imagem foi criada no editor, não exportada do app do banco.

Comprovante real vem do aplicativo; imagem editada é forte sinal de fraude.

POR QUE ISSO TE PROTEGE NO DIA A DIA

Família: desmascara o “comprovante de pagamento” forjado num editor.
Compras online: revela fotos de produto sem origem ou recortadas de outro site.
Crianças: ajuda a checar de onde veio realmente uma imagem suspeita.

ONDE USAR (GRÁTIS)

exif.tools · metadata2go.com — envie a imagem e leia EXIF, data, software e GPS (quando houver).

8. Busca reversa de imagem

O QUE É

A busca reversa faz o caminho contrário: você dá uma imagem e o buscador encontra onde mais ela aparece na internet. É uma das armas mais rápidas contra perfis falsos, lojas-clone e fotos roubadas.

O QUE REVELA

- Outros sites onde a mesma foto aparece.
- Se a “foto do vendedor” foi copiada de outra pessoa.
- A origem real de um produto anunciado.
- Perfis diferentes usando a mesma imagem.

SINAIS DE ALERTA

- Foto de perfil que aparece em dezenas de contas.
- Imagem de produto retirada do site do fabricante.
- Mesma “cliente satisfeita” em vários golpes.
- Foto de imóvel/carro copiada de outro anúncio.

EXEMPLO REAL — A PAQUERA QUE NÃO EXISTE

Um perfil romântico envia fotos para ganhar sua confiança (e depois, seu dinheiro).

A busca reversa mostra que as fotos são de um modelo/influencer de outro país.

Identidade roubada confirmada — é golpe de relacionamento (romance scam).

POR QUE ISSO TE PROTEGE NO DIA A DIA

- Redes sociais: descobre perfis falsos que usam foto roubada de outra pessoa.
- Relacionamento: expõe o golpe do amor (romance scam) em segundos.
- Compras online: encontra a origem real de um produto anunciado.

ONDE USAR (GRÁTIS)

Google Imagens / Lens · tineye.com · Yandex Imagens — envie a foto e veja onde mais ela aparece.

9. Reputação e histórico

O QUE É

Antes de confiar, ouça quem já passou por ali. Buscar a reputação de um site e consultar o histórico dele no tempo costuma resolver a investigação em minutos — golpe deixa rastro de vítimas.

O QUE REVELA

- Reclamações e relatos de outras vítimas.
- Nota e tempo de resposta no Reclame Aqui.
- Histórico do site no tempo (Wayback Machine).
- Alertas de segurança e listas de sites falsos.

SINAIS DE ALERTA

- Muitas reclamações de “não entregou / sumiu”.
- Site sem nenhum histórico antes deste mês.
- Página que mudou de ramo do dia para a noite.
- Avaliações 5 estrelas idênticas e sem detalhes.

EXEMPLO REAL — O SITE QUE NÃO TINHA PASSADO

Você pesquisa “lojax.com reclamação” e consulta a Wayback Machine.

Não há registro do site antes deste mês e já surgem queixas de produto não entregue.

Loja séria deixa rastro positivo no tempo. A ausência de história é, por si só, um alerta.

POR QUE ISSO TE PROTEGE NO DIA A DIA

Compras online: ouça quem já foi vítima antes de você abrir a carteira.
Geral: um site sem nenhum passado é, por si só, um forte alerta.
Família: ensine o hábito de pesquisar “nome + golpe” antes de confiar.

ONDE USAR (GRÁTIS)

Google: nome + “golpe/reclamação” · reclameaqui.com.br · web.archive.org (Wayback Machine) · PSafe/Konduto dfndr lab.

10. CNPJ, CPF e telefone

O QUE É

Lojas sérias têm CNPJ ativo e dados que batem. Consultas oficiais e gratuitas confirmam se a empresa existe, desde quando, em que ramo atua e onde fica — e ajudam a checar se um número de telefone já é conhecido por aplicar golpes.

O QUE REVELA

- Situação do CNPJ (ativo, baixado, suspenso).
- Razão social, data de abertura e ramo (CNAE).
- Endereço e sócios registrados.
- Se o telefone aparece em listas de denúncia.

SINAIS DE ALERTA

- CNPJ inexistente, baixado ou recém-aberto.
- Ramo de atividade que não combina com a loja.
- Endereço genérico, residencial ou inexistente.
- Telefone já marcado como spam/golpe por outros.

EXEMPLO REAL — A "IMPORTADORA" DE 1 MÊS

A loja exibe um CNPJ no rodapé para parecer confiável.

Na consulta oficial, a empresa foi aberta há 1 mês e o ramo é "comércio varejista" genérico.

CNPJ recém-aberto + idade do domínio + só Pix = padrão típico de fraude.

POR QUE ISSO TE PROTEGE NO DIA A DIA

Compras online: confirma se a empresa existe de verdade e desde quando.
Trabalho: valida um fornecedor, prestador ou "vaga de emprego" nova.
Geral: identifica números de telefone já denunciados por golpe.

ONDE USAR (GRÁTIS)

Receita Federal (consulta CNPJ) · Quem é Dono do Número / apps de identificação de chamadas · procon e consumidor.gov.br.

MÓDULO

3

Proteja sua família

A investigação aplicada ao dia a dia: compras, redes sociais, conversas em família e a segurança das crianças e dos adolescentes.

O que você vai aprender neste módulo

- Um passo a passo para investigar qualquer loja suspeita
- Compras e redes sociais: checklist antes de confiar
- O golpe do falso parente e a palavra-código da família
- Proteção de crianças e adolescentes na internet

Passo a passo: investigando uma loja

Junte as ferramentas do Módulo 2 numa rotina simples. Em poucos minutos, você sai do “será que é golpe?” para uma decisão segura.

1 — Idade do domínio
Cole o site na Consulta WHOIS (donodosite.com). Recente? Já acende o alerta.

2 — Identidade da loja
Procure CNPJ, endereço e telefone. Confira o CNPJ na Receita.

3 — Reputação
Pesquise o nome + “golpe/reclamação” e veja o Reclame Aqui e a Wayback.

4 — As fotos
Faça busca reversa das imagens de produto e de “clientes”.

5 — O pagamento
Recebeu Pix? Decodifique no donodosite.com e confira o recebedor.

6 — Decisão
Somou 2 ou mais alertas? Não pague. Na dúvida, a resposta é não.

Dica de ouro: você não precisa de todos os passos. Dois ou três sinais coerentes já bastam para uma decisão segura.

! COMECE PELO DONODOSITE.COM
A Consulta WHOIS e o Decodificador PIX já resolvem a maior parte dos casos em dois minutos. Comece sempre por eles antes de partir para as ferramentas externas.

Redes sociais e compras online

É onde a maioria dos golpes começa hoje. Dois contextos, duas checagens rápidas que cabem na palma da mão antes de clicar em “comprar” ou “seguir”.

ANTES DE COMPRAR ONLINE

- Vi a idade do domínio no WHOIS (donodosite.com).
- Confirmei CNPJ, endereço e telefone reais.
- Pesquisei reputação e Reclame Aqui.
- Desconfiei de preço bom demais e de urgência.
- Decodifiquei o Pix e conferi o recebedor.
- Prefiro cartão/boleto a Pix antecipado a CPF.

ANTES DE CONFIAR NUM PERFIL

- Vi a data de criação da conta.
- Comparei o @ letra por letra com o oficial.
- Fiz busca reversa da foto de perfil.
- Chequei o link da bio no WHOIS.
- Desconfiei de quem só chama no direct/Pix.
- Procurei o nome + “golpe” no Google.

POR QUE ISSO PROTEGE SUA FAMÍLIA

Compartilhe estes dois checklists no grupo da família. A maioria das fraudes morre no primeiro item.

Idosos e adolescentes são os alvos preferidos — uma checagem de 2 minutos evita o prejuízo de meses.

O golpe do falso parente

É um dos golpes que mais cresce: alguém finge ser seu filho, neto ou amigo “com número novo” e pede dinheiro urgente. Funciona porque mistura afinidade, urgência e vergonha. Veja como blindar a sua família.

“Mudei de número”

Mensagem de número novo dizendo ser parente próximo.

Emergência

“Bati o carro”, “estou preso”, “preciso pagar agora”.

Sigilo

Pede para não contar a ninguém e não ligar.

Pix na hora

Sempre termina num Pix para conta de terceiro.

A DEFESA: PALAVRA-CÓDIGO DA FAMÍLIA

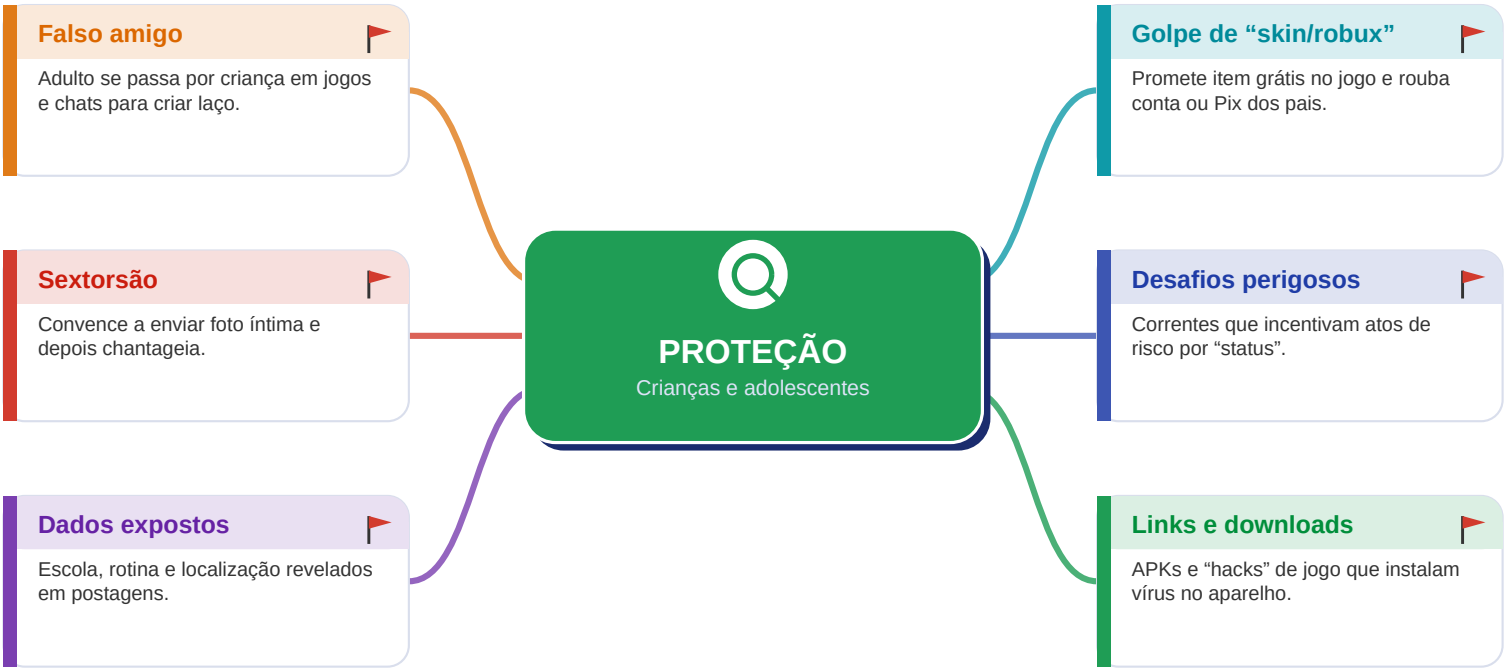
- Combine hoje uma palavra-código secreta com pais, filhos e avós.
- Regra de ouro: pedido de dinheiro por mensagem só é válido com a palavra correta.
- Sempre LIGUE para o número antigo e conhecido antes de pagar qualquer coisa.
- Se houver Pix, decodifique no donodosite.com — o recebedor nunca será seu parente.
- Combine que “não contar a ninguém” é, por si só, o maior sinal de golpe.

COMBINE HOJE, NÃO DEPOIS

Defina a palavra-código da família ainda hoje e avise todo mundo. O golpe do falso parente perde a força no instante em que existe uma senha combinada entre vocês.

Protegendo crianças e adolescentes

Os mais jovens vivem online e confiam rápido. Os riscos têm nome — e cada um tem uma conversa e uma atitude que protege. O melhor filtro não é um aplicativo: é o diálogo.



O QUE FAZER (SEM DRAMA)

- Converse: combine que nunca se envia foto íntima e nunca se encontra desconhecido da internet.
- Ative controles parentais e privacidade, mas trate-os como apoio — não como substituto do diálogo.
- Garanta que a criança possa contar qualquer coisa sem medo de punição. Acolhimento vence o medo.

Checklist mestre OSINT anti-golpe

Imprima, salve no celular e use sempre. Sua investigação cabe em sete perguntas.

- [ ] O domínio é antigo? (WHOIS — donodosite.com)
- [ ] A empresa tem CNPJ ativo e dados que batem?
- [ ] A reputação e o histórico (Reclame Aqui, Wayback) são bons?
- [ ] As fotos são originais? (busca reversa)
- [ ] O recebedor do Pix é a própria loja? (Decodificador PIX — donodosite.com)
- [ ] O preço é realista e não há pressão de urgência?
- [ ] Na dúvida com 2+ alertas: eu NÃO pago e NÃO clico.

JÁ CAIU NUM GOLPE? AJA RÁPIDO

- Acione o banco e peça o MED do Pix.
- Reúna prints, comprovantes e dados.
- Registre em consumidor.gov.br e B.O.

CONTINUE APRENDENDO

- Use o WHOIS e o PIX do donodosite.com.
- Compartilhe este curso com a família.
- Na dúvida, peça um laudo profissional.

Investigar leva minutos. Cair num golpe custa muito mais.

Ferramentas gratuitas: www.donodosite.com

Investigação profissional: donodositeoficial@gmail.com

PARABÉNS — VOCÊ CONCLUIU O CURSO OSINT

Agora você investiga antes de confiar. Releia este checklist sempre que tiver dúvida e compartilhe o que aprendeu com quem você ama — conhecimento que protege se multiplica.



Sobre o autor

Engenheiro de Software com experiência em desenvolvimento Full Stack, Computação em Nuvem, Inteligência Artificial (IA) e Segurança da Informação, construindo aplicações corporativas, projetando arquiteturas de software escaláveis e desenvolvendo soluções voltadas à segurança web, à confiança digital e à automação inteligente.

Fundador do Dono do Site (donodosite.com), projeto independente de pesquisa em segurança web e inteligência de fontes abertas (OSINT), dedicado a analisar sites, domínios e infraestruturas digitais usando exclusivamente informações públicas. O projeto promove a conscientização em cibersegurança, a prevenção de fraudes e o desenvolvimento de metodologias de avaliação de riscos online.

Ferramentas gratuitas: www.donodosite.com · **Contato:** donodositeoficial@gmail.com