ESTUDO - GOLPES E FRAUDES CONTRA O CONSUMIDOR DE TELECOM
PARTE 1 - IDENTIFICAÇÃO DE CASOS NA EUROPA, ESTADOS UNIDOS E BRASIL

Superintendência de Relações com Consumidores (SRC)

Gerência de Interações Institucionais, Satisfação e Educação para o Consumo (RCIC)

Brasília-DF, Setembro/2020

O presente trabalho procura identificar golpes e fraudes comumente realizados contra os consumidores dos serviços de telecomunicações, bem como procede a um benchmark *internacional e indicação das iniciativas nacionais de prevenção desses embustes. Essa análise foi desenvolvida no contexto de* Key Intelligence Topic *(KIT) definido no âmbito das competências da SRC na execução das atividades do macroprocesso de Inteligência Institucional. Produzido pela equipe da SRC com o objetivo de contribuir para o detalhamento do quadro das relações de consumo no setor de telecomunicações a fim de subsidiar ações regulatórias relacionadas ao tema. As conclusões ora apresentadas não representam, necessariamente, a posição final da Agência a respeito da matéria.*

Elaboração: Fabio Vianna Velloso e Pryscilla Oliveira.

Revisão: Fábio Koleski.

Este estudo tem por finalidade a identificação de golpes e fraudes frequentemente perpetrados contra os consumidores por intermédio dos serviços de telecomunicações em três mercados distintos: Europa, Estados Unidos e Brasil. Ele é a primeira parte de uma abordagem mais ampla, que será seguida pela identificação de iniciativas de prevenção realizadas por agências reguladoras e as maiores prestadoras de serviços de telecomunicações, nesses mesmos contextos.

A. GOLPES E FRAUDES CONHECIDOS

Há uma miríade de golpes e fraudes que se dão por meio das redes de telecomunicações, não tendo esse estudo a pretensão de exaurir os tipos de golpes e fraudes existentes nos contextos selecionados: o da Europa, o dos Estados Unidos e o do Brasil. Além de sua imensa variedade, há constante criação de novos tipos de fraudes e golpes, bem como a renovação de formas já existentes ou mesmo caídas em desuso.

Muitos golpes, em vez de se concentrarem na tentativa de quebra de mecanismos de segurança sofisticados de empresas, como instituições bancárias, por exemplo, focam-se em explorar a fragilidade dos usuários.[1] Entre os mecanismos empregados pelos criminosos virtuais para iludir os usuários está a engenharia social, técnica por meio da qual se procura persuadir as pessoas a abrirem *links* de *sites* infectados, acessar páginas falsas, fornecer dados confidenciais/sensíveis, infectar dispositivos por meio de *malware*[2], executar código maliciosos, bem como se aproveitar da falta de conhecimento do usuário.[3] Esse é um método altamente difundido, indicando a Kaspersky, empresa internacional de segurança virtual, que praticamente todo golpe virtual utiliza-se de algum método de engenharia social.[4] Ademais, a engenharia social é muito usada em golpes por *e-mail*, que é um meio altamente utilizado para golpes por ser um recurso simples para a difusão de *malware*.[5]

Os golpes também causam prejuízos financeiros altos. Segundo pesquisa de 2019 realizada pela Europol's European Cybercrime Centre, em conjunto com a empresa de segurança Trend Micro, as fraudes realizadas globalmente por meio das redes de telecom alcançam a soma de US$ 32,7 bilhões em perdas anualmente, sendo que a maioria dos prejuízos é absorvido pelas próprias empresas de telecomunicações, o que acaba por dificultar o compartilhamento de inteligência transnacional e, consequentemente, a prisão de fraudadores. O relatório aponta ainda que esse tipo de fraude é "cada vez mais originada em países normalmente considerados de 'terceiro mundo' ou estados falidos", "sendo usada para sustentar economias em decadência". Ademais, as fraudes realizadas por meio das redes de telecom são de baixo risco, aproveitando-se do fato de que, diferentemente dos crimes financeiros, não precisam contornar controles rigorosos contra a lavagem de dinheiro e são praticados com o uso de equipamentos *hackers* baratos e de fácil acesso.[6]

---

[1] CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL - CERT.br. *Cartilha de Segurança para Internet - Golpes na Internet*.

[2] "*Malware* é a abreviação de '*software* malicioso' (em inglês, *malicious software*) e se refere a um tipo de programa de computador desenvolvido para infectar o computador de um usuário legítimo e prejudicá-lo de diversas formas. O *malware* pode infectar computadores e dispositivos de várias maneiras (...)". Aspas do autor. Grifos nossos. KASPERSKY. *Aprenda sobre malware e como proteger todos os seus dispositivos contra eles*.

[3] CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL - CERT.br. *Cartilha de Segurança para Internet - Golpes na Internet*. KASPERSKY. *Engenharia social - Definição*.

[4] KASPERSKY. *Engenharia social - Definição*.

[5] CONVERGÊNCIA DIGITAL. *Brasil teve quase dois bilhões de ameaças cibernéticas de e-mail em 2019*, 03/03/2020.

[6] Aspas do autor. Tradução nossa. No original: "Telecom fraud, the report says, 'is increasingly originating in countries normally considered 'third world' or failed states,' and is more and more 'being used to prop up failing economies.'". ORGANIZED CRIME AND CORRUPTION REPORTING PROJECT - OCCRP. *Report: US$32.7 Billion Lost in Telecom Fraud Annually*, 22/03/2019.

1. GOLPES E FRAUDES NA EUROPA

Na Europa, um estudo publicado em janeiro de 2020 e realizado pela Agência Executiva para os Consumidores, a Saúde, a Agricultura e os Alimentos (Chafea) em nome da Direção-Geral da Justiça e dos Consumidores da Comissão Europeia, identifica nove tipos de golpes e fraudes[7] distribuídos em três categorias:[8]

Tabela 1 - Categorias e tipos de golpes e fraudes identificados pela Comissão Europeia

	CATEGORIA		
	Golpes em compras	**Roubo de identidade**	**Fraude monetária**
TIPO	1. Consumidor pensa solicitar produtos/serviços gratuitos ou relativamente baratos, mas é induzido a aderir a uma assinatura mensal cara	4. Pessoa passando-se por representante de uma instituição legítima, como um órgão governamental, um banco ou um prestador de serviços de telecomunicações, faz contato (presencialmente, por telefone, por *e-mail*, etc), solicitando à pessoa contatada que forneça ou confirme informações pessoais	6. Promete-se recebimento de produtos, serviços, descontos ou ganhos financeiros mediante o investimento ou a transferência de valores
	2. Consumidor compra produtos/serviços pensando tratar-se de um bom negócio, mas os produtos/serviços nunca são recebidos ou são falsos ou inexistentes	5. Pessoa realiza abordagem (presencial, por telefone, por *e-mail*, etc) ou ao acessar um *site* a vítima é informada sobre um suposto problema do dispositivo de acesso ou da conexão e, em seguida, são solicitadas informações pessoais ou dados bancários para que o problema seja resolvido	7. Realização de compra de ingressos para shows, eventos ou viagens que nunca são recebidos ou revelam-se falsos
	3. Consumidor recebe fatura falsa para pagamento de produtos que não solicitou	-	8. Pessoa passando-se por representante de uma instituição legítima, como um órgão governamental, um banco ou um prestador de serviços de telecomunicações, faz contato alegando que você tem problemas com sua documentação ou sua conta e faz ameaças caso você não pague para resolver o problema
	-	-	9. Notificação de ganho em loteria ou competição, mas necessidade de pagamento de taxa ou compra de produto para que o prêmio seja resgatado

FONTE: COMISSÃO EUROPEIA - Direção-Geral da Justiça e dos Consumidores. *Survey on "scams and fraud experienced by consumers" - Final report*, Janeiro 2020, p. 10.

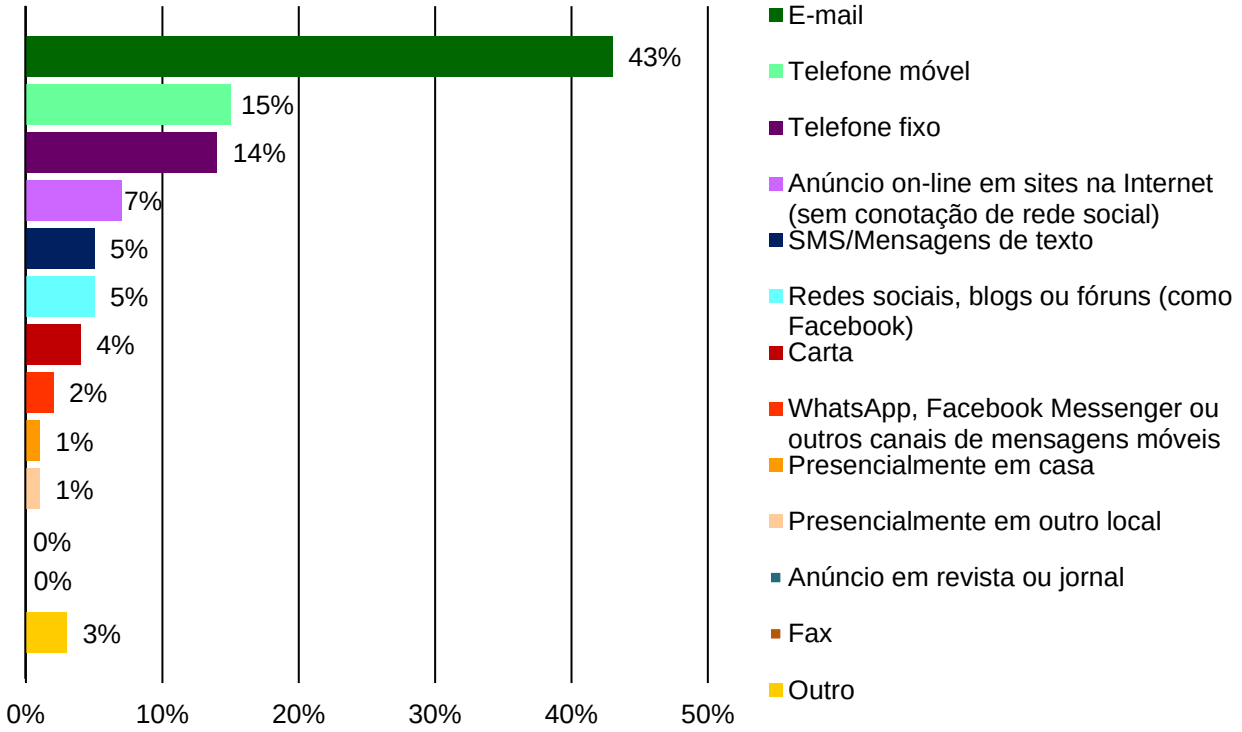
[7] A definição de golpes e fraudes adotada pelo estudo é ampla "incluindo ocasiões em que as pessoas podem ter visto uma fraude ou golpe, mas não se tornaram uma vítima ao reagir". Tradução nossa. No original: "(…) considering the broad definition of scams and fraud applied for this survey, which includes occasions where people may have seen a fraud or scam but did not become a victim by reacting to it". COMISSÃO EUROPEIA - Direção-Geral da Justiça e dos Consumidores. *Survey on "scams and fraud experienced by consumers" - Final report*, Janeiro 2020, p. 15.

[8] COMISSÃO EUROPEIA - Direção-Geral da Justiça e dos Consumidores. *Survey on "scams and fraud experienced by consumers" - Final report*, Janeiro 2020, p. 2 e 10.

Segundo o estudo, nos últimos dois anos, 39% dos golpes/fraudes estiveram relacionados à categoria da fraude monetária, 33% a do roubo de identidade e 23% ao dos golpes em compras.[9] Além disso, pouco mais da metade dos europeus (56%) experimentou pessoalmente pelo menos um dos nove tipos de golpes/fraudes nos últimos dois anos e aproximadamente um terço (34%) experimentou dois ou mais tipos. Em média, 1,26 foi o número de casos de golpes/fraudes experimentados pelos europeus nos últimos dois anos.[10]

No que tange ao meio pelo qual ocorrem os golpes/fraudes, induzir o consumidor a aderir a uma assinatura mensal, a compra de produtos/serviços que nunca são recebidos ou são falsos/inexistentes e a compra de ingressos falsos ou nunca recebidos[11] podem tanto ocorrer durante compras por meio da internet ou não[12]. Ademais, os canais de comunicação mais comuns pelos quais as pessoas experimentam práticas enganosas ou fraudulentas são:

Gráfico 1 - Canais de comunicação utilizados para a prática de golpes/fraudes na Europa



FONTE: elaboração própria a partir de dados da COMISSÃO EUROPEIA - Direção-Geral da Justiça e dos Consumidores. *Survey on "scams and fraud experienced by consumers" - Final report*, Janeiro 2020, p. 30-31.

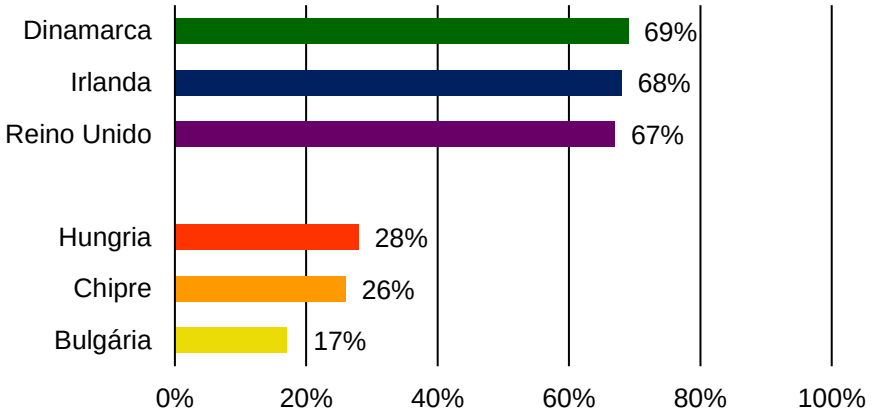
[9] COMISSÃO EUROPEIA - Direção-Geral da Justiça e dos Consumidores. *Survey on "scams and fraud experienced by consumers" - Final report*, Janeiro 2020, p. 11.
[10] COMISSÃO EUROPEIA - Direção-Geral da Justiça e dos Consumidores. *Survey on "scams and fraud experienced by consumers" - Final report*, Janeiro 2020, p. 10.
[11] Respectivamente os golpes/fraudes 1, 2 e 7 listados na Tabela 1.
[12] De fato, a pesquisa traz a nomenclatura *on-line* e *off-line*. COMISSÃO EUROPEIA - Direção-Geral da Justiça e dos Consumidores. *Survey on "scams and fraud experienced by consumers" - Final report*, Janeiro 2020, p. 10.

A pesquisa deixa claro o protagonismo do *e-mail* como o canal mais utilizado pelos golpistas na Europa. Ainda no âmbito do mundo *on-line*, os anúncios em *sites* vêm em quarto lugar, estando à frente de outros canais não *on-line*, como SMS/mensagens de texto ou cartas. Apesar disso, o telefone continua sendo um canal significativo. Nesse sentido, manifestamente observa-se que golpes e fraudes não estão restritos apenas aos meios *on-line*, mas também são regularmente praticados pelo serviços telefonia, tanto fixos, quanto móveis.[13]

O estudo aponta ainda que os canais de comunicação através dos quais os golpes e fraudes ocorreram diferem entre grupos sociodemográficos: jovens e pessoas com educação superior que compram *on-line*, isto é, pessoas tipicamente mais ativas *on-line* estão mais expostas a fraudes/golpes por esse meio, enquanto pessoas menos ativas na internet, como os mais idosos e pessoas com menor nível de escolaridade e que não compram *on-line* estão mais expostas a golpes/fraudes por telefone. Aduz o estudo que essas descobertas provavelmente derivam mais do comportamento das faixas demográficas do que de uma estratégia deliberada de direcionamento dos canais pelos golpistas/fraudadores.[14]

Quantos aos países, como se pode observar no gráfico abaixo, de forma geral, Dinamarca, Irlanda e Reino Unido foram os países em que os cidadãos mais experimentaram golpes/fraudes, enquanto Bulgária, Chipre e Hungria foram os países em que menos pessoas tiveram essa experiência.[15]

Gráfico 2 - Percentual de europeus que experimentaram pessoalmente qualquer tipo de fraude/golpe nos últimos dois anos - Países mais e menos afetados



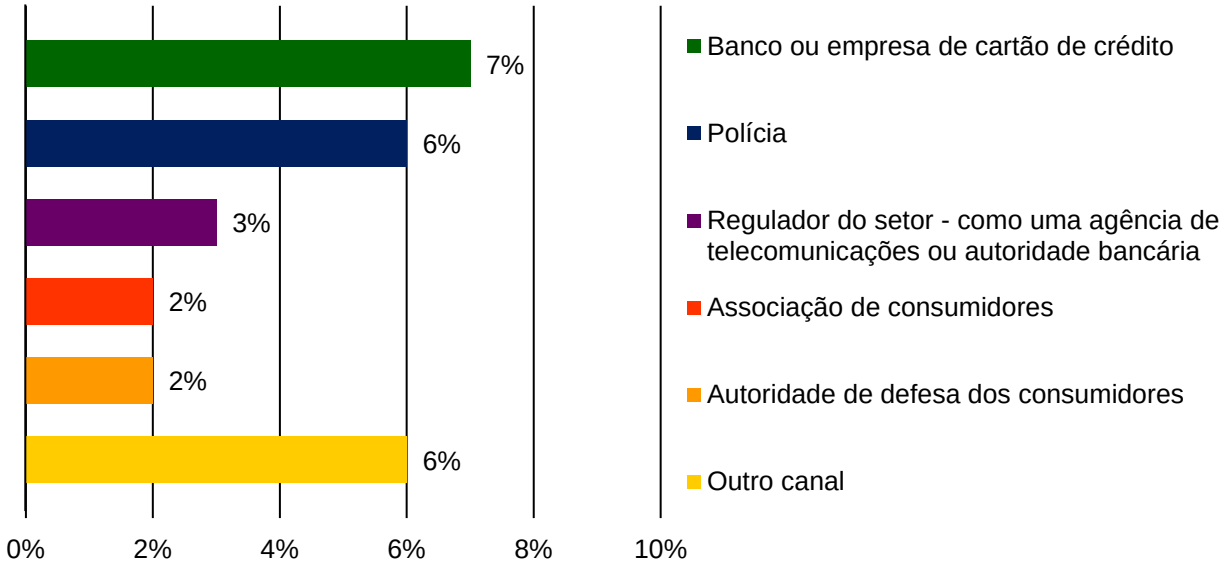
FONTE: elaboração própria a partir de dados da COMISSÃO EUROPEIA - Direção-Geral da Justiça e dos Consumidores. *Survey on "scams and fraud experienced by consumers" - Final report*, Janeiro 2020, p. 12-13.

[13] COMISSÃO EUROPEIA - Direção-Geral da Justiça e dos Consumidores. *Survey on "scams and fraud experienced by consumers" - Final report*, Janeiro 2020, p. 30-31.
[14] COMISSÃO EUROPEIA - Direção-Geral da Justiça e dos Consumidores. *Survey on "scams and fraud experienced by consumers" - Final report*, Janeiro 2020, p. 30-31.
[15] COMISSÃO EUROPEIA - Direção-Geral da Justiça e dos Consumidores. *Survey on "scams and fraud experienced by consumers" - Final report*, Janeiro 2020, p. 12-13.

No que concerne ao registro de reclamações sobre esses golpes e fraudes, a pesquisa indica que apenas cerca de um quinto (21%) das vítimas reportou o caso a uma autoridade oficial, enquanto uma em cada quatro (41%) não relataram a fraude a ninguém. Por outro lado, 38% das vítimas relatou a fraude a amigos ou familiares, mas não a uma autoridade. Ademais, os dados da pesquisa sobre o não reporte de ocorrências a autoridades parece confirmar indicações de trabalhos anteriores, como os estudos de 2017, *Fraud in cross-border e-commerce* (Fraude no comércio eletrônico transfronteiriço) da ECC-Net e *The growing threat of online fraud* (A ameaça crescente de fraude *on-line*) do Comitê de Contas Públicas da Câmara dos Comuns do Parlamento britânico, ambos indicando que a maioria não reporta ter sido vítima de golpe/fraude a qualquer autoridade.[16]

Por seu turno, entre as vítimas que indicaram ter relatado o golpe/fraude, o relato foi feito às seguinte autoridades/organizações:

Gráfico 3 - Reporte de golpe/fraude por tipo de autoridade na Europa



FONTE: elaboração própria a partir de dados da COMISSÃO EUROPEIA - Direção-Geral da Justiça e dos Consumidores. *Survey on "scams and fraud experienced by consumers" - Final report*, Janeiro 2020, p. 35-36.

Como visto, de forma geral, os países europeus com maiores incidências de golpes e fraudes são: Reino Unido, Irlanda e Dinamarca. Nesse sentido, no estudo seguinte, a presente análise examina os modelos de informação públicos e privados desses países, levando em consideração as informações encontradas nos *sites* dos órgãos reguladores do setor de telecom e na maior prestadora de serviços de telecomunicações de cada um dos três países.

[16] COMISSÃO EUROPEIA - Direção-Geral da Justiça e dos Consumidores. *Survey on "scams and fraud experienced by consumers" - Final report*, Janeiro 2020, p. 35.

2. GOLPES E FRAUDES NOS ESTADOS UNIDOS

Os órgãos de controle americanos, a Comissão Federal de Comunicações (Federal Communications Commission - FCC) e a Comissão Federal de Comércio (Federal Trade Commission - FTC), apontam para uma variedade de golpes e fraudes que ocorrem nos Estados Unidos.

Em especial a FTC mantém uma listagem crescente de informações sobre golpes/fraudes com ocorrência relatada no território americano.[17] No momento da produção desse estudo essa listagem contemplava um total de 34 páginas e 70 entradas somente no corrente ano (da página 1 à 4).[18] Nessa lista, em geral, são apresentados como esses golpes/fraudes ocorrem, como evitá-los e como registrar sua ocorrência perante a FTC.[19] Entre outros, pode-se destacar algumas temáticas pelas quais esses golpes/fraudes perpassam:[20]

- Loterias e prêmios;
- Roubo de identidade;
- Saúde;
- Investimentos;
- Ofertas de crédito e empréstimos;
- Transferência de valores;
- Compras;
- Caridade;
- Imigração;
- Relacionamentos *on-line*;
- *Phishing*;
- Fraude telefônica; e
- Viagens.[21]

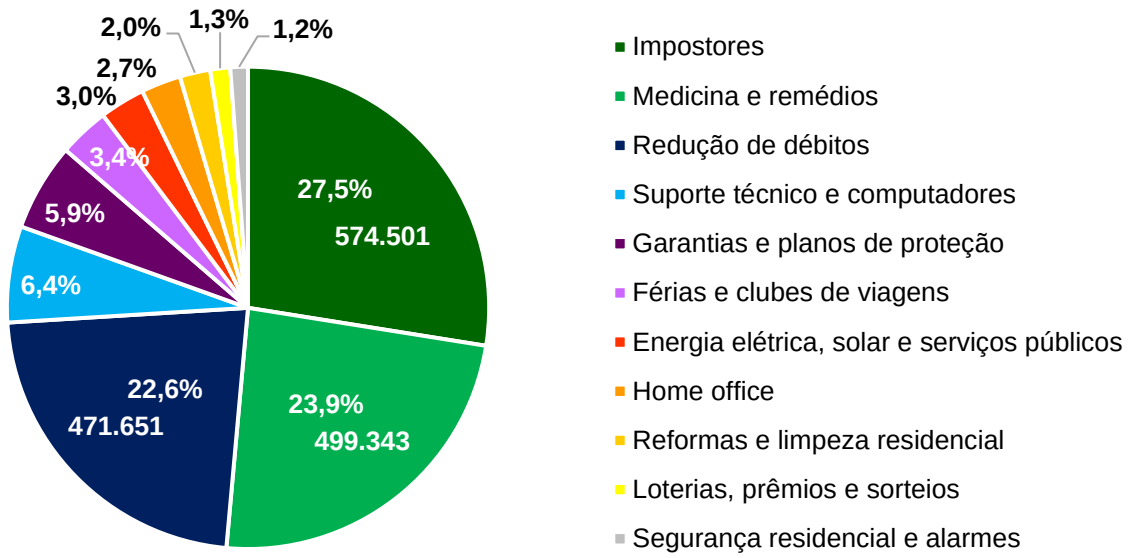
A Trend Micro apontou que em 2019 os Estados Unidos foram o país líder em *ransomware*[22], com 34,36% das ameaças mundiais e em disseminação de ameaças cibernéticas por *e-mail*, com a cifra de 10 bilhões, mais que o dobro do segundo colocado, a China, com 4 bilhões.[23] A FTC, por seu turno, indicou que, compilando os dados dos 3,2 milhões de relatos de golpes/fraudes por ela recebidos em 2019, os golpes/fraudes mais comumente praticados foram

[17] FEDERAL TRADE COMMISSION - FTC. Consumer information. *Scams*.
[18] Tendo em vista que essa lista é crescente, foram computadas 34 páginas e 70 entradas em 2020 na data de 25/09/2020. FEDERAL TRADE COMMISSION - FTC. Consumer information. *Scams*.
[19] FEDERAL TRADE COMMISSION - FTC. Consumer information. *Scams*.
[20] FEDERAL TRADE COMMISSION - FTC. Consumer information. *Scams - Brownse Scams by Topic*.
[21] FEDERAL TRADE COMMISSION - FTC. Consumer information. *Scams - Brownse Scams by Topic*.
[22] "*Ransomware* é um *software* malicioso que infecta seu computador e exibe mensagens exigindo o pagamento de uma taxa para fazer o sistema voltar a funcionar". Grifos nossos. KASPERSKY. *O que é ransomware?*.
[23] CONVERGÊNCIA DIGITAL. *Brasil teve quase dois bilhões de ameaças cibernéticas de e-mail em 2019*, 03/03/2020.

os golpes de impostor, que geraram mais US$ 667 milhões em prejuízos.[24] Nesses golpes, um impostor se passa por um interesse romântico, um órgão do governo, uma empresa bem conhecida ou até mesmo um familiar em uma emergência, induzindo assim a vítima a enviar valores.[25] Ademais, os cartões de presente foram o meio mais frequente de envio de dinheiro aos golpistas e os impostores mais comumente se passaram pelo órgão do seguro social do governo americano (Social Security Administration - SSA).[26] Com relação ao meio, o telefone foi o recurso mais usado para perpetrar as fraudes.[27]

Outros dados, também compilados pela FTC e relativos a reclamações registradas por violações à lista nacional de Não Perturbe (Do Not Call Registry), indicam que, das reclamações com temas reportados, conforme demonstrado em gráfico abaixo, aquelas de impostores foram as mais representativas com 574.501 reclamações ou 27,5% do total de reclamações registradas com indicação de tema no ano fiscal[28] de 2019. Adicionalmente, chama a atenção, também conforme disposto em gráficos abaixo, que a maioria das ligações feitas em descumprimento ao Do Not Call Registry foi realizada por meio de *robocall*.[29]

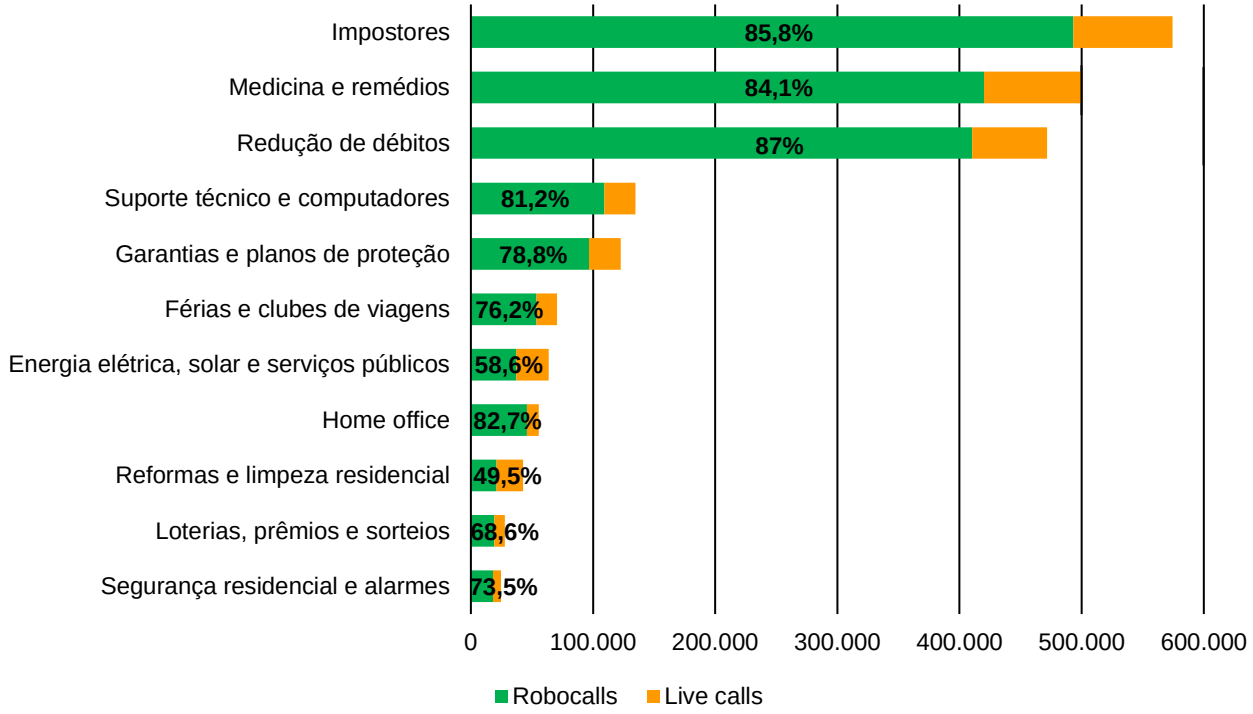
Gráfico 4 - Representatividade e número de reclamações registradas na FTC por violação à lista nacional de Não Perturbe (Do Not Call Registry) por tema - 2019 (ano fiscal)



FONTE: elaboração própria a partir de dados da FEDERAL TRADE COMMISSION - FTC. *The National Do Not Call Registry Data Book 2019*, Outubro 2019, p. 7.

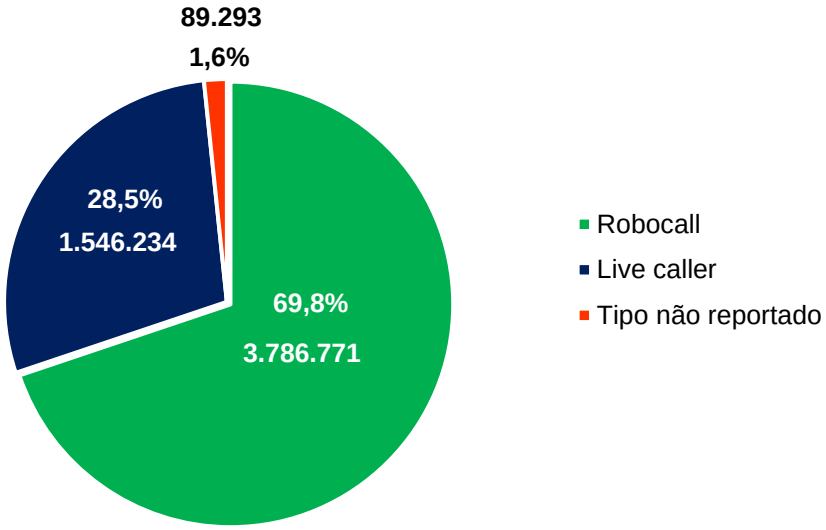
[24] FEDERAL TRADE COMMISSION - FTC. *The top frauds of 2019*.
[25] FEDERAL TRADE COMMISSION - FTC. *The top frauds of 2019*.
[26] FEDERAL TRADE COMMISSION - FTC. *The top frauds of 2019*.
[27] FEDERAL TRADE COMMISSION - FTC. *The top frauds of 2019*.
[28] O ano fiscal refere-se ao período de 1º de outubro de um ano a 30 de setembro do ano seguinte. O número de referência do ano é sempre o da data de término. UNITED STATES SENATE. *Glossary Term - Fiscal Year*. Nesse sentido o ano fiscal de 2019 começou em 1º de outubro de 2018, terminando em 30 de setembro de 2019.
[29] Nem todas as reclamações registradas tiveram temas reportados. FEDERAL TRADE COMMISSION - FTC. *The National Do Not Call Registry Data Book 2019*, Outubro 2019, p. 7.

Gráfico 5 - Representatividade de *robocalls*[30] e *live calls*[31] nas reclamações registradas na FTC por violação à lista nacional de Não Perturbe (Do Not Call Registry) por tema - 2019 (ano fiscal)



FONTE: elaboração própria a partir de dados da FEDERAL TRADE COMMISSION - FTC. *The National Do Not Call Registry Data Book 2019*, Outubro 2019, p. 7.

Gráfico 6 - Representatividade e número de reclamações registradas na FTC por violação à lista nacional de Não Perturbe (Do Not Call Registry) por tipo de chamada - 2019 (ano fiscal)



FONTE: elaboração própria a partir de dados da FEDERAL TRADE COMMISSION - FTC. *The National Do Not Call Registry Data Book 2019*, Outubro 2019, p. 7.

[30] Conforme indicado mais à frente nessa seção, *robocalls* são ligações realizadas por meio de mensagem gravada, voz artificial ou autodiscagem. FEDERAL COMMUNICATIONS COMMISSION - FCC. *Stop Unwanted Robocalls and Texts - Robocalls*.
[31] *Live calls* são ligações realizadas por pessoas. FEDERAL TRADE COMMISSION - FTC. *Robocalls*.

Ademais, a maior prestadora de serviços de telecomunicações nos Estados Unidos também possui uma seção de segurança cibernética em sua página na internet, enumerando vários golpes[32].

Nesse sentido, tendo em vista o elevado número de golpes e fraudes catalogados, em especial pela FTC, segue uma seleção de golpes e fraudes identificados pela FTC e pela FCC, bem como por essa prestadora.

1.1. Golpes que fazem uso de PBX/PABX

Golpe que ocorre normalmente em locais de trabalho com linhas de PBX/PABX[33]. Suposto funcionário da companhia telefônica informa à potencial vítima que está investigando problemas técnicos na linha ou eventuais ligações feitas para outros estados/países, solicitando que sejam feitas algumas ações[34], que podem permitir que o golpista realize ligações por meio da linha PBX/PABX[35].

1.2. Golpes solicitando doações após desastres

Após desastres naturais e condições climáticas adversas, como furacões, tempestades, inundações e queimadas, golpistas podem aproveitar-se da vulnerabilidade e do sentimento de caridade das pessoas.[36] Telefone, SMS, correio e até mesmo o comparecimento porta-a-porta são usados por esses golpistas.[37]

1.3. Golpes de garantia/seguro automotivo

Golpistas se passando por representantes de uma concessionária, fabricante ou seguradora, ligam para a vítima indicando que a garantia ou seguro do automóvel está prestes a expirar, induzindo-a a renovar a garantia ou apólice com algum tipo de benefício. Essas chamadas visam obter dados pessoais da vítima, que é induzida a permanecer na linha ou digitar certos números. Geralmente a ligação se inicia com uma mensagem automática ou pré-gravada e a dificuldade em identificá-la como golpe dá-se pelo fato de que o golpista pode ter dados efetivos do veículo, dando um ar de legitimidade à chamada. [38]

---

[32] A AT&T é a maior empresa de telecomunicações dos Estados Unidos em termos de receita, de acordo com a Statista. STATISTA. *Revenue of major U.S. telecommunication services providers in 2019*.
[33] AT&T. *Cyber Aware - Protecting Phone Systems from International Fraud*. FEDERAL COMMUNICATIONS COMMISSION - FCC. *Don't Fall for the 90# Telephone Scam*.
[34] FEDERAL COMMUNICATIONS COMMISSION - FCC. *Don't Fall for the 90# Telephone Scam*.
[35] AT&T. *Cyber Aware - Protecting Phone Systems from International Fraud*. FEDERAL COMMUNICATIONS COMMISSION - FCC. *Don't Fall for the 90# Telephone Scam*.
[36] FEDERAL COMMUNICATIONS COMMISSION - FCC. *After Storms, Watch Out for Scams*. FEDERAL TRADE COMMISSION - FTC. *Dealing with Weather Emergencies*. FEDERAL TRADE COMMISSION - FTC. *Scammers prey on your kindness during disasters*. FEDERAL TRADE COMMISSION - FTC. *Tips to help you avoid post-disaster scams*.
[37] FEDERAL COMMUNICATIONS COMMISSION - FCC. *After Storms, Watch Out for Scams*.
[38] FEDERAL COMMUNICATIONS COMMISSION - FCC. *Watch out for Auto Warranty Scams*.

1.4. Golpes envolvendo *spoofing*

Spoofing é a falsificação deliberada do número originador de um chamada para ocultar a identidade do chamador. Comumente, para induzir a vítima a atender a chamada, simula-se um número da mesma área local do número da possível vítima ou de um número já conhecido de um órgão governamental ou empresa. Uma vez atendida a ligação, os golpistas utilizar-se-ão de *scripts* para tentar conseguir informação pessoal ou roubar valores.[39]

1.5. Fraude de celular

"É definida como o uso não autorizado, adulteração ou manipulação de um telefone ou serviço celular". Entre esses tipos de fraude incluem-se:[40]

- Troca de SIM (*SIM swap*) ou golpe da portabilidade: golpistas roubam o cartão SIM ou passam-se por terceiro para realizar a portabilidade de um número para um dispositivo em posse dos fraudadores, podendo assim ter acesso a ligações, mensagens, informações bancárias e credenciais de mídias sociais[41]. A Kaspersky indica que esse golpe é disseminado em todo o mundo[42];
- Clonagem: envolve replicação da identificação de um celular ou cartão SIM em um dispositivo controlado pelos fraudadores, que passam a usar o telefone como se fossem a vítima;[43] e
- Fraude da contratação: fraudadores contratam serviços telefônicos em nome de terceiros com dados obtidos ilegalmente ou uma identidade falsa. Em especial, a FCC recomenda que em caso de suspeita, a possível vítima entre em contato com a polícia, reporte fraude de identidade junto à FTC, informe sua prestadora de serviços atual e a prestadora em que o contrato fraudulento foi realizado, bem como realize um alerta de fraude junto a um dos três maiores birôs de crédito do país.[44]

1.6. Fraudes no serviço de retransmissão de IP

"O serviço de retransmissão de protocolo da Internet [Internet Protocol Relay Service - IP Relay Service] permite que pessoas com deficiência auditiva ou de fala usem o serviço de retransmissão de telecomunicações por meio de um computador ou dispositivo habilitado para

[39] FEDERAL COMMUNICATIONS COMMISSION - FCC. *Caller ID Spoofing*.
[40] Tradução nossa. No original: "Cellular fraud is defined as the unauthorized use, tampering or manipulation of a cellular phone or service". FEDERAL COMMUNICATIONS COMMISSION - FCC. *Cell Phone Fraud*.
[41] AT&T. *Cyber Aware - Prevent Porting to Protect Your Identity*. AT&T. *Cyber Aware - What You Need to Know About SIM Swap Scams*. FEDERAL COMMUNICATIONS COMMISSION - FCC. *Cell Phone Fraud*.
[42] KASPERSKY. *Clonagem de celular no Brasil rouba até R$ 10 mil por vítima*, 17/04/2019.
[43] FEDERAL COMMUNICATIONS COMMISSION - FCC. *Cell Phone Fraud*.
[44] FEDERAL COMMUNICATIONS COMMISSION - FCC. *Cell Phone Fraud*.

web para se comunicarem por telefone com pessoas que ouvem".[45] Os golpistas usam esse serviço para se envolver em transações comerciais fraudulentas, geralmente usando cartões de crédito falsos ou roubados.[46]

1.7. Golpe de ligações a cobrar originadas no México

Tal golpe visa pessoas com sobrenomes hispânicos ou em comunidades hispânicas, enganando-as a aceitar ligações a cobrar de emergência ou com mensagens importantes supostamente de suas famílias no México. Tanto alguns consumidores acabam por aceitar a ligação, que pode envolver informações como o sobrenome do consumidor, o nome do suposto parente no México ou o nome de algum familiar, como do esposo(a) da vítima; quanto algumas operadoras completam a chamada antes mesmo de o consumidor aceitar a cobrança. Em ambos os casos a vítima acaba sendo tarifada por uma ligação de valor elevado.[47]

1.8. Golpe da ligação de um toque

Esse golpe tenta induzir a vítima a retornar uma ligação, tanto por meio de uma ligação que toca brevemente, não dando tempo de ser atendida[48], quanto variações que incluem mensagens falsas deixadas em caixa postal solicitando a realização de uma ligação para que a vítima seja informada sobre um parente supostamente doente ou para agendar uma entrega[49]. Essas ligações são realizadas de forma a parecerem ligações nacionais de dentro dos Estados Unidos, tanto por meio do uso de códigos de países que se parecem com os códigos de área de três dígitos americanos, quanto por meio de *spoofing*[50]. Todavia, tratam-se, na verdade, de ligações internacionais, acabando por fazer com que o consumidor seja elevadamente tarifado, além de pagar taxas de completamento de chamada[51].

1.9. Ligações e mensagens automatizadas não autorizadas

Ligações automatizadas (*robocalls*) são aquelas tanto realizadas por meio de mensagem gravada, voz artificial ou autodiscagem[52], enquanto as mensagens automatizadas (*robotexts*) são

[45] Tradução nossa. No original: "Internet Protocol Relay Service allows persons with a hearing or speech disability to use Telecommunications Relay Service through a computer or web-enabled device to communicate through the telephone system with hearing persons". FEDERAL COMMUNICATIONS COMMISSION - FCC. *IP Relay Service*.
[46] FEDERAL COMMUNICATIONS COMMISSION - FCC. *IP Relay Fraud*.
[47] FEDERAL COMMUNICATIONS COMMISSION - FCC. *Mexico Collect Call Scam*.
[48] AT&T. *Cyber Aware - Alerts & Reporting - One-Ring Call Scams*. FEDERAL COMMUNICATIONS COMMISSION - FCC. *'One Ring' Phone Scam*.
[49] FEDERAL COMMUNICATIONS COMMISSION - FCC. *'One Ring' Phone Scam*.
[50] FEDERAL COMMUNICATIONS COMMISSION - FCC. *'One Ring' Phone Scam*.
[51] AT&T. *Cyber Aware - Alerts & Reporting - One-Ring Call Scams*. FEDERAL COMMUNICATIONS COMMISSION - FCC. *'One Ring' Phone Scam*.
[52] FEDERAL COMMUNICATIONS COMMISSION - FCC. *Stop Unwanted Robocalls and Texts - Robocalls*.

aquelas realizadas por meio desse último método[53]. A FCC proíbe o envio de *robotexts*, exceto mensagens de emergência e mediante consentimento, não sendo necessário cadastro na lista nacional de Não Perturbe (Do Not Call Registry)[54]. Por seu turno, as ligações de *telemarketing*, de forma geral, devem ser precedidas de consentimento por parte do consumidor[55]. Ademais, essas ligações e mensagens podem estar associadas a golpes e fraudes[56], além de se utilizarem de *spoofing*[57].

1.10. Golpe de mudança de prestadora sem autorização (*slamming*)

Aqui ocorre a troca da prestadora do consumidor, de forma ilegal e sem autorização, em ligações locais ou longa distância.[58]

1.11. Apropriação de caixa postal

O golpista procura, por meio de ligação a sistema de caixa postal, caixas com senhas padrão ou fáceis e passa a fazer e aceitar ligações internacionais. O golpista também pode quebrar o sistema de encaminhamento da caixa postal e programar o redirecionamento para um número internacional. Esse tipo de golpe costuma visar caixas postais corporativas, mas isso não isenta os usuários não comerciais desse tipo de embuste.[59]

1.12. *Phishing*

Esse tipo de golpe tenta coletar informações pessoais por meio de mensagens de texto, páginas falsas e *e-mails*, bem como mensagens ou ligações (*voice phishing* - *vishing*) em que o golpista se passa por representante legítimo de uma instituição.[60]

1.13. *Catfishing*

Golpistas criam identidades falsas para se aproveitarem das emoções ou ganância de possíveis vítimas, tanto tentando obter dinheiro, quanto dados pessoais, financeiros e senhas. Entre os tipos desse golpe pode-se apontar:[61]

- Golpe do romance: o golpista se passa por um interesse amoroso em um *site* de relacionamentos, alongando a relação até se sentir confiante o suficiente para começar a

[53] FEDERAL COMMUNICATIONS COMMISSION - FCC. *Stop Unwanted Robocalls and Texts - Robotexts*.
[54] FEDERAL COMMUNICATIONS COMMISSION - FCC. *Stop Unwanted Robocalls and Texts - Robotexts*.
[55] FEDERAL COMMUNICATIONS COMMISSION - FCC. *Stop Unwanted Robocalls and Texts - Robocalls*.
[56] FEDERAL COMMUNICATIONS COMMISSION - FCC. *Stop Unwanted Robocalls and Texts - Consumer Tips*.
[57] FEDERAL COMMUNICATIONS COMMISSION - FCC. *Stop Unwanted Robocalls and Texts - Consumer Tips*. FEDERAL COMMUNICATIONS COMMISSION - FCC. *Stop Unwanted Robocalls and Texts - Spoofing*.
[58] FEDERAL COMMUNICATIONS COMMISSION - FCC. *Slamming: Switching Your Authorized Telephone Company Without Permission*.
[59] FEDERAL COMMUNICATIONS COMMISSION - FCC. *Voicemail System Hacking*.
[60] AT&T. *Cyber Aware - Phishing: Know Bait When You See It*.
[61] AT&T. *Cyber Aware - Stop Catfishing Before They Reel You In*.

fazer pedidos de itens, em geral irrastreáveis e sem possibilidade de reembolso, como cartões de presente[62] ou dinheiro, além da realização de grandes compras, sempre prometendo pagar de volta ou enviando um pagamento fraudulento como comprovação de que irá devolver a quantia[63]. A FTC indica que o pedido de valores, nesse caso, prontamente caracteriza o golpe e que esse embuste gerou prejuízos US$ 201 milhões em 2019[64];

- Golpe da caridade: o golpista se passa por uma instituição de caridade induzindo a vítima a realizar compras ou doações[65], comumente aproveitando-se de situações de desastre[66], como em golpe já abordado anteriormente[67]; e
- Golpe do dinheiro fácil: o golpista oferece dinheiro para que a vítima faça uma tarefa para ele, incluindo, em geral, instruções detalhadas, fazendo tudo parecer simples e ético.[68]

1.14. Golpes de suporte técnico

Um *e-mail*, uma tela de aviso ou uma ligação indicam que há algum problema com seu computador ou um *e-mail* ou tela de aviso apontam que há alguma questão de segurança que deve ser resolvida por meio de uma ligação ou do *download* de um antivírus. Ao realizar uma ligação para um número encontrado em pesquisa na internet ou indicado nos dois primeiros e no quarto casos, ou já estando na ligação no terceiro, a vítima é induzida, por um golpista que se passa por representante de suporte técnico, a conceder acesso remoto a seu computador.[69]

1.15. Golpes de loterias, prêmios e sorteios

A vítima é informada que ganhou um sorteio de loteria ou um prêmio, mas que para resgatá-lo é necessário pagar uma taxa ou impostos.[70] O golpista então geralmente solicita dados de cartão crédito, de cartão de crédito pré-pago ou informação financeira.[71]

1.16. Golpes de cartões de presente

Os golpistas solicitam pagamento por meio de cartões de presente[72] para, entre outros, supostas resolução de pendências no número do seguro social[73], liberação de prêmios de loteria,

[62] Sobre cartões de presente, vide subseção *1.16. Golpes de cartões de presente* nesta seção.
[63] AT&T. *Cyber Aware - Stop Catfishing Before They Reel You In*.
[64] FEDERAL TRADE COMMISSION - FTC. *It's not true love if they ask for money*. FEDERAL TRADE COMMISSION - FTC. *Online Dating Scams Infographic*.
[65] AT&T. *Cyber Aware - Stop Catfishing Before They Reel You In*. FEDERAL TRADE COMMISSION - FTC. *Donating in difficult times*.
[66] AT&T. *Cyber Aware - Stop Catfishing Before They Reel You In*.
[67] *1.2. Golpes solicitando doações após desastres* nesta seção.
[68] AT&T. *Cyber Aware - Stop Catfishing Before They Reel You In*.
[69] AT&T. *Cyber Aware - Alerts & Reporting - Coronavirus Scam*.
[70] AT&T. *Cyber Aware - Alerts & Reporting - Lottery & Prize Scams*. FEDERAL TRADE COMMISSION - FTC. *"You've won! Now pay us" is always a scam*.
[71] AT&T. *Cyber Aware - Alerts & Reporting - Lottery & Prize Scams*.

pagamento de multas referentes a imposto de renda, pagamento de suporte técnico de computadores e pagamento de serviços públicos, como água ou esgoto, com ameaça de corte caso não seja efetuado o pagamento[74]. A FTC alerta que a insistência em que se pague com cartões de presente pode ser sempre identificada como um golpe[75] e que essa é uma forma comum de roubar valores das vítimas, pois tais cartões se assemelham a dinheiro vivo e dificilmente será possível obter um reembolso no caso de uso pelos golpistas[76].

1.17. Golpes de compras de final de ano (*Holiday Scams*)

Os golpistas se aproveitam da generosidade nas compras do período de final de ano e tentam, por meio do oferecimento de ótimas ofertas, aplicar golpes de cartões de presente, *phishing* e *catfishing*, na variação do golpe da caridade.[77]

1.18. Mula de dinheiro

Aqui a vítima é usada para movimentar dinheiro roubado para os golpistas, que mandam dinheiro ou cheque para que a vítima repasse a terceiro, comumente por transferências ou cartões de presente. A vítima é induzida por meio do oferecimento de prêmios, de um relacionamento *on-line* ou pela promessa de um emprego, em geral em *home office*.[78]

1.19. Golpes de criptomoedas

Os golpistas induzem a vítima a mandar valores por meio de criptomoedas, como Bitcoin, seja por meio de chantagem, *e-mails*, *posts* em mídias sociais ou oportunidades falsas de investimentos ou negócios.[79]

1.20. Golpes da Receita Federal ou impostos (*IRS/Tax Scams*)

Nesses golpes o foco está em tentar fazer com que a vítima envie dinheiro[80], aproveitando-se especialmente de momentos em que as pessoas estão ocupadas com suas declarações de

[72] Cartões de presente são cartões carregados com certa quantia em valor. O cartão dá ao possuidor a liberdade de escolher onde e quanto utilizá-lo: dependendo do tipo, em lojas/grupo de lojas específicas ou em qualquer local que aceite cartões de crédito. Ademais, os cartões têm data de validade, bem como a quantia carregada é limitada e, em geral, uma vez usada, o cartão não pode ser recarregado. INVESTOPEDIA. *Prepaid Cards vs. Gift Cards: What's the Difference?*.
[73] FEDERAL TRADE COMMISSION - FTC. *Did someone tell you to pay with gift cards? It's a scam*.
[74] FEDERAL TRADE COMMISSION - FTC. *Paying Scammers with Gift Cards*.
[75] FEDERAL TRADE COMMISSION - FTC. *Did someone tell you to pay with gift cards? It's a scam*. FEDERAL TRADE COMMISSION - FTC. *Paying Scammers with Gift Cards*.
[76] FEDERAL TRADE COMMISSION - FTC. *Paying Scammers with Gift Cards*.
[77] AT&T. *Cyber Aware - Alerts & Reporting - Beware of Holiday Scams*.
[78] FEDERAL TRADE COMMISSION - FTC. *Money Mule Scams Infographic*. FEDERAL TRADE COMMISSION - FTC. *What's a money mule scam?*.
[79] FEDERAL TRADE COMMISSION - FTC. *Avoiding a cryptocurrency scam*. FEDERAL TRADE COMMISSION - FTC. *Cryptocurrency blackmail scam alert*. FEDERAL TRADE COMMISSION - FTC. *Scam emails demand Bitcoin, threaten blackmail*.

renda e restituição de impostos[81]. Todavia, os golpistas têm diversificado esse esquema e, além de tentarem se passar por representantes da Receita Federal americana (Internal Revenue Service - IRS)[82], tem-se tentado passar por outros órgãos governamentais, como o órgão do seguro social (Social Security Administration - SSA)[83].

1.21. Golpes relativos à pandemia do novo coronavírus

Com a atual situação da pandemia do novo coronavírus, golpistas têm visado a situação de calamidade pública para se aproveitar das pessoas por meio do envio de mensagens, *e-mails* ou *posts* em mídias sociais, todos tentando se passar por informações oficiais, que induzem a vítima a clicar em anexos com *malware* ou ser redirecionada para páginas falsas que coletam informações.[84]

Na página de golpes e fraudes da FTC[85] há pelo menos 35 entradas, em 2020, com informações sobre golpes/fraudes se referindo ao novo coronavírus e, entre janeiro e 15 de abril, o órgão tinha recebido mais de 18 mil relatos de fraudes/golpes sobre essa temática, totalizando mais de US$ 13 milhões em perdas financeiras.[86]

Os golpistas têm se aproveitando da atual situação para captar informações pessoais ou induzir o envio de valores por meio de *sites* falsos, *posts* em redes sociais ou envio de *e-mails* e mensagens com informações falsas[87] sobre pagamento de auxílio emergencial ou seguro desemprego[88], realização de testes para detectar contaminação pelo coronavírus[89], tratamento para a Covid-19[90], rastreamento de contatos[91], venda de máscaras[92], ofertas de trabalho em *home office*[93] e adoção de animais de estimação[94].

---

[80] AT&T. *Cyber Aware - Alerts & Reporting - IRS/Tax Scams and Similar Government Agency Scams Alert*. FEDERAL TRADE COMMISSION - FTC. *IRS Imposter Scams Infographic*.
[81] AT&T. *Cyber Aware - Alerts & Reporting - IRS/Tax Scams and Similar Government Agency Scams Alert*.
[82] AT&T. *Cyber Aware - Alerts & Reporting - IRS/Tax Scams and Similar Government Agency Scams Alert*. FEDERAL TRADE COMMISSION - FTC. *IRS Imposter Scams Infographic*.
[83] AT&T. *Cyber Aware - Alerts & Reporting - IRS/Tax Scams and Similar Government Agency Scams Alert*.
[84] AT&T. *Cyber Aware - Alerts & Reporting - Coronavirus Scam*.
[85] FEDERAL TRADE COMMISSION - FTC. Consumer information. *Scams*.
[86] FEDERAL TRADE COMMISSION - FTC. *COVID-19 scam reports, by the numbers*.
[87] FEDERAL TRADE COMMISSION - FTC. *Coronavirus: Scammers follow the headlines*. FEDERAL TRADE COMMISSION - FTC. *FTC: Coronavirus scams, Part 2*.
[88] FEDERAL TRADE COMMISSION - FTC. *Coronavirus checks: flattening the scam curve*. FEDERAL TRADE COMMISSION - FTC. *Coronavirus stimulus payment scams: What you need to know*. FEDERAL TRADE COMMISSION - FTC. *Did an ID thief steal your stimulus payment? Report it to us*. FEDERAL TRADE COMMISSION - FTC. *Economic impact payments for U.S. citizens abroad*. FEDERAL TRADE COMMISSION - FTC. *Fake emails about fake money from a fake COVID-19 fund*. FEDERAL TRADE COMMISSION - FTC. *Is a scammer getting unemployment benefits in your name?*. FEDERAL TRADE COMMISSION - FTC. *Small businesses: Where to go for financial relief information*. FEDERAL TRADE COMMISSION - FTC. *The IRS won't call about your stimulus money*. FEDERAL TRADE COMMISSION - FTC. *Want to get your Coronavirus relief check? Scammers do too*.
[89] FEDERAL TRADE COMMISSION - FTC. *Not every COVID-19 testing site is legit*.
[90] FEDERAL TRADE COMMISSION - FTC. *FTC & FDA: Warnings sent to sellers of scam Coronavirus treatments*. FEDERAL TRADE COMMISSION - FTC. *FTC: Sellers need proof for COVID treatment claims*. FEDERAL TRADE COMMISSION - FTC. *FTC sends more warnings to sellers of scam Coronavirus treatments*. FEDERAL TRADE COMMISSION - FTC. *FTC warns 45 more sellers of scam Coronavirus treatments*. FEDERAL TRADE COMMISSION - FTC. *More FTC warnings about scam Coronavirus treatments*.

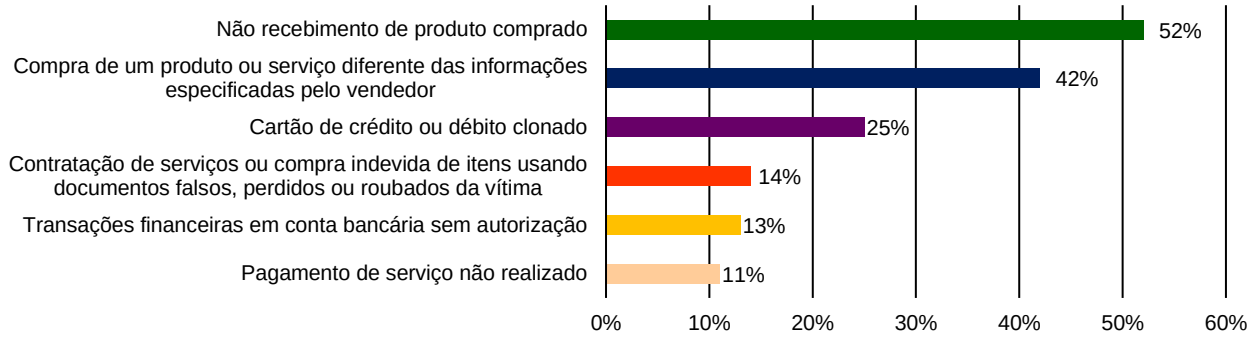
3. GOLPES E FRAUDES NO BRASIL

Os golpes e fraudes são altamente disseminados no Brasil. Dados da Serasa indicam que a cada 17 segundos há uma tentativa de fraude no país[95] e que essas fraudes visam mais comumente pessoas que ganham entre dois e quatro salários mínimos, moram nas regiões Sudeste e Nordeste e estão na faixa etária de 36 a 45 anos[96]. Ademais, quem foi roubado ou perdeu documentos tem o dobro de chances de ser fraudado.[97]

Dados da Trend Micro, por seu turno, indicam que o Brasil foi, em 2019, o vice-líder em ataques de *ransomware* (31,97% dos ataques globais), atrás dos Estados Unidos (34,36%), bem como o terceiro maior país com ameaças cibernéticas disseminas por *e-mail* (quase 2 bilhões), atrás apenas de Estados Unidos (10 bilhões) e China (4 bilhões). Além disso, a empresa bloqueou no país quase 13 milhões de *malwares*, ocupando o Brasil a 10ª posição entre os países com maior registro de *malwares* detectados.[98]

Pesquisa da Confederação Nacional de Dirigentes Lojistas (CNDL) e do Serviço de Proteção ao Crédito (SPC Brasil) indica que entre agosto de 2018 e julho de 2019, 12 milhões de brasileiros foram vítimas de golpes na internet, alcançando um prejuízo acumulado de R$ 1,8 bilhão. Os golpes mais comuns apontados por essa pesquisa, conforme gráfico abaixo, foram o não recebimento de produto comprado (52%) e a compra de produto/serviço diferente das especificações fornecidas pelo vendedor (42%).[99]

Gráfico 7 - Golpes mais comuns na internet no Brasil

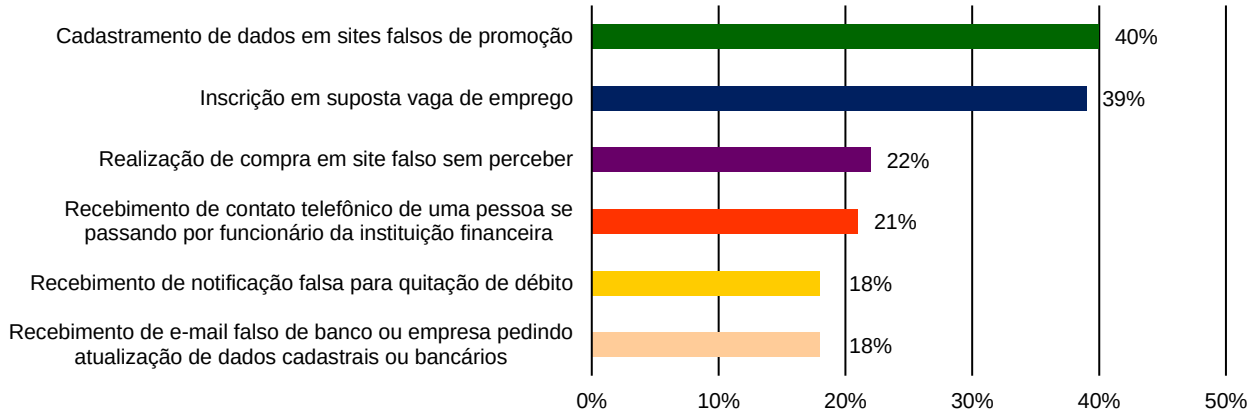


FONTE: elaboração própria a partir de dados de pesquisa da Confederação Nacional de Dirigentes Lojistas (CNDL) e do Serviço de Proteção ao Crédito (SPC Brasil) referenciados em VALOR INVESTE. *12 milhões de brasileiros são vítimas de golpes na internet; veja os mais comuns*, 15/08/2019.

[91] FEDERAL TRADE COMMISSION - FTC. *Contact Tracing Infographic*. FEDERAL TRADE COMMISSION - FTC. *COVID-19 contact tracing text message scams*. FEDERAL TRADE COMMISSION - FTC. *Help COVID-19 contact tracers, not scammers*.
[92] FEDERAL TRADE COMMISSION - FTC. *Scammers offer facemasks but don't deliver*.
[93] FEDERAL TRADE COMMISSION - FTC. *Steer clear of work-at-home scams*.
[94] FEDERAL TRADE COMMISSION - FTC. *Finding a furry friend in the era of COVID-19*.
[95] SERASA. *Como escapar das fraudes online?*. SERASA. *Você sabe que está sujeito a fraude?*.
[96] SERASA. *Você sabe que está sujeito a fraude?*.
[97] SERASA. *Saiba o que é fraude e quais os tipos mais comuns*.
[98] CONVERGÊNCIA DIGITAL. *Brasil teve quase dois bilhões de ameaças cibernéticas de e-mail em 2019*, 03/03/2020.
[99] VALOR INVESTE. *12 milhões de brasileiros são vítimas de golpes na internet; veja os mais comuns*, 15/08/2019.

Essa pesquisa aponta ainda que entre os serviços que foram contratados *on-line* e não realizados, o mais representativo foi o de falsa agência de emprego (32%) e que as principais fraudes que solicitaram das vítimas o fornecimento de dados pessoais, conforme gráfico abaixo, foram os de cadastramento em falsos *sites* de promoção (40%) e inscrição para suposta vaga de emprego.[100]

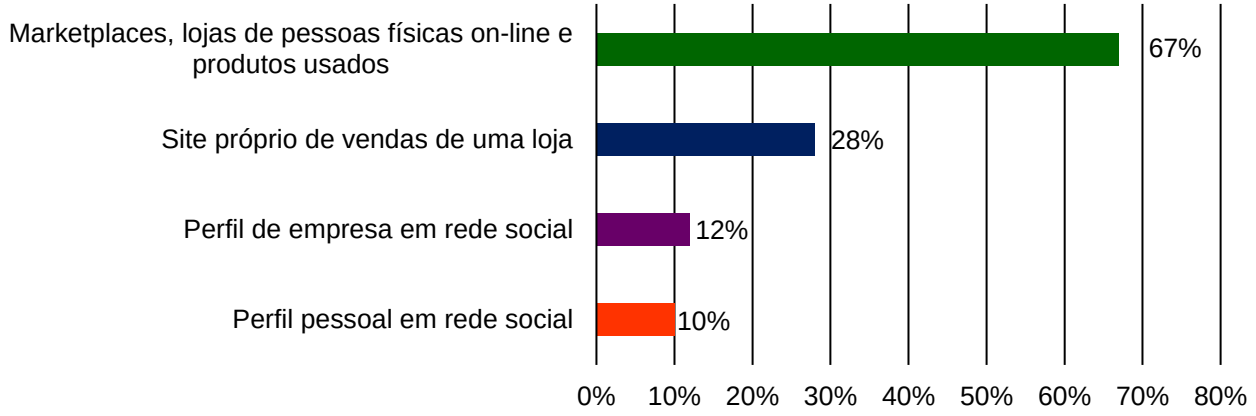
Gráfico 8 - Principais fraudes que pedem fornecimento de dados no Brasil



FONTE: elaboração própria a partir de dados de pesquisa da Confederação Nacional de Dirigentes Lojistas (CNDL) e do Serviço de Proteção ao Crédito (SPC Brasil) referenciados em VALOR INVESTE. *12 milhões de brasileiros são vítimas de golpes na internet; veja os mais comuns*, 15/08/2019.

Enfim, essa pesquisa aponta também os canais de compra em que mais ocorreram problemas, conforme gráfico abaixo, com grande liderança para *markeptlaces*, lojas de pessoas físicas *on-line* e produtos usados (67%)[101]

Gráfico 9 - Canais de compra em que mais ocorrem problemas no Brasil



FONTE: elaboração própria a partir de dados de pesquisa da Confederação Nacional de Dirigentes Lojistas (CNDL) e do Serviço de Proteção ao Crédito (SPC Brasil) referenciados em VALOR INVESTE. *12 milhões de brasileiros são vítimas de golpes na internet; veja os mais comuns*, 15/08/2019.

[100] VALOR INVESTE. *12 milhões de brasileiros são vítimas de golpes na internet; veja os mais comuns*, 15/08/2019.
[101] VALOR INVESTE. *12 milhões de brasileiros são vítimas de golpes na internet; veja os mais comuns*, 15/08/2019.

Além de pesquisas, conforme abordado acima, o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.Br), mantido pelo Núcleo de Informação e Coordenação do Ponto BR (NIC.br), que, por sua vez, está ligado ao Comitê Gestor da Internet no Brasil (CGI.br), aponta alguns dos principais golpes que se dão por meio da conexão à internet. Ademais, a própria Anatel também faz alertas de golpes e fraudes aos consumidores, o Serasa possui um serviço de educação ao consumidor[102] e, além disso, notícias de golpes e fraudes que tentam se aproveitar dos consumidores de serviços de telecom também são constantemente noticiados na imprensa. Com efeito, essas são as fontes utilizadas aqui para apresentar golpes e fraudes com recorrência no território nacional.

1.1. Furto de identidade

Ocorre quando uma pessoa tenta se passar por outra para obter vantagens indevidas. O golpista pode enviar *e-mails* ou simular um perfil em redes sociais se passando por terceiros e assim levar as pessoas ao erro, acreditando estarem em contato com a vítima.[103]

1.2. Fraude de antecipação de recursos (*advance fee fraud*)

Nessa fraude a vítima é induzida a realizar um adiantamento financeiro ou a fornecer dados pessoais para que receba algum tipo de benefício futuro.[104]

Um dos tipos mais famosos dessa fraude é o chamado Golpe da Nigéria (*Nigerian 4-1-9 Scam*[105]) em que a vítima é levada a acreditar que receberá uma grande soma em dinheiro para intermediar transferência internacional de fundos originada na Nigéria. Para isso, a vítima é convencida a depositar adiantamentos para custos. O próprio golpista identifica a transferência como ilegal, solicitando assim resposta rápida e sigilo absoluto da possível vítima.[106]

O golpe é conhecido como Golpe da Nigéria pela alta incidência de sua origem nesse país, mas há casos de outros países também, normalmente países passando por problemas políticos, econômicos ou raciais.[107]

A fraude de antecipação de recursos possui muitas variações:[108]

---

[102] SERASA. *Serasa ensina*.
[103] CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL - CERT.br. *Cartilha de Segurança para Internet - Golpes na Internet*.
[104] CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL - CERT.br. *Cartilha de Segurança para Internet - Golpes na Internet*.
[105] O número 419 é uma referência à seção do Código Penal nigeriano que equivale ao crime de estelionato no Código Penal Brasileiro (artigo 171).
[106] CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL - CERT.br. *Cartilha de Segurança para Internet - Golpes na Internet*.
[107] CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL - CERT.br. *Cartilha de Segurança para Internet - Golpes na Internet*.
[108] CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL - CERT.br. *Cartilha de Segurança para Internet - Golpes na Internet*.

Tabela 2 - Tipos de fraudes de antecipação de recursos

GOLPE	MEIO UTILIZADO	DESCRIÇÃO
Loteria internacional	*E-mail*	A vítima é induzida a fornecer dados pessoais e bancários para receber suposto prêmio de loteria
Crédito fácil	*E-mail*	A vítima é induzida a realizar depósito bancário para conseguir financiamento com taxas de juros muito mais baixas que as de mercado
Doação de animais	*Sites* na internet	Ao pesquisar por animais de estimação caros para comprar, a vítima encontra *sites* doando esses animais e é levada a enviar dinheiro para despesas com transporte
Oferta de emprego	SMS	Para ser contratada, a vítima deve informar detalhes da sua conta bancária
Noiva russa	Redes sociais	O golpista promete um relacionamento amoroso e convence a vítima a enviar dinheiro para que ela saia de seu país (geralmente a Rússia) e viaje até ela

FONTE: CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL - CERT.br. *Cartilha de Segurança para Internet - Golpes na Internet*.

1.3. *Phishing* e *pharming*

Phishing[109], *phishing-scam* ou *phishing*/*scam*, é um dos tipos mais comuns de fraude na internet. No *phishing*, o golpista envia uma mensagem (por *e-mail*, SMS, redes sociais) para a vítima simulando alguma fonte confiável, como uma instituição conhecida, um banco, uma empresa ou um *site* conhecido e, usando táticas de engenharia social, como atiçar a curiosidade, promessa de vantagens, necessidade de correção de cadastro, táticas de susto, etc. induz a vítima a clicar em *links* para *sites* maliciosos, preencher formulários falsos ou enviar dados pessoais.[110]

Para atrair possíveis vítimas, os golpistas utilizam-se, nas mensagens, de temas como oferecimento de antivírus; exibição de fotos/vídeos de celebridades; doações para associações assistenciais (Teleton, Criança Esperança); notificações judiciais para participação em audiências, protesto de valores e ordem de despejo; promoções e milhagens de companhias aéreas; convocações para trabalhar como mesário ou cancelamento de título eleitoral; oferecimento de vagas de emprego ou solicitação de atualização de currículo; questões/pendências relacionas a declaração de imposto de renda ou *download* do programa eletrônico de preenchimento e entrega da declaração; recebimento de prêmios de loteria; notícias sobre *reality shows*; notificações de redes sociais; falsas faturas/débitos de serviços de telefonia; *sites* com dicas de segurança; inscrição em serviços de proteção de crédito; recebimento de telegrama *on-line*; etc.[111]

[109] "A palavra *phishing*, do inglês '*fishing'*, vem de uma analogia criada pelos fraudadores, na qual 'iscas' (mensagens eletrônicas) são usadas para 'pescar' senhas e dados financeiros de usuários da internet". Aspas do autor. Grifos do autor. CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL - CERT.br. *Cartilha de Segurança para Internet - Golpes na Internet*.
[110] CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL - CERT.br. *Cartilha de Segurança para Internet - Golpes na Internet*.
[111] CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL - CERT.br. *Cartilha de Segurança para Internet - Golpes na Internet*.

O *phishing* também pode ocorrer, entre outras, nas seguintes situações:

- Páginas falsas de comércio eletrônico ou *internet banking*: a vítima recebe um *e-mail* simulando ser de um *site* ou instituição conhecida com um *link* para um *site* malicioso que simula o *site* da instituição verdadeira e coletará seus dados pessoais e financeiros;
- Páginas falsas de redes sociais ou de companhias aéreas: novamente a pessoa recebe uma mensagem com um *link*, nesse caso para uma rede social ou companhia aérea que a vítima usa. O *link* leva para um *site* falso no qual será solicitado que a vítima coloque seu *login* e senha. Esses dados vão para os golpistas, que poderão então agir como se fossem a própria vítima, realizando o envio de mensagens ou emitindo passagens aéreas, por exemplo;
- Mensagens contendo formulários: a mensagem já vem com um formulário em seu corpo para digitação de dados pessoais e um botão enviar que, ao ser clicado, transmite os dados para os golpistas;
- Mensagens contendo *links* para códigos maliciosos: nesse caso, a ideia é instalar um código malicioso no computador da vítima que abrirá portas nesse dispositivo para acesso dos golpistas. O método é o mesmo do envio de *link*, mas aqui a vítima é convencida a instalar um arquivo em seu computador; e
- Solicitação de recadastramento: a vítima é levada a crer que precisa realizar um recadastramento para acesso a conta de *e-mail* em uma instituição de ensino que frequenta ou empresa em que trabalha.[112].

Segundo dados da Kaspersky referentes ao primeiro trimestre de 2019, o Brasil é o país com maior incidência do golpe de *phishing*. Nesse período, 22% de usuários foram vítimas do golpe, configurando-se aumento em relação ao mesmo período de 2018, quanto esse número alcançou 19%. Em especial o golpe está ligado à variação do envio de *spams* de oferta de trabalho que, de forma sofisticada, se passava por recrutadores conhecidos e tinha objetivo de instalação de *malware* para roubo de valores das vítimas.[113]

O *phishing* também tem uma variação específica denominada *pharming*. No *pharming* o servidor DNS (*Domain Name System*), principalmente de empresas, é atacado, por exemplo, por meio do comprometimento do servidor de DNS do provedor, pela ação de códigos maliciosos projetados para alterar o comportamento do serviço de DNS do computador ou pela ação direta de um invasor, que tenha acesso às configurações de serviço do DNS. Comprometido o DNS, a

[112] CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL - CERT.br. *Cartilha de Segurança para Internet - Golpes na Internet*.
[113] KASPERSKY. *Brasil é o País com mais usuários atacados por phishing*, 20/05/2019.

vítima, ao tentar entrar em determinado *site*, é redirecionada para uma página falsa que imita aquela que se quer efetivamente acessar.[114]

1.4. Golpes de comércio eletrônico

Aqui os golpistas, visando obter vantagens financeiras, procuram se aproveitar de uma relação de confiança entre as partes de uma transação comercial. Entre as variações desse golpes estão:[115]

- Golpe do *site* de comércio eletrônico fraudulento: o golpista simula um *site* de comércio eletrônico levando as vítimas a realizarem compras de produtos que na verdade não existem e nunca serão enviados. Para reforçar a atração de vítimas, o golpista vale-se de artifícios como *spam*, promoções, propaganda através de *links* patrocinados e em *sites* de compra coletiva, além de oferecer preços muito abaixo dos normalmente praticados no mercado. Esse tipo de golpe pode fazer várias vítimas: quem compra e não recebe o produto, a empresa cujo nome tenha sido vinculado ao golpe, *sites* de compra coletiva que tenham servido de veículos para a transação, etc;
- Golpe envolvendo *sites* de compras coletivas: além da utilização dos *sites* de compras coletivas como portal de anúncio de ofertas falsas que realizam o direcionamento para *sites* fraudulentos e dos riscos típicos do comércio eletrônico, os *sites* de compra coletiva possuem características próprias como a do tempo para decidir pela compra, fazendo com que, sob a pressão do tempo máximo para aproveitar uma oferta, o comprador seja influenciado a comprar sem realizar uma análise mais cuidadosa; e
- Golpe do *site* de leilão e venda de produtos: aqui os golpistas não cumprem com o que foi acordado na transação de um leilão/venda ou utilizam dados obtidos nesse processo para outros fins. Os golpistas podem tanto ser vendedores como compradores: quando são vendedores, a vítima arremata o produto, deposita o valor e depois não recebe o produto, enquanto no caso dos compradores, os golpistas tentam receber o produto vendido sem realizar o pagamento. Tem sido muito comum nos leilões de veículos.[116]

1.5. Boato

O boato (*hoax*) é uma notícia falsa que tem o intuito de chamar a atenção, geralmente tendo por isso teor alarmante. Normalmente espalhado como *spam*, para que se alcance o maior

[114] CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL - CERT.br. *Cartilha de Segurança para Internet - Golpes na Internet*.
[115] CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL - CERT.br. *Cartilha de Segurança para Internet - Golpes na Internet*.
[116] CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL - CERT.br. *Cartilha de Segurança para Internet - Golpes na Internet*.

número de pessoas possível, o boato traz, em geral, informações sem sentido, além de tentativas de golpe propriamente ditas, incluindo esquemas de pirâmide e correntes. Muitas vezes o boato simula remetentes que dão credibilidade, como órgãos do governo ou instituições e empresas conhecidas.[117]

São muitos os efeitos nocivos que um boato pode causar, como, entre outros, disseminar desinformação pela internet, espalhar códigos maliciosos, comprometer a credibilidade e a reputação de pessoas ou instituições atacadas nas mensagens, assim como das pessoas que repassam os boatos, pois dão a entender que estão endossando o mesmo.[118]

Em especial no caso brasileiro, se somente 2% dos brasileiros disseram desconhecer o termo *fake news* em pesquisa realizada pela Kaspersky, por outro lado, 62% disseram não saber identificar ou não ter certeza se conseguem apontar se uma notícia na internet é falsa, enquanto somente 42% ocasionalmente questiona o que lê na internet.[119]

1.6. Golpe do falso boleto

Esse golpe tanto pode ser realizado pelo envio de um boleto falso para a possível vítima por SMS, *e-mail* ou WhatsApp, quanto pela instalação de programas maliciosos que passam a alterar os dados de boletos gerados pela internet. Em ambos os casos, a vítima acaba por realizar o pagamento na conta dos golpistas, que se aproveitam aqui do fato de o boleto ser o segundo maior meio usado para pagamentos no país, atrás apenas do cartão de crédito. Ademais, dados do Serasa indicam que em 2019 cresceu em 55% esse tipo de golpe em relação a 2018.[120]

1.7. Golpe do anúncio na internet

Aqui os golpistas utilizam-se somente de engenharia social para enganar as vítimas. Os criminosos monitoram anúncios em *sites* de venda na internet, conseguindo assim os dados da vítima. Em seguida se passam por representantes desses *sites* solicitando que a vítima envie ou fale um código que receberá por SMS para resolver uma questão pendente referente ao anúncio. O código enviado, todavia, é o código de ativação do aplicativo WhatsApp, o que permite que os golpistas passem a utilizar esse aplicativo se passando pela vítima, em geral para pedir dinheiro aos contatos listados no *app*.[121]

---

[117] CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL - CERT.br. *Cartilha de Segurança para Internet - Golpes na Internet*.
[118] CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL - CERT.br. *Cartilha de Segurança para Internet - Golpes na Internet*.
[119] KASPERSKY. *Mais de 60% dos brasileiros não sabem reconhecer notícia falsa*, 21/02/2020.
[120] SERASA. *5 dicas para se proteger de um boleto falso*. SERASA. *Saiba o que é fraude e quais os tipos mais comuns*.
[121] CANAL TECH. *Novo golpe "rouba" WhatsApp de quem anunciou algum produto na internet*, 27/05/2019. KASPERSKY. *Anunciou na Internet? Novo golpe rouba seu WhatsApp*, 27/05/2019. TECMUNDO. *Golpe clona WhatsApp e rouba dinheiro de usuários da OLX e Mercado Livre*, 22/10/2019. UOL - Tilt. *Entenda o golpe que rouba conta de WhatsApp sem usar vírus*, 22/10/2019.

1.8. Clonagem de celular

O golpe comumente conhecido no Brasil como clonagem de celular ou clonagem de *chip* é o equivalente ao golpe de *SIM swap*[122], descrito anteriormente nos golpes conhecidos nos Estados Unidos[123]. Além de ser bastante comum no país, esse golpe também é disseminado em todo o mundo.[124]

Nesse golpe, a partir da ativação do número em um *chip* em posse dos fraudadores, os criminosos passam a usar o telefone como se fossem a vítima se aproveitando "não apenas para roubar credenciais e capturar senhas de uso único (OTPs) enviadas por SMS, mas também para roubar dinheiro das vítimas".[125] Após obter dados das vítimas por meio de engenharia social, vazamento de dados, *phishing* ou compra de informações, os golpistas se aproveitam do processo legítimo da portabilidade e habilitam o número em um novo *chip*, passando a controlar chamadas e mensagens com origem e destino no número da vítima, passando a comprometer serviços que dependem de autenticação em dois fatores.[126] Em especial esse tipo de golpe tem sido utilizado para que os fraudadores habilitem o aplicativo WhatsApp no novo *chip* e passem a pedir dinheiro a contatos da vítima nesse *app*.[127]

1.9. Golpes e fraudes se utilizando do nome da Anatel

O nome da Anatel tem sido utilizado de forma criminosa por golpistas. A Agência, em seu Portal do Consumidor[128], salienta que não contacta consumidores para oferecer serviços, realizar cobranças, conceder prêmios ou fazer quaisquer testes técnicos de qualidade de ligações telefônicas, bem como não envia *links* por SMS ou WhatsApp[129]. Também é ressaltado que os consumidores não devem fornecer informações pessoais, bem como, em caso de suspeita de tentativa de fraude, os consumidores devem se informar por meio do *site* da Agência e, conforme o caso, devem registrar o fato junto à polícia.[130]

Ademais, a Agência possui, desde 2005, o Grupo Executivo Antifraude de Telecomunicações (GEAFT) que conta com a participação tanto da Agência, quanto de representantes das prestadoras de serviços de telecomunicações.[131] O GEAFT tem como sede

[122] KASPERSKY. *Clonagem de celular no Brasil rouba até R$ 10 mil por vítima*, 17/04/2019.
[123] Vide subseção *1.5. Fraude de celular* na seção *2. Golpes e fraudes nos Estados Unidos*.
[124] KASPERSKY. *Clonagem de celular no Brasil rouba até R$ 10 mil por vítima*, 17/04/2019.
[125] KASPERSKY. *Clonagem de celular no Brasil rouba até R$ 10 mil por vítima*, 17/04/2019.
[126] KASPERSKY. *Clonagem de celular no Brasil rouba até R$ 10 mil por vítima*, 17/04/2019.
[127] KASPERSKY. *Clonagem de celular no Brasil rouba até R$ 10 mil por vítima*, 17/04/2019.
[128] ANATEL. *Consumidor*.
[129] ANATEL. *Anatel alerta sobre fraudes*, 20/02/2019, 08/03/2019 (última atualização).
[130] ANATEL. *Anatel alerta sobre fraudes*, 20/02/2019, 08/03/2019 (última atualização).
[131] ANATEL. *Anatel alerta sobre fraudes*, 20/02/2019, 08/03/2019 (última atualização).

propor ações com foco em prevenir, diminuir ou extinguir a prática de fraudes nos serviços de telecomunicações.[132]

1.10. Golpes relativos à pandemia do novo coronavírus

Vários tem sido os golpes aproveitando-se da atual situação de pandemia. No final de março, a Agência alertou aos consumidores sobre golpes utilizando seu nome e prometendo oferecer internet grátis.[133] A Agência também tem alertado aos consumidores sobre golpes oferecendo falsos serviços de filmes e séries gratuitos e distribuição de álcool gel.[134]

Em especial o Auxílio Emergencial tem sido utilizado como isca para fraudes por meio de *e-mails*, ligações, SMSs, correntes de WhatsApp e aplicativos falsos, já tendo sido bloqueados mais de 60 desses *apps* pela Caixa.[135] Com efeito, a Refinaria de Dados[136] aponta que as palavras mais usadas para "pescar" a atenção dos brasileiros têm sido "covid" "auxílio" e "Caixa" e que o meio mais utilizado para as tentativas de golpe é o SMS (73%).[137]

Outros golpes se aproveitando da pandemia têm sido utilizados para roubar dados pessoais e instalar programas maliciosos por meio de *e-mails* com boletos falsos de compra de álcool gel usando o nome de uma farmácia ou, por meio do WhatsApp, pelo oferecimento de *kit* gratuito com máscara e álcool gel ou promessa de conta grátis no serviço de *streaming* Netflix.[138] Ademais, golpistas também têm se aproveitado do momento para realizar o golpe de doações falsas[139], em similaridade com os golpes solicitando doações após desastres nos Estados Unidos[140].

Globalmente, *malware*, *ransomware spam*, engenharia social e domínios maliciosos utilizando-se da palavra corona têm sido usado pelos golpistas[141] e, no país, dados da Kaspersky mostram que uma a cada oito pessoas sofreu tentativas de golpe entre abril e junho, colocando os brasileiros na posição de um dos mais atacados por golpes durante a pandemia. Os brasileiros estão entre os mais comuns alvos de *phishing*, que tem se utilizado de notícias falsas, especialmente ligadas a falsos programas de auxílio social.[142] Os ataques de *phishing* contra

---

[132] ANATEL. *Anatel alerta sobre fraudes*, 20/02/2019, 08/03/2019 (última atualização).
[133] ANATEL. *Tem fraude no isolamento: todo cuidado é pouco*, 24/03/2020, 13/04/2020 (última atualização).
[134] ANATEL. *#ConexãoSegura: confira dicas para proteger seus dados pessoais*, 25/11/2019, 05/08/2020 (última atualização).
[135] SERASA. *Auxílio Emergencial em Análise: Como Evitar Golpes*.
[136] A empresa Refinaria de Dados é especializada na coleta e análise de informações digitais. ÉPOCA NEGÓCIOS. *Golpes virtuais disparam com covid-19*, 14/06/2020.
[137] Aspas nossas. ÉPOCA NEGÓCIOS. *Golpes virtuais disparam com covid-19*, 14/06/2020.
[138] KASPERSKY. *Centenas de domínios maliciosos usam o tema COVID-19*, 26/03/2020. KASPERSKY. *Golpes via WhatsApp usam coronavírus para roubar dados pessoais*, 20/03/2020.
[139] INFOR CHANNEL. *Seis dicas de como fugir de golpes de doações falsas*, 14/04/2020. INFOR CHANNEL. *Serasa Ensina alerta o consumidor sobre como evitar golpes na internet*, 06/04/2020. SERASA. *Cuidado: fake news e golpes usando coronavírus*.
[140] Vide subseção *1.2. Golpes solicitando doações após desastres* da seção *2. Golpes e fraudes nos Estados Unidos*.
[141] CONVERGÊNCIA DIGITAL. *Brasil é top 5 em ataques hackers usando o coronavírus*, 15/04/2020.
[142] KASPERSKY. *Brasileiros estão entre os mais atacados por golpes durante a pandemia*, 14/08/2020.

dispositivos móveis também cresceram, tendo mais que dobrado na comparação do período março-maio e fevereiro.[143]

Dados da Axur[144] referentes ao 1º trimestre de 2020, por seu turno, indicam que o país bateu novo recorde no registro de ataques de *phishing*: um aumento de 24,23% em comparação com o 4º trimestre de 2019 e de 238,82% em comparação ao 1º trimestre de 2019, com a pandemia do novo coronavírus[145] fazendo aumentar ainda mais esses golpes.[146] Já a Federação Brasileira de Bancos (Febraban) indica que no período pós-Covid o *phishing* cresceu em 70%.[147]

B. CONSIDERAÇÕES FINAIS

São muitos os golpes e fraudes que tentam se aproveitar dos consumidores de telecomunicações ao redor do mundo, utilizando-se muitas vezes de métodos simples como engenharia social e *e-mails*. O presente estudo focou-se em três realidades, mas, de forma geral, para além dessas realidades, as fontes estudadas nesse trabalho parecem indicar que o roubo de identidade e o *phishing*, são práticas comuns em âmbito global e telefone e internet são meios corriqueiramente utilizados para o cometimento de golpes e fraudes.

Golpes em compras, com variações, aparecem nas realidades brasileira, americana e europeia, bem como os golpes/fraudes em que os criminosos tentam se passar por representantes legítimos de instituições públicas e privadas e os golpes que tentam convencer o consumidor que ganhou algum tipo de prêmio.

Na Europa, a Comissão Europeia aponta que o *e-mail* é o recurso predominantemente usado pelos golpistas, mas o telefone, tanto fixo, quanto móvel, ainda é importante, vindo logo atrás. Nos Estados Unidos, por seu turno, dados da Trend Micro indicam uma alta incidência de *ransomware* e liderança global, com folga, na disseminação de ameaças cibernéticas por *e-mail*, enquanto dados de golpes/fraudes registrados junto à FTC referentes a 2019 indicam que o telefone é o meio preferencial para golpes/fraudes e que a maioria das chamadas que viola as restrições de números inseridos na lista nacional de Não Perturbe é, na verdade, de impostores. Enfim, no Brasil, dados da Serasa mostram que uma tentativa de fraude ocorre a cada 17 segundos e dados da Trend Micro mostram que o país também têm grande incidência de ameaças por *e-mail* e *ransomware*, assim como nos Estados Unidos.

---

[143] KASPERSKY. *Brasileiros estão entre os mais atacados por golpes durante a pandemia*, 14/08/2020.
[144] A empresa Axur realiza monitoramento e reação a riscos digitais na internet. INFOR CHANNEL. *Brasil bate novo recorde no número de ataques de phishing*, 02/05/2020.
[145] A incidência de golpes relativos à pandemia nos Estados Unidos foi discutida na subseção *1.21. Golpes relativos à pandemia do novo coronavírus* da seção *2. Golpes e fraudes nos Estados Unidos*.
[146] INFOR CHANNEL. *Brasil bate novo recorde no número de ataques de phishing*, 02/05/2020.
[147] ÉPOCA NEGÓCIOS. *Golpes virtuais disparam com covid-19*, 14/06/2020.

Como se pode perceber pelas informações trazidas por este estudo, os golpes e fraudes que visam os consumidores de serviços de telecomunicações são bastante variados e dinâmicos. Nesse sentido, os consumidores devem estar todo o tempo atentos a possíveis embustes que tentam se aproveitar deles. Com efeito, sendo os serviços de telecomunicações serviços essenciais na atualidade, o número de potenciais vítimas de fraudes/golpes alcança uma magnitude considerável. Assim, não somente a atenção dos consumidores é necessária para coibir essas práticas, mas também a atuação das autoridades reguladoras e das próprias prestadoras de serviços de telecomunicações. Portanto, estudo seguinte a esse abordará iniciativas com foco em informar os consumidores e receber reportes de vítimas, tanto no âmbito governamental, quanto no privado, além de discorrer sobre uma iniciativa internacional.