Personal Glasswing

PESQUISA · EDIÇÃO DE NOVEMBRO DE 2026

Golpes online no Brasil: o que os dados mostram e o que não mostram

Um dos países mais visados, sem posição confiável de 1º lugar. Evidências, lacunas e o papel do perfil público, com todas as fontes verificadas.

Fact-check número a número | Fontes primárias marcadas | Lacunas declaradas

Publicação
Iwlabs · Personal Glasswing
Lucas Wetten

Data de corte
29 de novembro de 2026
Versão 1.0

Disponível em
personalglasswing.com

Resumo executivo

O Brasil é um dos países mais visados por golpes online, mas nenhum levantamento de golpe, fraude ou phishing que conseguimos verificar o coloca em primeiro lugar no mundo. A posição muda conforme a métrica, e a evidência mais sólida está dentro do país: nos registros policiais, nas pesquisas de vitimização e no uso do Pix.

2,26 mi

ocorrências de estelionato registradas em 2025, alta de 429,8% sobre 2018 [1]

15,8%

dos brasileiros de 16 anos ou mais (≈ 26,3 mi) disseram ter perdido dinheiro em golpe pela internet ou celular em 12 meses [2]

6º

lugar do Brasil em % de usuários Kaspersky que encontraram phishing em 2025; o 1º é o Peru [3]

O que a evidência sustenta

- **Posição do Brasil no mundo:** entre os mais expostos, mas sem 1º lugar confiável. É 6º em phishing por usuário (Kaspersky, 2025), 10º entre os países mais alvejados na plataforma da Zscaler (dados de 2024) e 4º em chamadas de spam ou fraude (Truecaller, 2025). O "1º" aparece apenas em recortes restritos: três países na Veriff, a América Latina na SOCRadar, ligações indesejadas na Hiya.
- **Tamanho interno:** os registros de estelionato passaram de 426.799 em 2018 para 2.261.055 em 2025. Mede boletins de ocorrência, não crimes ocorridos, e a série mistura efeito da Lei 14.155/2021.
- **Vítimas segundo pesquisas:** entre 15,8% e 33,4% da população, conforme a pergunta e o período. As pesquisas não são comparáveis entre si.
- **Como o golpe chega:** a identidade é o ponto comum. Em 2025, 11,4% disseram que alguém se passou por eles, 7,0% tiveram o perfil invadido e 8,7% o celular "clonado". Aplicativos de mensagem são o canal mais citado.
- **Prevenção:** há medidas oficiais no Pix, mas as fontes não avaliam seu impacto, e o próprio Banco Central descreve a eficácia do MED como limitada (9,3% do valor contestado recuperado em média em 2025).

O que nenhum estudo que encontramos mede: quantos golpes começam com informação pública do perfil, e se ajustar a privacidade das redes reduz golpes. Este documento não afirma nenhum desses dois números.

1 Pergunta, método e interesse declarado

A pergunta que orienta este documento é simples: o Brasil é, de fato, um país especialmente visado por golpes online, e o que se sabe sobre como eles começam? A afirmação de que o Brasil seria "o país com mais golpes do mundo" circula com frequência. Preferimos testá-la a repeti-la.

Reunimos relatórios oficiais, pesquisas de vitimização, rankings de empresas de segurança e literatura acadêmica. Em 29/11/2026, cada número usado aqui foi reaberto na fonte por uma conferência independente. Cada referência recebe uma marca: Primária quando o documento original foi aberto e lido, e Secundária quando só foi possível confirmar por um relato de terceiros. Números que não puderam ser conferidos na fonte ficaram de fora ou aparecem assinalados.

> **Interesse declarado.** O Personal Glasswing é um serviço comercial da lwlabs: uma auditoria de privacidade das redes sociais contra golpes. Este documento foi produzido por quem tem interesse nesse tema. Por isso separamos o que a evidência mostra (seções 2 a 5) da nossa posição (seção 6), e listamos as lacunas na seção 7.

2 O Brasil no mundo: muito exposto, sem 1º lugar confiável

Não existe um ranking único e aceito de "países com mais golpes". Cada levantamento mede uma coisa diferente: usuários que encontraram phishing, ataques bloqueados, perdas autodeclaradas, chamadas de spam. A tabela reúne o que conseguimos verificar e o que cada métrica mede.

MÉTRICA E FONTE	BRASIL	O QUE MEDE E O QUE NÃO MEDE
Usuários que encontraram phishing, % dos usuários Kaspersky, 2025 [3] Primária	**6º, com 15,48%.** 1º: Peru (17,46%)	Detecção em produtos Kaspersky, enviesada para a base de clientes de cada país. Não mede vítimas nem perdas.
Ataques de phishing bloqueados, Zscaler, dados de 2024 [4] Primária	**10º**, primeira vez no top 10. 1º: EUA	Tráfego corporativo da plataforma Zscaler (2 bilhões de transações bloqueadas). Não representa o público geral.

MÉTRICA E FONTE	BRASIL	O QUE MEDE E O QUE NÃO MEDE
Chamadas de spam ou fraude, Truecaller, 2025 [5] Secundária	**4º**, atrás de Indonésia, Chile e Vietnã	Parcela de chamadas de números desconhecidos classificadas como spam ou fraude pelos usuários do aplicativo. Só canal telefônico.
Perdas como % do PIB, GASA/Feedzai 2025, via CNN Brasil [6] Secundária	**9º, com 0,8%.** Nigéria 11,3%, Quênia 10,9%	Perdas autodeclaradas em survey. A tabela original é restrita a membros e não foi consultada: tratar como indicação.
Participação no phishing da América Latina, SOCRadar, mai/2024 a mai/2025 [7] Primária	**51,25%** dos ataques da região	Posição relativa dentro da região, na base da própria empresa. Não compara com outros continentes.
Ligações indesejadas por pessoa, Hiya, 1º tri/2025 [8] Primária	**1º** entre mais de 40 países (28 por mês)	Chamadas fora da agenda. Inclui telemarketing legítimo: não é medida de golpe.
Fraude vista 5 ou mais vezes em 12 meses, Veriff 2025 [9] Primária	26,3% (EUA 15,7%; Reino Unido 10,6%)	Só três países, 2.000 pessoas que já sofreram fraude online nos últimos cinco anos. Não é ranking mundial.

De onde vem o “primeiro do mundo”

O título de “1º do mundo” circulou na imprensa a partir de uma pesquisa da empresa Veriff, vendedora de verificação de identidade. O documento original comparou apenas Brasil, Estados Unidos e Reino Unido [9], e a reportagem que o popularizou contém imprecisões em relação a ele, como falar em “cinco vezes mais” quando a razão é de 1,7 e 2,5 vezes [10]. Ser o primeiro entre três países não é ser o primeiro do mundo.

> **Cuidado com os números da GASA.** A Global Anti-Scam Alliance estimou perdas de R$ 297,7 bilhões no Brasil em 2024 (1.322 respondentes) [11] e de R$ 99 bilhões em 2025 (1.000 respondentes, com os maiores relatos de perda excluídos) [12]. As amostras e métodos diferem; isso não indica queda real. Mesmo na edição global de 2025, a própria GASA publica taxas que não se reconciliam (57% de pessoas que encontraram golpe no comunicado, “sete em dez” na página do relatório) [13].

Conclusão da seção

O Brasil aparece entre os países muito expostos em quase todas as métricas verificáveis, e no topo da América Latina em phishing. Nenhum ranking de golpe, fraude ou phishing que verificamos o coloca em 1º no mundo. A formulação que a evidência sustenta é **"um dos países mais visados"**.

Números de imprensa que não conseguimos confirmar na fonte e que, por isso, não usamos: "553 milhões de detecções, 2º lugar atrás da Índia" [14] e "101º de 112 no índice da Sumsub" [15].

3 O tamanho do problema dentro do Brasil

3.1 Registros policiais

Em 2025, as polícias estaduais registraram 2.261.055 ocorrências de estelionato, 3,1% a mais que as 2.193.122 de 2024. A taxa por 100 mil habitantes passou de 1.031,7 para 1.059,4 (+2,7%). Em 2018 eram 426.799: uma alta de 429,8% em sete anos [1].

Três cuidados de leitura. Primeiro, o dado conta boletins de ocorrência, não crimes ocorridos, e o próprio Anuário observa que a taxa acompanha também a bancarização e a estrutura policial. Segundo, o estelionato inclui a fraude eletrônica desde a Lei 14.155/2021 [16], e o salto de 2019 a 2021 coincide com a lei e com a pandemia sem que o Anuário separe os efeitos. Terceiro, a série é revisada a cada edição: o mesmo ano aparece com valores diferentes em edições anteriores, e aqui usamos a de 2026.

Os registros de estelionato por meio eletrônico somaram 346.753 em 2025, contra 286.226 em 2024, nas 24 unidades da federação com dado; São Paulo, Rio de Janeiro e Ceará constam como informação não disponível nessa coluna. O número é, portanto, um piso nacional, e não deve ser dividido pelo total de estelionatos [1].

O mesmo Anuário mostra o outro lado do funil: em 2025 foram abertos 63.771 processos penais, o equivalente a 2,8% dos boletins, e havia 4.819 presos. A comparação é entre contagens do mesmo ano de fontes diferentes, não de uma mesma coorte de casos [1].

3.2 Pesquisas de vitimização: o que pessoas dizem ter vivido

PESQUISA	AMOSTRA E CAMPO	PERGUNTA	RESULTADO
FBSP/Datafolha, mar/2026 [2]	2.004 pessoas de 16+, 137 municípios, 9–10/03/2026, ±2 p.p.	Foi vítima, nos 12 meses anteriores, de golpe em que perdeu dinheiro pela internet ou celular; e de fraude ou desvio em aplicativo bancário ou Pix	**15,8%** (≈ 26,3 mi) e **12,4%** (≈ 20,7 mi)

PESQUISA	AMOSTRA E CAMPO	PERGUNTA	RESULTADO
FBSP/Datafolha, jun/2025 [17]	2.007 pessoas de 16+, 130 municípios, 2–6/06/2025, ±2 p.p.	Ao menos um golpe ou fraude digital com prejuízo financeiro direto (cartão, conta, Pix ou boleto, produto pago e não entregue, investimento), jul/2024 a jun/2025	**33,4%** (≈ 56 mi)
Observatório Febraban/IPESPE, jun/2025 [18]	3.000 adultos, telefone com complemento online, 12–26/06/2025, ±1,8 p.p.	Já foi vítima de golpe ou de tentativa de golpe envolvendo a conta bancária (sem janela de tempo)	**39%**
Cetic.br, Painel TIC, dez/2025 [19]	2.500 usuários de internet de 16+, questionário online	Tentaram aplicar golpe usando seus dados pessoais; foi vítima de golpe que usou seus dados pessoais	**32%** e **20%**

Por que não se pode comparar, somar nem calcular tendência: as perguntas, os períodos e as bases são diferentes. O 33,4% é a união de cinco tipos de fraude e inclui "produto pago e não entregue"; o 15,8% mede um único tipo. O 39% da Febraban inclui tentativa e não tem janela de tempo, e vem de uma pesquisa encomendada pela associação dos bancos. Os 32% e 20% do Cetic.br são perguntas separadas. Nenhum desses números é "quantos brasileiros foram enganados por ano".

3.3 O Pix como cenário

Em 2025, o Pix registrou quase 80 bilhões de transações (+25,7% sobre 2024) e movimentou mais de R$ 35 trilhões (+33,8%). O Banco Central afirma que, dada a alta adesão e eficiência do Pix, fraudes e golpes têm "crescentemente utilizado o Pix como meio de distribuição". O relatório descreve as medidas de segurança, mas não publica o número de fraudes, golpes ou valores recuperados [20].

O Banco Mundial reporta uma estimativa de danos por fraude no Brasil de cerca de R$ 2,5 bilhões em 2022, dos quais 70% teriam envolvido o Pix, mas não indica a fonte original, nem quem arcou com as perdas, nem se o 70% é de casos ou de valor [21]. Usamos como ordem de grandeza, não como medida.

3.4 Subnotificação

O Anuário observa que os registros policiais "revelam uma provável enorme subnotificação" ao compará-los com as pesquisas de vitimização [1]. É uma interpretação razoável, mas não uma taxa: boletim e autodeclaração em pesquisa têm definições diferentes. Como referência de outro

país, um painel populacional holandês encontrou que apenas 11,8% dos eventos de fraude foram denunciados à polícia [22]. Não existe estimativa brasileira equivalente nas fontes que verificamos.

4 Como o golpe chega: da identidade à abordagem

O que os dados deixam ver é menos o "como" técnico e mais o ponto de contato: o golpista se apresenta como alguém, por algum canal, e pede algo. As pesquisas brasileiras permitem desenhar esse retrato por partes.

4.1 Identidade usada contra a vítima

Na pesquisa FBSP/Datafolha de junho de 2025, nos 12 meses anteriores, 11,4% (≈ 19,2 milhões) disseram que alguém se passou por eles no ambiente digital (aplicativos do governo, redes sociais ou aplicativos de mensagens), 7,0% (≈ 11,7 milhões) tiveram identidade ou perfil invadido e bloqueado em redes e aplicativos de mensagens, e 8,7% (≈ 14,7 milhões) tiveram o celular "clonado", isto é, o número usado por terceiros para aplicar golpes. São itens sobrepostos, que não devem ser somados, e a "clonagem" é a definição do questionário, sem verificação técnica [17].

Entre quem teve o celular roubado ou furtado (9,3% da população), 35,1% sofreram golpe de Pix ou boleto falso, contra 14,3% na população geral. Num modelo estatístico, o roubo do aparelho se associou a uma razão de chances de 3,66 (intervalo de confiança de 95%: 2,68 a 5,02) de ter sofrido algum dos sete crimes virtuais considerados. É razão de chances, não risco "3,7 vezes maior" [17].

4.2 O canal: aplicativos de mensagem e redes sociais

Entre os usuários de internet que relataram tentativa de golpe com seus dados, os aplicativos de mensagem foram o canal mais citado: 84% no resumo executivo do Cetic.br e 80% na tabela de detalhe (os dois números divergem no próprio material). Isso descreve o canal usado entre quem foi afetado, não o risco de cada faixa etária [19].

No Observatório Febraban, entre as pessoas que sofreram golpe ou tentativa envolvendo a conta bancária, 34% citaram o golpe do WhatsApp, em que alguém se passa por conhecido para pedir dinheiro; 31% a falsa central e 24% o golpe do Pix (respostas múltiplas) [18]. A Meta informou ter banido 6,8 milhões de contas do WhatsApp ligadas a centrais de golpe no primeiro semestre de 2025, sem recorte por país; é uma informação da própria empresa [23].

4.3 Dados pessoais e vazamentos

A pesquisa do FBSP interpreta que dados pessoais obtidos de forma ilícita (endereço, CPF, fotos, conversas, dados bancários) compõem uma "linha de produção" do estelionato, ao permitir que o criminoso se passe pela vítima perante amigos e familiares. É a leitura dos autores, e o relatório não testa essa relação causalmente [17].

4.4 Falso executivo e criadores de conteúdo

Fora do Brasil, o FBI recebeu 24.768 queixas de comprometimento de e-mail empresarial (BEC) em 2025, com perdas declaradas de US$ 3,05 bilhões (2024: 21.442 queixas, US$ 2,77 bilhões). São queixas voluntárias nos Estados Unidos, e a categoria do FBI é ampla: não equivale a "perfil clonado de executivo em rede social" [24] [25]. O relatório de violações da Verizon de 2026, que mede organizações, aponta o elemento humano em 62% das violações confirmadas e a engenharia social em cerca de 16% a 17% (o texto e o gráfico do mesmo resumo divergem) [26]. Para criadores de conteúdo, o Google descreveu em 2021 uma campanha global de falsas propostas de colaboração que sequestrava canais do YouTube, com 1,6 milhão de mensagens bloqueadas [27]. Nenhuma dessas fontes tem recorte para executivos ou criadores brasileiros.

> **Lacunas que a pesquisa não preencheu.** Não encontramos dado confiável sobre: (1) a parcela dos golpes que começa com informação pública do perfil; (2) a clonagem de perfis de executivos no Brasil; (3) golpes contra criadores brasileiros; (4) prevalência de golpe por faixa etária. Não vamos estimar o que as fontes não medem.

5 O que a evidência diz sobre prevenção

A pergunta prática é o que reduz o risco. A literatura e as fontes oficiais respondem em partes, e muitas das medidas recaem sobre bancos e plataformas, não sobre o usuário.

MEDIDA	O QUE A FONTE CONFIRMA	LIMITE DA EVIDÊNCIA
Regras do Pix: limite de R$ 200 por transação e R$ 1.000 por dia em dispositivo não cadastrado (desde nov/2024); bloqueio cautelar de até 72 h [20]	O Banco Central descreve as medidas e as datas em que entraram em vigor.	O documento não avalia o efeito dessas regras sobre as fraudes.
MED (Mecanismo Especial de Devolução) [28] [29]	O pedido de devolução pode ser feito mesmo quando a vítima autorizou a transação, desde que haja fraude ou golpe. Em apresentação de 14/10/2025, o Banco Central informou que, em 2025, foram recuperados em média 9,3% do valor contestado e reconheceu eficácia limitada, porque o bloqueio só alcança a primeira conta recebedora.	O período de 2025 é parcial; "recuperado em média" não é definido nos slides. Não misturar com o 8,2% que a imprensa publicou para o acumulado de 2021 a jun/2025, de origem indireta.

MEDIDA	O QUE A FONTE CONFIRMA	LIMITE DA EVIDÊNCIA
Verificação em duas etapas [30]	Em estudo de um ano com dados do Google, um código SMS para o telefone de recuperação bloqueou 96% do phishing em massa e 76% dos ataques direcionados; o aviso no aparelho, 99% e 90%.	Mede sequestro de contas Google. Não protege contra golpe em que a vítima faz o pagamento, como alerta o Banco Mundial [21]. Fonte com interesse corporativo.
Educação do usuário [31] [32]	Evidência mista. No Quênia (N = 1.000), dicas de como identificar golpes não melhoraram a distinção entre golpe e mensagem legítima, por excesso de cautela. Nos EUA (N = 2.000), educação online curta reduziu a suscetibilidade a fraude de investimento, mas o efeito se dissipou em seis meses sem lembrete.	Cenários experimentais, não perdas reais. Nenhum dos estudos é brasileiro.
Reembolso obrigatório (Reino Unido) [33]	Avaliação encomendada pelo regulador estimou que o valor mensal dos golpes em que a vítima autoriza o pagamento ficou cerca de 21% menor no primeiro ano (≈ £ 73 milhões por ano), com reembolso subindo de 54% para 65%.	Desenho não experimental, primeiro ano, consultoria contratada pelo regulador. Houve deslocamento para outros canais. Transposição ao Brasil é inferência.
Configurações de privacidade das redes [34] [35] [36]	A Cartilha do CERT.br orienta deixar a conta privada, limitar dados como telefone no perfil, ativar a verificação em duas etapas e revisar os aplicativos com acesso à conta. O WhatsApp e o LinkedIn documentam seus controles de quem vê o perfil e quem pode contatar. O WhatsApp informa que não é possível ocultar o número de telefone.	**Nenhuma fonte que verificamos mede se esses ajustes reduzem golpes.** São recomendações institucionais, sem dado de eficácia.

Conclusão da seção

As melhores evidências de redução de golpes tratam de controles de bancos e plataformas e de proteção de contas, não de golpes em que a vítima autoriza o pagamento. Sobre o que o próprio usuário pode ajustar no perfil, há recomendação oficial, mas não há medida de eficácia.

6 O que isso significa para quem tem perfil exposto

Esta seção é a posição da lwlabs, não um resultado de pesquisa. Ela relaciona os fatos acima ao serviço Personal Glasswing e deve ser lida como argumento.

Três pontos se apoiam nos dados. **Primeiro**, o golpe começa por uma identidade: nas pesquisas brasileiras, personificação, perfil invadido e número clonado atingem de 7% a 11% da população, e os aplicativos de mensagem são o canal mais citado. **Segundo**, as proteções oficiais existem e são gratuitas, mas estão espalhadas entre plataformas, com nomes e caminhos diferentes, e mudam com o tempo. **Terceiro**, ninguém mediu quanto elas reduzem o risco.

Por isso, a promessa honesta do Personal Glasswing não é “eliminar golpes” nem “tapar o caminho de X% dos ataques”. É reduzir, de forma documentada e verificável, as portas que o próprio perfil deixa abertas: quem pode abordar, quem acha o seu contato, quais aplicativos ainda têm acesso. O serviço lê as configurações sem alterá-las, classifica cada uma por risco, propõe a correção e só a aplica com a aprovação do cliente, voltando depois para revisar.

O que **não** afirmamos: que a maioria dos golpes começa pelo perfil, que ajustar privacidade impede golpes em que a vítima autoriza o pagamento, ou que o Brasil seja o país com mais golpes. Quando houver evidência melhor, este documento será atualizado.

7 Limitações

- **Autodeclaração e definições diferentes.** Quase todos os números de vítimas vêm de pesquisas com perguntas, períodos e bases distintos; não formam série.
- **Fontes comerciais.** Rankings de segurança vêm de empresas que vendem proteção, e a Febraban é a associação dos bancos. Indicamos isso em cada caso.
- **Fontes secundárias.** Cinco itens usados ou citados vieram de relatos de terceiros e estão marcados como Secundária.
- **Cobertura incompleta.** Não obtivemos dado oficial de golpe da Polícia Federal, do CERT.br nem da Senacon, e o Banco Central não publica, nos documentos consultados, o número de fraudes no Pix.
- **Datas.** Pesquisa e conferência concluídas em 29/11/2026. Páginas de ajuda de plataformas mudam sem aviso.
- **Correções.** Se você encontrar um número que não confere com a fonte, escreva para o contato do último quadro. Corrigiremos e registraremos a mudança.

Anexo A: afirmações populares e o que os dados sustentam

AFIRMAÇÃO QUE CIRCULA	VEREDITO	O QUE A FONTE DIZ
“O Brasil é o país com mais golpes online do mundo.”	**Não sustentada**	Nenhum ranking de golpe, fraude ou phishing verificado o coloca em 1º. Seção 2.
“39% dos brasileiros foram vítimas de golpe.”	**Impreciso**	Observatório Febraban: 39% dos adultos entrevistados já foram vítimas de golpe *ou de tentativa* envolvendo a conta bancária, sem janela de tempo [18].
“1 em cada 3 brasileiros sofreu golpe digital com prejuízo.”	**Parcialmente correto**	33,4% na pesquisa de jun/2025, que reúne cinco tipos de fraude, inclusive produto pago e não entregue. Os valores em reais citados na imprensa são estimativas autodeclaradas e referem-se a itens específicos [17].
“Os golpes cresceram 429,8%.”	**Parcialmente correto**	Os *registros de estelionato* cresceram 429,8% entre 2018 e 2025; a série mistura efeito da Lei 14.155/2021 e da pandemia [1].
“Quem tem o celular roubado tem 3,7 vezes mais risco de golpe.”	**Impreciso**	3,66 é razão de chances, não risco. A diferença observada é de 35,1% contra 14,3% no golpe de Pix ou boleto [17].
“Brasil lidera o ranking mundial de vítimas de fraude (Veriff).”	**Enganosa**	Pesquisa com três países e pessoas que já sofreram fraude; não é ranking mundial [9].
“Ajustar a privacidade das redes evita golpes.”	**Sem evidência medida**	Há recomendação oficial, mas nenhuma fonte verificada mede o efeito. Seção 5.

Referências

Todas as páginas e documentos foram consultados em 29/11/2026. Primária: documento original aberto e lido. Secundária: confirmado apenas por relato de terceiros.

1. FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA. *20º Anuário Brasileiro de Segurança Pública 2026*. São Paulo: FBSP, 2026. Tabela 17 (p. 120), texto (p. 121–125), Gráfico 33 (p. 122), Quadro 04 (p. 125). forumseguranca.org.br/wp-content/uploads/2026/07/anuario-2026.pdf PRIMÁRIA
2. FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA; DATAFOLHA. *Medo do crime e eleições 2026: os gatilhos da insegurança*. São Paulo: FBSP, 2026. Resumo p. 9; relatório completo p. 11 e 22. publicacoes.forumseguranca.org.br/handle/fbsp/303 PRIMÁRIA
3. KASPERSKY (SECURELIST). *Spam and phishing in 2025*. 11 fev. 2026. securelist.com/spam-and-phishing-report-2025/118785/ PRIMÁRIA
4. ZSCALER THREATLABZ. *2025 Phishing Report*. Zscaler, 2025 (dados de 2024). zscaler.com/learn/2025-phishing-report PRIMÁRIA
5. TRUECALLER. *Spam and Fraud Report 2025*, conforme divulgado por ANTARA/ACN Newswire: the machine era of spam calls, 6 maio 2026. en.antaranews.com/amp/news/414776 SECUNDÁRIA
6. BONETS, V. Brasil está entre dez países que mais perdem dinheiro com golpes digitais. *CNN Brasil*, 24 jul. 2026 (análise da PP Tech sobre o relatório GASA/Feedzai 2025; a tabela original é restrita a membros e não foi consultada). cnnbrasil.com.br/nacional/brasil/brasil-esta-entre-dez-paises-que-mais-perdem-dinheiro-com-golpes-digitais/ SECUNDÁRIA
7. SOCRADAR. *LATAM Regional Threat Landscape Report 2025*. 2025. socradar.io/wp-content/uploads/2025/05/LATAM-Regional-Threat-Landscape-Report-2025.pdf PRIMÁRIA
8. HIYA. Brazilians lead the world with 28 spam calls per month. *Hiya Blog*, 17 jun. 2025. blog.hiya.com/brazilians-lead-the-world-with-28-spam-calls-per-month PRIMÁRIA
9. VERIFF. *Veriff Fraud Index 2025* (e-book) e comunicado de 7 out. 2025. veriff.com/resources/ebooks/veriff-fraud-index-2025 PRIMÁRIA
10. SOUSA, J. Brasil está no topo do ranking mundial de vítimas de fraudes digitais. *Canaltech*, 30 out. 2025 (reportagem que popularizou o "1º lugar"; contém imprecisões em relação ao documento original). canaltech.com.br/seguranca/brasil-esta-no-topo-do-ranking-mundial-de-vitimas-de-fraudes-digitais/ SECUNDÁRIA
11. GASA; SCAMADVISER; WHOSCALL. 1-in-3 Brazilians targeted by scammers in the last 12 months: State of Scams in Brazil 2024. 30 out. 2024. gasa.org/knowledge-base/blog/1-in-3-brazilians-targeted-by-scammers-in-2024-state-of-scam-report PRIMÁRIA
12. GASA. New report reveals Brazilians face 252 scam encounters annually despite high confidence in spotting scams. 12 nov. 2025. gasa.org/knowledge-base/blog/new-report-reveals-brazilians-face-252-scam-encounters-annually-despite-high-confidence-in-spotting PRIMÁRIA
13. GLOBAL ANTI-SCAM ALLIANCE (GASA); FEEDZAI. Global scams on the rise: over half of adults worldwide report scam encounters, 23% lost money. 7 out. 2025. gasa.org/knowledge-base/blog/global-scams-on-the-rise-over-half-of-adults-worldwide-report-scam-encounters PRIMÁRIA
14. KASPERSKY, conforme DURANZI, B. Fique atento: Brasil registra aumento de 80% em tentativas de golpe via SMS. *Viva*, 13 set. 2025; e comunicado Kaspersky LATAM, 10 set. 2025 (1,29 bilhão de bloqueios na América Latina; o número do Brasil não consta no comunicado). viva.com.br/tecnologia/fique-atento-brasil-registra-aumento-de-80-em-tentativas-de-golpe-via-sms.html SECUNDÁRIA
15. SUMSUB. *Global Fraud Index 2025: methodology* (metodologia, fonte primária). A posição do Brasil (101ª entre 112) vem de COINSPEAKER, 5 nov. 2025, e não foi confirmada no original. sumsub.com/global-fraud-index/methodology-2025/ SECUNDÁRIA

16. BRASIL. *Lei nº 14.155, de 27 de maio de 2021*. Diário Oficial da União, 28 maio 2021. planalto.gov.br/ccivil_03/_ato 2019-2022/2021/lei/L14155.htm PRIMÁRIA

17. FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA; DATAFOLHA. *Pesquisa de vitimização e percepção sobre violência e segurança pública 2025: um olhar sobre crime patrimonial e violência*. São Paulo: FBSP, ago. 2025. Gráfico 1 (p. 9), p. 13–20, anexo (p. 26). publicacoes.forumseguranca.org.br/items/fb7046a0-c12c-4a9b-bab8-1b 8fdfa2c561 PRIMÁRIA

18. FEBRABAN; IPESPE. *Observatório Febraban: Pesquisa Semestral Educação Financeira no Brasil, julho 2025*. São Paulo: Febraban, 2025. p. 4 e 62–64. cmsarquivos.febraban.org.br/Arquivos/documentos/PDF/observatorio julho 2025.pdf PRIMÁRIA

19. NÚCLEO DE INFORMAÇÃO E COORDENAÇÃO DO PONTO BR (NIC.br); CETIC.br. *Privacidade e Proteção de Dados Pessoais 2025: resumo executivo (Painel TIC)*. São Paulo: NIC.br, 2026. p. 4 e 6; tabela PR21. cetic.br/pt/ti cs/privacidade-e-protecao-de-dados-pessoais/2025/usuarios/PR21/ PRIMÁRIA

20. BANCO CENTRAL DO BRASIL. *Relatório de Gestão do Pix 2023–2025*. Brasília: BCB, 2026. p. 10–14. bcb.gov.br/co ntent/estabilidadefinanceira/pix/relatorio_de_gestao_pix/relatorio_gestao_pix_2026.pdf PRIMÁRIA

21. WORLD BANK. *Fraud Risks in Fast Payments*. Focus Note. Washington, DC: Payment Systems Development Group, out. 2023. p. 6 e 18 do PDF. fastpayments.worldbank.org/sites/default/files/2023-10/Fraud in Fast Paymen ts_Final.pdf PRIMÁRIA

22. KONING, L.; JUNGER, M.; VELDKAMP, B. Reporting fraud victimization to the police: factors that affect whether victims report. *Psychology, Crime & Law*, 2025. DOI 10.1080/1068316X.2025.2468347. PRIMÁRIA

23. META. Novas ferramentas e dicas do WhatsApp para combater os golpes por mensagem. *Meta Brasil*, 5 ago. 2025. about.fb.com/br/news/2025/08/novas-ferramentas-e-dicas-do-whatsapp-para-combater-os-golpes-por-mensagem/ PRIMÁRIA

24. FEDERAL BUREAU OF INVESTIGATION. Internet Crime Complaint Center. *2025 Internet Crime Report*. p. 6–8, 25–26. ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf PRIMÁRIA

25. FEDERAL BUREAU OF INVESTIGATION. Internet Crime Complaint Center. *2024 Internet Crime Report*. p. 4, 9–10, 18–19. ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf PRIMÁRIA

26. VERIZON. *2026 Data Breach Investigations Report: Executive Summary*. Verizon Business, 2026. p. 2, 5 e 11. veriz on.com/business/resources/executivebriefs/dbir-2026-executive-summary.pdf PRIMÁRIA

27. GOOGLE THREAT ANALYSIS GROUP (SHEN, A.). Phishing campaign targets YouTube creators with cookie theft malware. *Google Blog*, 20 out. 2021. blog.google/threat-analysis-group/phishing-campaign-targets-youtube-crea tors-cookie-theft-malware/ PRIMÁRIA

28. BANCO CENTRAL DO BRASIL. *Circuito Pix, Dia 1: Aprimoramentos no Mecanismo Especial de Devolução (MED 2.0)*. Apresentação, Brasília, 14 out. 2025. Slide 4. bcb.gov.br/content/estabilidadefinanceira/pix/MED/MED_2-0_C ircuito_Pix-Dia_1.pdf PRIMÁRIA

29. BANCO CENTRAL DO BRASIL. *Guia de implementação dos procedimentos de devolução no Pix, com ênfase no MED*, versão 4.3. Seção 4.2.3, p. 12–13. bcb.gov.br/content/estabilidadefinanceira/pix/Guia_MED.pdf PRIMÁRIA

30. THOMAS, K.; MOSCICKI, A. New research: how effective is basic account hygiene at preventing hijacking. *Google Security Blog*, 17 maio 2019. security.googleblog.com/2019/05/new-research-how-effective-is-basic.html PRIMÁRIA

31. KUBILAY, E.; RAIBER, E.; SPANTIG, L.; CAHLÍKOVÁ, J.; KAARIA, L. Can you spot a scam? Measuring and improving scam identification ability. *Journal of Development Economics*, v. 165, 103147, 2023. DOI 10.1016/j.jdeveco.2023.103147. PRIMÁRIA

32. BURKE, J.; KIEFFER, C.; MOTTOLA, G.; PEREZ-ARCE, F. Can educational interventions reduce susceptibility to financial fraud? *Journal of Economic Behavior & Organization*, v. 198, p. 250–266, 2022. DOI 10.1016/j.jebo.2022.03.028. PRIMÁRIA

33. FRONTIER ECONOMICS. *Independent Evaluation of APP Scam Policies: Summary Report*. Londres, para o Payment Systems Regulator, 1 jul. 2026. p. 8–10, 33–45. frontier-economics.com/media/2ctd3jq2/app-fraud-evalu

ation-final-summary-report-26-06-26.pdf PRIMÁRIA

34. CERT.br/NIC.br. *Cartilha de Segurança para Internet: fascículo Redes Sociais*. São Paulo: NIC.br, fev. 2023. p. 5–12. cartilha.cert.br/fasciculos/redes-sociais/fasciculo-redes-sociais.pdf PRIMÁRIA
35. WHATSAPP. Central de Ajuda: como mudar suas configurações de privacidade; como se proteger de golpes e mensagens suspeitas; sobre a verificação em duas etapas. Páginas consultadas em 29 nov. 2026. faq.whatsapp.com PRIMÁRIA
36. LINKEDIN. Central de Ajuda: what people can see on your profile. Página consultada em 29 nov. 2026. linkedin.com/help/linkedin/answer/a545600/what-people-can-see-on-your-profile PRIMÁRIA

Personal Glasswing

Auditoria de privacidade anti-golpes dos seus perfis: lemos as configurações de cada rede, mostramos o que está aberto e fechamos com a sua aprovação.

personalglasswing.com · lucaswetten@gmail.com · (11) 97497-0281

Encontrou um número que não confere com a fonte? Escreva para o e-mail acima. Corrigimos e registramos a mudança. Este documento é uma pesquisa da lwlabs e não constitui aconselhamento jurídico ou financeiro.