

ESTUDO - GOLPES E FRAUDES CONTRA O CONSUMIDOR DE TELECOM

PARTE 2 - INICIATIVAS INTERNACIONAIS, NORTE-AMERICANAS, EUROPEIAS E BRASILEIRAS DE PREVENÇÃO

Superintendência de Relações com Consumidores (SRC)

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

Brasília-DF, Outubro/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.

Elaboração¹: Fabio Vianna Velloso e Pryscilla Oliveira.

Revisão: Fábio Koleski e Mariana Fagundes.

Este estudo tem por finalidade a identificação de iniciativas de prevenção de golpes e fraudes contra os consumidores dos serviços de telecomunicações, realizadas por agências reguladoras e as maiores prestadoras de serviços de telecomunicações em três mercados distintos: Europa, Estados Unidos e Brasil. Adicionalmente, especificamente para as realidades britânica, norte-americana e brasileira também é examinado brevemente o arranjo institucional de controle e repressão a golpes e fraudes. O presente trabalho é a segunda parte de uma abordagem mais ampla que realizou, em estudo anterior², a identificação de golpes e fraudes frequentemente perpetrados contra os consumidores nos contextos europeu, norte-americano e brasileiro.

¹ Agradecimentos ao coordenador do Processo de Interações Institucionais e Educação para o Consumo (RCIC1), Octavio Pieranti, e às servidoras Fabiana Marques e Mariana Fagundes, do mesmo processo, pelo fornecimento de informações sobre as iniciativas da Anatel. Agradecimentos também a Eduardo Kruehl, coordenador de processo da Gerência de Qualidade (COQL) da Superintendência de Competição (SCO), por informações gerais e indicação de fontes sobre golpes e fraudes.

² [Estudo - Golpes e fraudes contra o consumidor de telecom - Parte 1 - Identificação de casos na Europa, Estados Unidos e Brasil.](#)

C. INICIATIVAS DE PREVENÇÃO³

Se, por um lado, há uma disseminação de golpes e fraudes que se aproveitam dos usuários dos serviços de telecomunicações para sua realização, por outro, também há iniciativas de prevenção realizadas por órgãos reguladores e prestadores desses serviços. Nesse sentido, essa seção examina ações de cunho público e privado voltadas a comunicar aos usuários sobre a existência de tais embustes e sobre como se precaver para não se tornar uma vítima.

Em que pese o fato de a natureza dos golpes muitas vezes carregarem características de diversos setores, o intuito da análise é verificar as respostas dentro do setor de telecomunicações. Assim, optou-se por verificar os sites das agências reguladoras e da maior empresa de telecomunicações de Reino Unido, Irlanda, Dinamarca⁴ e Estados Unidos. Para o caso do Brasil, além das iniciativas desta Agência Nacional de Telecomunicações e das maiores prestadoras de serviços de telecomunicações do país⁵, também é abordada iniciativa do Comitê Gestor da Internet no Brasil (CGI.br). Adicionalmente, apresenta-se brevemente iniciativa internacional do *econsumer.gov*.

1. INICIATIVAS NA EUROPA

Como visto em estudo da União Europeia⁶, há uma concentração da incidência de golpes e fraudes em alguns países⁷. A Direção-Geral da Justiça e dos Consumidores da Comissão Europeia classifica os golpes/fraudes experimentados pelos europeus em três grandes categorias: golpes em compras, roubo de identidade e fraude monetária.⁸ O Reino Unido lidera os casos de roubo de identidade e roubo em compras, a Irlanda aparece nas três primeiras posições em todas as três

³ Continuação das seções A. *Golpes e fraudes conhecidos* e B. *Considerações finais do Estudo - Golpes e fraudes contra o consumidor de telecom - Parte 1 - Identificação de casos na Europa, Estados Unidos e Brasil*.

⁴ Países com maior incidência de golpes/fraudes na Europa de acordo com estudo realizado pela Comissão Europeia (COMISSÃO EUROPEIA - Direção-Geral da Justiça e dos Consumidores. *Survey on "scams and fraud experienced by consumers" - Final report*, Janeiro 2020), conforme discutido extensamente no *Estudo - Golpes e fraudes contra o consumidor de telecom - Parte 1 - Identificação de casos na Europa, Estados Unidos e Brasil*, p. 3-6.

⁵ O artigo 1º do *Ato nº 6539, de 18 de outubro de 2019* declara que o Grupo Telefônica (Vivo), o Grupo Telecom Américas (Claro), o Grupo Telecom Itália (Tim), o Grupo Oi e o Grupo Sky/AT&T não se enquadram na categoria de Prestadoras de Pequeno Porte. De acordo com a atualização do Plano Geral de Metas de Competição - PGM (Resolução nº 600, de 8 de novembro de 2012) pela *Resolução nº 694, de 17 de julho de 2018*, Prestadora de Pequeno Porte é o "grupo detentor de participação de mercado nacional inferior a 5% (cinco por cento) em cada mercado de varejo em que atua" (artigo 4º, inciso XV).

⁶ COMISSÃO EUROPEIA - Direção-Geral da Justiça e dos Consumidores. *Survey on "scams and fraud experienced by consumers" - Final report*, Janeiro 2020.

⁷ Conforme abordado em estudo anterior: *Estudo - Golpes e fraudes contra o consumidor de telecom - Parte 1 - Identificação de casos na Europa, Estados Unidos e Brasil*, p. 3-6.

⁸ COMISSÃO EUROPEIA - Direção-Geral da Justiça e dos Consumidores. *Survey on "scams and fraud experienced by consumers" - Final report*, Janeiro 2020, p. 10 in *Estudo - Golpes e fraudes contra o consumidor de telecom - Parte 1 - Identificação de casos na Europa, Estados Unidos e Brasil*, p. 3-6.

categorias e a Dinamarca também figura entre as três primeiras posições nas categorias fraude monetária e roubo de identidade⁹.

Tendo em vista que os problemas relacionados aos golpes e fraudes são maiores nesses países, a presente análise segue a opção de verificar a forma como as entidades dos mesmos vêm lidando com isso e como informam os consumidores em seus *sites*.

1.1. Reino Unido

a) Office of Communications - Ofcom

O Office of Communications, mais conhecido como Ofcom, é o regulador britânico de serviços de comunicações e, em seu *site*, possui uma página dedicada a informações sobre chamadas e mensagens indesejadas chamada “Nuisance calls and messages” (Ligações e mensagens incômodas). Nessa seção, o Ofcom caracteriza essas mensagens e ligações indesejadas, incluindo as fraudulentas.¹⁰

Nessa página há em destaque um vídeo instrutivo, de curta duração (2:48m), no qual, por meio de desenhos, o Ofcom dá instruções básicas e rápidas sobre como reduzir chamadas e mensagens incômodas e indesejadas e como reagir ao recebê-las, incluindo indicações de cuidado no fornecimento de informações pessoais e não fornecimento de dados financeiros, bem como instrução para que as vítimas reportem o ocorrido. A página inicial dessa seção foca-se no vídeo, em um curto texto concentrado em informar ao usuário sobre subseções com informações mais detalhadas e, ademais, há também um *link* para um guia fácil sobre como receber menos ligações indesejadas.¹¹

O guia “How to get fewer phone calls you do not want” (Como receber menos ligações que você não deseja) traz de forma instrutiva, por meio de textos curtos e, também, novamente, com a ajuda de desenhos, dicas para receber menos ligações e como reagir ao receber uma ligação ou mensagem indesejada, incluindo instruções sobre não fornecer dados pessoais e financeiros e registrar uma reclamação. Por fim, o guia se encerra narrando uma pequena história de recebimento de ligação indesejada, bem como indica como o usuário pode obter mais informações sobre o tema.¹²

Por seu turno, as páginas dedicadas referenciadas na seção inicial “Nuisance calls and messages” são acessíveis por meio de *links* constantes dessa página principal e abordam vários temas, entre os quais se pode destacar:

⁹ COMISSÃO EUROPEIA - Direção-Geral da Justiça e dos Consumidores. [Survey on “scams and fraud experienced by consumers” - Final report](#), Janeiro 2020, p. 12-13.

¹⁰ OFFICE OF COMMUNICATIONS - OFCOM. [Nuisance calls and messages](#).

¹¹ OFFICE OF COMMUNICATIONS - OFCOM. [Nuisance calls and messages](#).

¹² OFFICE OF COMMUNICATIONS - OFCOM. [How to get fewer phone calls you do not want](#). [Nuisance calls and messages](#).

- Chamadas abusivas e ameaçadoras (*Abusive and threatening calls*): ressalta a importância de se denunciar esse tipo de ligação à empresa de telefonia e até à polícia, indicando tratar-se de ofensa criminal;¹³
- Ligações automatizadas de *telemarketing* (*Automated marketing calls*): caracteriza esse tipo de ligação e indica que ligações gravadas de *telemarketing* podem tratar-se de golpes em que o consumidor é induzido a transferir dinheiro, comprar antecipadamente algum produto ou realizar ligações telefônicas com tarifação elevada para que possa receber algum prêmio ou oferta, bem como essas ligações podem também solicitar informações pessoais ou bancárias. Nesses casos em que a ligação traz a característica de golpe, a Ofcom instrui os consumidores a contactarem, para mais informações e registro de ocorrências, a polícia, no caso da Escócia e o Action Fraud¹⁴, no caso da Inglaterra, País de Gales e Irlanda do Norte;¹⁵
- Proteja-se de chamadas incômodas (*Protect yourself from nuisance calls*): traz informações específicas para as pessoas aprenderem a se proteger de chamadas incômodas, através de duas subseções: “Como reduzir chamadas incômodas” (*How to reduce nuisance calls*) e “O que fazer ao receber chamadas e mensagens incômodas” (*What to do when you receive nuisance calls and messages*). Nesta subseção, em especial, é enfatizado que dados pessoais e bancários não devem ser fornecidos, além da indicação de que, em caso de ligações solicitando dados financeiros, o consumidor deve desligar a ligação, esperar pelo menos cinco minutos para garantir que o fraudador não esteja mais ocupando a linha e ligar para os números fornecidos por sua instituição financeira, por exemplo, em uma fatura;¹⁶
- Golpes de investimento (*Investment scams*): explica como os golpes de investimento acontecem, afirma que acontecem 3,5 vezes mais com pessoas acima dos 65 anos e com economias acima de £ 10.000, bem como informa como os golpistas agem e o que pode ser feito para se prevenir e denunciar;¹⁷
- Ligações de televendas (*Live telesales calls*): caracteriza as ligações de vendas e, assim como no caso das ligações automatizadas, indica que podem se tratar de golpes;¹⁸ e
- Golpes de falsificação de números (*Number spoofing scams*): presta informações sobre a prática do *spoofing*, divididas nas seguintes subseções: “Por que eles fazem isso” (*Why do they do this?*), “O que está sendo feito” (*What is being done?*), “O que você deveria fazer”

¹³ OFFICE OF COMMUNICATIONS - OFCOM. [Abusive and threatening calls](#).

¹⁴ Informações sobre o Action Fraud mais à frente na subseção [c\) Action Fraud e National Fraud Intelligence Bureau](#) desta seção.

¹⁵ OFFICE OF COMMUNICATIONS - OFCOM. [Automated marketing calls](#)

¹⁶ OFFICE OF COMMUNICATIONS - OFCOM. [How to protect yourself from nuisance calls and messages](#).

¹⁷ OFFICE OF COMMUNICATIONS - OFCOM. [Cold call investment scams](#).

¹⁸ OFFICE OF COMMUNICATIONS - OFCOM. [Live telesales calls](#).

(*What should you do?*) e “Eu acho que fui vítima de *spoofing*” (*I think I've been a victim of Caller ID spoofing*). Essa última subseção aponta que, além de alertar pessoas próximas, como família, amigos e vizinhos, os consumidores devem realizar denúncias ao Action Fraud e ao Trading Standards^{19, 20}

b) British Telecom

A British Telecom (BT)²¹ mantém página dedicada ao assunto em seu *site* intitulada “Scam calls”²². Logo no início da página há botão/link em destaque para denúncias, que abre um formulário *on-line* para esse tipo de reporte.²³

Além de alertar aos consumidores sobre informações que a empresa nunca solicita por telefone (referentes a dados bancários, bem como ao funcionamento do serviço de banda larga e do próprio computador do consumidor), a página também traz indicações de como o consumidor pode se manter protegido no que se refere a ligações, ao uso do computador e à navegação na internet; além de *links* úteis, incluindo informações sobre denúncia ao Action Fraud.²⁴

c) Action Fraud e National Fraud Intelligence Bureau

Conforme visto nas duas seções anteriores, tanto o Ofcom, quanto a British Telecom fazem referência direta ao Action Fraud como o órgão a ser acionado pelos consumidores no contexto de golpes e fraudes. O Action Fraud é o órgão nacional do Reino Unido encarregado do registro de golpes, fraudes e crimes cibernéticos. Responsável pela centralização dessas ocorrências na Inglaterra, País de Gales e Irlanda do Norte (na Escócia a polícia nacional continua com a jurisdição sobre esses casos específicos), o Action Fraud é gerido pela força policial da cidade de Londres juntamente com o Birô Nacional de Inteligência em Fraude (National Fraud Intelligence Bureau - NFIB). Nesse sentido, o Action Fraud centraliza os registros sobre crimes com motivação financeira na internet, bem como fraudes, enquanto o National Fraud Intelligence Bureau avalia esses registros e os distribui. Assim, apesar de fornecer o número da ocorrência policial, não é o Action Fraud que investiga os casos, repassando-os ao NFIB.²⁵

¹⁹ O Trading Standards é um serviço de proteção aos consumidores e à comunidade contra comerciantes desonestos ou que agem de forma desleal. OFFICE OF COMMUNICATIONS - OFCOM. [Number spoofing scams](#).

²⁰ OFFICE OF COMMUNICATIONS - OFCOM. [Number spoofing scams](#).

²¹ De acordo com dados da Statista, a British Telecom foi líder na telefonia móvel em 2018 (28% de *market share*) e na telefonia fixa em 2019 (40% de *market share*). STATISTA. [Market share held by mobile operators in the United Kingdom \(UK\) 2018, by subscriber. Market share held by landline-based telecommunications suppliers in the United Kingdom \(UK\) from 2015 to 2020](#). Por seu turno, de acordo com dados da OFCOM, em 2018 a British Telecom foi líder no *market share* da banda larga fixa com 34,59% das conexões. OFFICE OF COMMUNICATIONS - OFCOM. [The Communications Market Report - Interactive data - Fixed broadband connections by ISP \(%\)](#).

²² BRITISH TELECOM. [Scam calls](#).

²³ BRITISH TELECOM. [Report scam calls](#).

²⁴ BRITISH TELECOM. [Report scam calls](#).

²⁵ ACTION FRAUD. [What is Action Fraud?](#).

O National Fraud Intelligence Bureau, também ligado à polícia de Londres e com atuação na perspectiva nacional, analisa as ocorrências reportadas ao Action Fraud, tanto gerando inteligência, quanto encaminhando-as a agências policiais ou forças policiais locais para investigação. A NFIB também tem um nível de *enforcement*, podendo derrubar *sites* e telefones ligados a fraudadores, bem como bloquear contas bancárias. Com efeito, nem todas as ocorrências são seguidas de investigação, mas todas geram inteligência para que, de forma geral, o ambiente do Reino Unido torne-se desfavorável à operação de fraudadores e, assim, sejam poupadas potenciais vítimas.²⁶

O Action Fraud oferece a possibilidade de registro de ocorrências em seu *site* ou por telefone, incluindo, no caso de empresas, organizações ou instituições de caridade, o reporte de ataques cibernéticos em progresso a qualquer hora do dia.²⁷ Também em sua página na *web* o órgão informa sobre crimes cibernéticos e fraudes, bem como seus tipos; dá orientações para prevenção e veicula notícias sobre essa temática.²⁸

Entre as dicas de prevenção dadas pela Action Fraud estão: instalar e manter atualizados antivírus e *firewall*; não informar quaisquer dados pessoais, incluindo dados financeiros, antes de se certificar da autenticidade da solicitação; estar atento a *e-mails* de *phishing*; configurar o navegador de internet no nível máximo de segurança; nunca clicar em *links* de *e-mails* ou mensagens suspeitas; instalar as versões mais recentes de *softwares* e aplicativos, bem como mantê-los atualizados em todos os seus dispositivos; desconfiar de contas, boletos ou faturas de produtos que você não comprou ou de empresas com as quais você geralmente não faz negócios e, nas compras *on-line*, sempre que disponível, utilizar opções de segurança oferecidas por empresas de cartão de crédito.²⁹

1.2. Irlanda

a) Commission for Communications Regulation - ComReg

O órgão regulador de telecomunicações na Irlanda, o Commission for Communications Regulation (ComReg) possui página dedicada em seu *site* para informar os consumidores sobre chamadas móveis³⁰ e fixas³¹ fraudulentas, não havendo informações sobre golpes e fraudes nas páginas dedicadas à banda larga³².

As páginas dedicadas a fraudes realizadas por meio dos serviços telefônicos são subseções das páginas dedicadas a esses serviços, que, por sua vez, encontram-se na seção do *site* dedicada a informações ao consumidor.³³ Em ambas as páginas as informações são basicamente as

²⁶ ACTION FRAUD. [Who are the National Fraud Intelligence Bureau?](#).

²⁷ ACTION FRAUD. [Reporting fraud and cyber crime](#).

²⁸ ACTION FRAUD. [Action Fraud](#).

²⁹ ACTION FRAUD. [Protect yourself from fraud and cyber crime](#).

³⁰ COMMISSION FOR COMMUNICATIONS REGULATION - ComReg. [Consumer information - Scam phone numbers](#).

³¹ COMMISSION FOR COMMUNICATIONS REGULATION - ComReg. [Consumer information - Scam calls](#).

³² COMMISSION FOR COMMUNICATIONS REGULATION - ComReg. [Consumer information - Internet](#).

³³ COMMISSION FOR COMMUNICATIONS REGULATION - ComReg. [Consumer information](#).

mesmas³⁴, indicando ao consumidor que o regulador entende que há uma miríade de golpes telefônicos e que os consumidores devem estar alerta em todos os momentos. Nesse sentido, o regulador apresenta alguns alertas ao consumidor, como: tomar cuidado com várias ligações recebidas/perdidas de números desconhecidos, entrar em contato com a prestadora de serviços de telecomunicações e seguir seu código de conduta em caso de o usuário eventualmente retornar ligação de número desconhecido ou receber ligações persistentes de números desconhecidos e, ainda, não fornecer quaisquer informações pessoais.³⁵

b) EIR

A prestadora de telecomunicações EIR³⁶ mantém uma página dedicada ao tema segurança *on-line* dividida nas seções: “*Phishing* e ameaças atuais” (*Phishing & Current Threats*), “Como a EIR te protege” (*How eir protects you*) e “Dicas para segurança *on-line*” (*Tips for Online Security*)³⁷.

Na seção “*Phishing* e ameaças atuais” são caracterizados o que é *phishing* e suas variações (chamadas telefônicas de *phishing* - chamadas conhecidas como *vishing*, *e-mails* de *phishing* e mensagens de texto SMS de *phishing* - conhecidas como *smishing*), bem como são descritos exemplos de ameaças atuais, reproduzindo-se *e-mails* que os golpistas costumam enviar. Por seu turno, na seção “Como a EIR te protege” a prestadora lista seus endereços *web*, aconselhando que os consumidores sempre confirmem os endereços, bem como alerta aos usuários que denunciem, à polícia, chamadas, mensagens de texto, *e-mails* ou qualquer suspeita. Por fim, a seção “Dicas para segurança *on-line*” apresenta dicas para identificar um *e-mail* de *phishing*, o que fazer em caso de se receber um desses *e-mails* e dicas adicionais que envolvem navegar e baixar arquivos de forma segura, instalar antivírus, criar senhas fortes e manter o sistema operacional e os navegadores de internet atualizados.³⁸

1.3. Dinamarca

a) Agência Dinamarquesa de Energia (ENS)

A Agência Dinamarquesa de Energia é também o órgão regulador do setor de telecom na Dinamarca. Não foi encontrada nenhuma informação estruturada sobre o assunto de golpes e fraudes praticados contra consumidores de telecom no site do regulador³⁹.

³⁴ A única diferença é um alerta referente a eventual existência de identificador de chamadas no caso dos aparelhos fixos. COMMISSION FOR COMMUNICATIONS REGULATION - ComReg. [Consumer information - Scam calls](#).

³⁵ COMMISSION FOR COMMUNICATIONS REGULATION - ComReg. [Consumer information - Scam calls](#). [Consumer information - Scam phone numbers](#).

³⁶ Segundo dados da ComReg referentes ao primeiro trimestre de 2020, a EIR lidera nos mercados de telefonia fixa e banda larga fixa na Irlanda. COMMISSION FOR COMMUNICATIONS REGULATION - ComReg. [Irish Communications Market - Quarterly Key Data Report Q1 2020](#), p. 5-6.

³⁷ Grifos nossos. EIR. [Phishing & Current Threats](#). Ao clicar no link *Online Safety* ao final da página inicial da prestadora (<https://www.eir.ie/>) o usuário é direcionado para a URL <https://www.eir.ie/online-safety/> que possui as três seções referenciadas, sendo que o usuário é automaticamente direcionado para a seção *Phishing & Current Threats*.

³⁸ Grifos nossos. EIR. [Phishing & Current Threats](#).

³⁹ ENERGISTYRELSEN. [Ansvarsområder](#).

b) TDC

A TDC⁴⁰ é a maior empresa de telecomunicações da Dinamarca⁴¹, possuindo página dedicada a informações sobre golpes⁴². Nela, a empresa fala que as chamadas fraudulentas tornaram-se um grande problema nos últimos anos, disponibiliza um botão/link para denunciar golpes e informa sobre os principais tipos de golpe, quais sejam: “Golpes de Wangiri (números estrangeiros)” (*Wangiri-svindel (udenlandske numre)*) e “Spoofing (geralmente de um número dinamarquês)” (*Spoofing (Oftest fra et dansk nummer)*)⁴³.

Ainda nessa página há uma seção de perguntas e respostas com as seguintes questões: “Outros dizem que recebem ligações do meu número” (*Andre siger, at de bliver ringet op fra mit nummer*), “Por que os golpistas usam spoofing?” (*Hvorfor bruger svindlere spoofing?*), “O que você deve fazer se for exposto a spoofing?” (*Hvad skal du gøre, hvis du er udsat for spoofing?*) e “Se o seu número for usado para falsificação?” (*Hvis dit nummer bliver brugt til spoofing?*)⁴⁴.

Ao final da página, o botão/link para denunciar golpes é repetido, informa-se um número de telefone para quem queira sanar dúvidas e acrescenta-se um botão/link para clientes da Yousee.⁴⁵

c) Yousee

A Yousee é uma subsidiária do grupo TDC que, em 2016, absorveu a base de clientes não comerciais da TDC⁴⁶. A empresa também mantém página dedicada à segurança *on-line* em seu *website*. A página possui uma grande área central para busca sobre o assunto no *site* da Yousee e, logo abaixo, três abas de informações: “Os perigos da *web*” (*Farerne på nettet*), “Crianças e segurança” (*Børne & sikkerhed*) e “Segurança para celulares” (*Mobil sikkerhed*)⁴⁷.

Na aba “Os perigos da *web*” são apresentados *links* com informações sobre: “Ameaças e proteção *on-line*”, “Segurança de rede em casa”, “Segurança de rede em redes públicas” e “Conceitos de segurança de TI”.⁴⁸

Por seu turno, a seção “Ameaças e proteção *on-line*” apresenta as opções “Proteção” e “Ameaças”, sendo que, por sua vez, cada uma dessas opções apresenta novas subseções com informações sobre *firewall*, antivírus, *antispyware*, atualização de *software*, filtro de *spam*, filtro de *phishing*, senha e precauções para a opção “Proteção” e *phishing*, *sites* infectados, programas infectados, *hacking*, *malware*, *spam*, *spyware* e *ransomware* para a opção “Ameaças”, bem como

⁴⁰ Anteriormente Tele Danmark. Houve mudança do nome para TDC Group no ano 2000. TDC GROUP. [History of the TDC - In short](#).

⁴¹ Dados da Alertify indicam que TDC lidera o *market share* na Dinamarca, com 37% do mercado. ALERTIFY. [Denmark telecom companies](#).

⁴² TDC ERHVERV. [Fupopkald - hvad er det?](#).

⁴³ Tradução do Google. TDC ERHVERV. [Fupopkald - hvad er det?](#).

⁴⁴ Tradução do Google. TDC ERHVERV. [Fupopkald - hvad er det?](#).

⁴⁵ Tradução do Google. TDC ERHVERV. [Fupopkald - hvad er det?](#).

⁴⁶ TDC ERHVERV. [Historien om TDC Erhverv - kort fortalt](#).

⁴⁷ Grifos nossos. Tradução do Google. YOUSEE. [Sikkerhed på nettet](#).

⁴⁸ Grifos nossos. Tradução do Google. YOUSEE. [Sikkerhed på nettet](#).

uma subseção presente em ambas as opções, denominada “Visão geral de ameaças e proteção on-line”. Em especial nessa última subseção há um quadro indicando medidas de proteção que são eficazes em relação a certas ameaças.⁴⁹

Tabela 1 - Visão geral de ameaças e como se proteger⁵⁰

Beskyttelse Trusler	Firewall	Antivirus	Antispyware	Opdatering	Spam-filter	Phishing-filter	Adgangskode	Omtanke
Inficerede hjemmesider		✓		✓				✓
Inficerede programmer		✓		✓				✓
Hacking	✓			✓			✓	✓
Malware		✓		✓			✓	
Spam					✓			✓
Phishing				✓		✓		✓
Spyware		✓	✓	✓	✓			
Ransomware		✓		✓			✓	✓

FONTE: YOUSEE. [Sikkerhed på nettet - Farerne på nettet - Online trusler og beskyttelse - Beskyttelse - Oversigt over online trusler og beskyttelse - Oversigt over trusler og hvordan du beskytter dig.](#)

A seção “Segurança de rede em casa” apresenta dicas no mínimo curiosas, pois sugere que os consumidores não tomem medidas de proteção. Primeiro, alerta para que não se faça nada para se proteger a internet sem fio, porque a empresa já garante que seu *modem* wi-fi possui um *firewall* embutido com criptografia WPA2-Personal, que já protege contra *hackers* e que embora o código seja curto, é virtualmente inquebrável. Nesse sentido, a prestadora aponta então que fazer alterações na configuração do *modem* pode tornar a rede menos segura. Depois, sugere que as pessoas não alterem as senhas de suas redes e se o fizerem que tomem cuidado. Por fim, não recomenda que os clientes ocultem o nome de suas redes sem fio e afirma que apesar de a rede estar bem protegida por parte da prestadora, o consumidor deve ter atenção ao baixar arquivos e instalar programas, certificando-se sempre que o sistema operacional e o antivírus estejam atualizados, bem como que os arquivos baixados sejam provenientes de *sites* e *e-mails* confiáveis.⁵¹

Enfim, a seção “Conceitos de segurança de TI”, como o nome diz, traz as definições dos conceitos apresentados ao longo das seções e subseções e a seção “Segurança de rede em redes

⁴⁹ Grifos nossos. Tradução do Google. YOUSEE. [Sikkerhed på nettet](#).

⁵⁰ De acordo com o [Google Tradutor](#): *beskyttelse* - proteção; *opdatering* - atualizando (supõe-se que a forma “atualização” enquadre-se melhor nesse contexto); *adgangskode* - senha; *omtanke* - cuidado; *trusler* - ameaças; *inficerede hjemmesider* - sites infectados; e *inficerede programmer* - programas infectados.

⁵¹ Tradução do Google. YOUSEE. [Sikkerhed på nettet](#).

públicas” apresenta dicas para se manter seguro ao acessar uma rede pública, entre os quais, verificar o nome da rede, ativar o *firewall*, usar uma conexão segura (https) e utilizar antivírus.⁵²

A aba “Crianças e segurança”, por seu turno, é dividida nas seções “Proteja seu filho *on-line*”, “Netiqueta - mantenha o bom tom *on-line*” e “Regras familiares no Pacote de Segurança”.⁵³

A seção “Proteja seu filho *on-line*” traz nove dicas de proteção para os pais quanto ao uso da internet pelas crianças:⁵⁴

1. “Converse com seu filho sobre a internet;
2. Siga seu filho *on-line*;
3. Trate os outros *on-line* como gostaria de ser tratado;
4. Discuta o consumo de rede na família;
5. Ensine seu filho a não compartilhar informações pessoais;
6. Esteja presente se seu filho quiser encontrar um conhecido da rede;
7. Lembre-se de ter bom senso;
8. Não critique a curiosidade do seu filho;
9. Relate informações e situações que você acredita serem graves”.⁵⁵

As seções “Netiqueta - mantenha o bom tom *on-line*” e “Regras familiares no Pacote de Segurança”, por seu turno, falam, respectivamente, sobre dicas de etiqueta na internet para crianças e jovens, como empatia, linguagem, estar alerta, pensar antes de marcar as pessoas nas redes sociais, bem como evitar ironia e sobre informações sobre a ativação, no pacote de segurança da prestadora, de regras familiares visando a segurança das crianças e adolescentes.⁵⁶

Enfim, a aba “Segurança para celulares” subdivide-se em “Antivírus em celulares e *tablets*”, “7 dicas para segurança em dispositivos móveis”, “Golpe - evite ser enganado” e “*Spoofing* - chamadas falsas de números dinamarqueses”.⁵⁷

A seção “Antivírus em celulares e *tablets*” ressalta a importância de se ter um antivírus e dá sugestões nesse sentido, enquanto a seção “7 dicas para segurança em dispositivos móveis” propõe as seguintes sete dicas de segurança para dispositivos móveis:⁵⁸

1. Pacote de segurança e antivírus móvel: recomenda a instalação;
2. Redes sem fio (públicas): recomenda tomar cuidado ao acessar redes abertas, além de sempre solicitar que seu dispositivo não mantenha na memória a conexão automática a esses tipos de redes;

⁵² Tradução do Google. YOUSEE. [Sikkerhed på nettet](#).

⁵³ Grifos nossos. Tradução do Google. YOUSEE. [Sikkerhed på nettet](#).

⁵⁴ Grifos nossos. Tradução do Google. YOUSEE. [Sikkerhed på nettet](#).

⁵⁵ Grifos nossos. Tradução do Google. YOUSEE. [Sikkerhed på nettet](#).

⁵⁶ Grifos nossos. Tradução do Google. YOUSEE. [Sikkerhed på nettet](#).

⁵⁷ Grifos nossos. Tradução do Google. YOUSEE. [Sikkerhed på nettet](#).

⁵⁸ Grifos nossos. Tradução do Google. YOUSEE. [Sikkerhed på nettet](#).

3. Senha/PIN/Bloqueio de tela: recomenda que mesmo que pareça irritante, o usuário insira proteção de desbloqueio para seus dispositivos;
4. Faça um *backup*: assim a perda de fotos, contatos e arquivos é evitada e na troca ou eventual roubo de dispositivos fica fácil restaurar os conteúdos;
5. Encontre o celular: além de funções dos sistemas operacionais permitirem a exclusão de dados no caso de roubo, é também necessário comunicar à prestadora a ocorrência para que o cartão SIM seja bloqueado;
6. Baixando aplicativos: é necessário verificar a confiabilidade dos aplicativos, pois eles podem conter vírus ou *spyware* e, nesse sentido, a instalação de um antivírus ou pacote de segurança garantem ainda mais proteção; e
7. Bom senso: é sempre necessário estar atento às suas atividades *on-line* para que você fique menos exposto a crimes cibernéticos.⁵⁹

Por fim, a seção “Golpe - evite ser enganado” alerta para o crescente número de golpes em que pessoas se passam por representantes da prestadora para enganar o consumidor, apresentando a possibilidade de denúncia, bem como caracterizando o esquema de Wangiri e os golpes de *spoofing*; enquanto a seção “*Spoofing* - chamadas falsas de números dinamarqueses” se debruça mais propriamente sobre esse último golpe.⁶⁰

2. INICIATIVAS NOS ESTADOS UNIDOS

No que tange ao registro de fraudes nos Estados Unidos, em termos de tema, roubo de identidade e fraude contra consumidores devem ser reportados à Comissão Federal de Comércio (Federal Trade Commission - FTC), enquanto fraudes em geral, fraudes na internet e fraudes de sorteio/loterias pela internet devem ser reportados ao Birô Federal de Investigação (Federal Bureau of Investigation - FBI) - nos últimos dois casos, especificamente ao Centro de Reclamação de Crimes na Internet (Internet Crime Complaint Center - IC3).⁶¹ Ademais, no caso de golpes telefônicos, as reclamações são registradas junto a Comissão Federal de Comunicações (Federal Communications Commission - FCC).⁶²

Como se pode perceber, o Internet Crime Complaint Center (IC3) tem como foco crimes cometidos por meio da internet⁶³, sendo um centro de recebimento de reportes que, com propósitos

⁵⁹ Tradução do Google. No caso da dica 7, o Google traduziu a palavra *omtanke* como pensamento, tendo-se optado aqui, pelo restante da tradução desse item, em renomeá-lo para bom senso. YOUSEE. [Sikkerhed på nettet](#).

⁶⁰ Grifos nossos. Tradução do Google. YOUSEE. [Sikkerhed på nettet](#).

⁶¹ UNITED STATES DEPARTMENT OF JUSTICE. [Report fraud](#).

⁶² FEDERAL COMMUNICATIONS COMMISSION - FCC. [After Storms, Watch Out for Scams](#). [Mexico Collect Call Scam](#). [Slamming: Switching Your Authorized Telephone Company Without Permission](#). [Watch out for Auto Warranty Scams](#).

⁶³ FEDERAL BUREAU OF INVESTIGATION - FBI. INTERNET CRIME COMPLAINT CENTER - IC3. [Internet Crime Complaint Center IC3](#).

de investigação e inteligência, analisa e divulga as informações recebidas a forças policiais e para conscientização do público em geral⁶⁴. No *site* do centro, além da possibilidade de registro de reclamação⁶⁵, também são disponibilizados relatórios de crimes na internet⁶⁶, realizados alertas ao consumidor⁶⁷ e à indústria⁶⁸, caracterizados alguns tipos de golpes e fraudes, bem como fornecidas orientações sobre como evitá-los e instruções sobre como proceder em caso de se tornar vítima⁶⁹.

De forma geral, o FBI tem como missão a defesa e o *enforcement* das leis criminais norte-americanas, tendo entre suas principais funções a condução de investigações, a produção de inteligência e o desmantelamento de organizações criminosas.⁷⁰ Ademais, é a agência federal a cargo da liderança da resposta investigativa a ataques cibernéticos e intrusões⁷¹, bem como investiga fraudes e produz inteligência sobre.⁷² O Birô também encabeça a Força-Tarefa Conjunta Nacional de Investigação Cibernética (National Cyber Investigative Joint Task Force - NCIJTF)⁷³, que congrega mais de 30 agências entre comunidade de inteligência, Departamento de Defesa americano e forças policiais⁷⁴.

O *site* do FBI propriamente dito também oferece um panorama sobre golpes na internet⁷⁵ e dicas de como se proteger, incluindo utilização e manutenção de *softwares* de sistema operacional, *firewall*, antivírus e *antispyware* atualizados, cuidado com os arquivos de *download*, atenção a endereços de *e-mails* e de páginas na internet, não clicar em *links* de mensagens e *e-mails* não solicitados, cuidado com o que se compartilha *on-line* e em redes sociais, realizar *backups* e mantê-los seguros, optar por autenticação em duas etapas ou multifator sempre que disponível, bem como informações específicas para proteger as crianças.⁷⁶

A Federal Trade Commission (FTC), por seu turno, além de educação e defesa, tem poder de *enforcement* para proteger o consumidor e a competição.⁷⁷ O órgão tanto fornece informações aos

⁶⁴ FEDERAL BUREAU OF INVESTIGATION - FBI. INTERNET CRIME COMPLAINT CENTER - IC3. [About IC3](#).

⁶⁵ FEDERAL BUREAU OF INVESTIGATION - FBI. INTERNET CRIME COMPLAINT CENTER - IC3. [File a complaint](#).

⁶⁶ FEDERAL BUREAU OF INVESTIGATION - FBI. INTERNET CRIME COMPLAINT CENTER - IC3. [Annual Reports](#).

⁶⁷ FEDERAL BUREAU OF INVESTIGATION - FBI. INTERNET CRIME COMPLAINT CENTER - IC3. [Consumer Alerts](#).

⁶⁸ FEDERAL BUREAU OF INVESTIGATION - FBI. INTERNET CRIME COMPLAINT CENTER - IC3. [Industry Alerts](#).

⁶⁹ FEDERAL BUREAU OF INVESTIGATION - FBI. INTERNET CRIME COMPLAINT CENTER - IC3. [Internet Crime Prevention Tips](#). [Internet Crime Schemes](#). [What is BEC?](#). [What is Ransomware?](#).

⁷⁰ UNITED STATES DEPARTMENT OF JUSTICE. [Organization, mission and functions manual: Federal Bureau of Investigation](#).

⁷¹ FEDERAL BUREAU OF INVESTIGATION - FBI. [What we investigate - The Cyber Threat](#).

⁷² FEDERAL BUREAU OF INVESTIGATION - FBI. [What we investigate - White-Collar Crime](#).

⁷³ FEDERAL BUREAU OF INVESTIGATION - FBI. [What we investigate - The Cyber Threat](#).

⁷⁴ FEDERAL BUREAU OF INVESTIGATION - FBI. [What we investigate - Cyber Crime - National Cyber Investigative Joint Task Force](#).

⁷⁵ FEDERAL BUREAU OF INVESTIGATION - FBI. [Scams and safety - Common Scams And Crimes - Business Email Compromise](#). [Scams and safety - Common Scams And Crimes - Identity Theft](#). [Scams and safety - Common Scams And Crimes - Ransomware](#). [Scams and safety - Common Scams And Crimes - Spoofing and Phishing](#). [Scams and safety - On the Internet](#). [What we investigate - The Cyber Threat](#).

⁷⁶ FEDERAL BUREAU OF INVESTIGATION - FBI. [Scams and safety - Common Scams And Crimes - Business Email Compromise](#). [Scams and safety - Common Scams And Crimes - Identity Theft](#). [Scams and safety - Common Scams And Crimes - Ransomware](#). [Scams and safety - Common Scams And Crimes - Spoofing and Phishing](#). [Scams and safety - On the Internet](#). [Scam and safety - Protecting Your Kids](#).

⁷⁷ FEDERAL TRADE COMMISSION - FTC. [About the FTC](#).

consumidores, quanto investiga fraudes.⁷⁸ De fato, a FTC é a única agência federal com jurisdição geral sobre a fraude contra o consumidor.⁷⁹ O *enforcement* da agência tem circunscrição civil, não podendo a agência realizar prisões propriamente, cabendo esse encargo a órgãos governamentais e forças policiais com as quais a FTC trabalha em parceria. Em especial, a FTC alerta a promotorias criminais quando alguma de suas investigações revela infringência a leis criminais⁸⁰. Apesar de não ter autoridade criminal, a agência possui uma unidade específica de intermediação criminal, a FTC's Criminal Liaison Unit (CLU), focada em melhorar a coordenação entre a FTC e órgãos com poder de execução criminal e, assim, aumentar os números de casos de fraude contra o consumidor processados criminalmente⁸¹.

Já a Federal Communications Commission (FCC) tem como responsabilidade a implementação e a aplicação das leis e regulamentos de comunicações norte-americanas.⁸² Entre os Birôs que compõem a FCC encontra-se o Enforcement Bureau (EB), encarregado da fiscalização e aplicação do "Ato de Comunicações de 1934 [Communications Act of 1934], outros estatutos e as regras, ordens e termos e condições de licenças e outras autorizações da FCC"⁸³. O EB tem poderes investigativos, podendo, entre outros, realizar auditorias e emitir intimações.⁸⁴ Em especial, esse Birô possui uma divisão de consumidor, a Telecommunications Consumers Division (TCD), incumbida de "proteger os consumidores de práticas fraudulentas e enganosas, bem como de outras práticas prejudiciais".⁸⁵ O Enforcement Bureau pode, entre outros, realizar confiscos⁸⁶ e ordenar a cessação de condutas (*cease and desist*)⁸⁷, mas, para a abertura de um processo criminal, a FCC deve acionar o Departamento de Justiça americano, ou seja, a FCC em si não tem autoridade para abrir um processo criminal⁸⁸.

Além das informações trazidas nessa introdução, seguindo a estrutura adotada por este estudo, são abordados, com maior profundidade, nas seções a seguir, as iniciativas das agências reguladoras FCC e FTC para informar aos consumidores sobre como evitar e relatar golpes/fraudes,

⁷⁸ FEDERAL TRADE COMMISSION - FTC. [About the FTC - Office of Inspector General - FTC Imposter Scams](#).

⁷⁹ FEDERAL TRADE COMMISSION - FTC. [Enforcement - Criminal Liaison Unit](#).

⁸⁰ FEDERAL TRADE COMMISSION - FTC. [FTC aids criminal prosecutions](#), 14/06/2018.

⁸¹ FEDERAL TRADE COMMISSION - FTC. [Enforcement - Criminal Liaison Unit](#).

⁸² FEDERAL COMMUNICATIONS COMMISSION - FCC. [About the FCC - About the FCC Overview](#).

⁸³ Tradução nossa. No original: "The Enforcement Bureau (EB or Bureau) has primary responsibility for the FCC's enforcement of the Communications Act of 1934, as amended (Act), other statutes, and the FCC's rules, orders, and terms and conditions of licenses and other authorizations". FEDERAL COMMUNICATIONS COMMISSION - FCC. ENFORCEMENT BUREAU. [Enforcement overview](#), Abril 2020, p. 4.

⁸⁴ FEDERAL COMMUNICATIONS COMMISSION - FCC. ENFORCEMENT BUREAU. [Enforcement overview](#), Abril 2020, p. 4.

⁸⁵ Tradução nossa. No original: "The Telecommunications Consumers Division (TCD) focuses on protecting consumers from fraudulent, misleading, and other harmful practices involving telecommunications". FEDERAL COMMUNICATIONS COMMISSION - FCC. ENFORCEMENT BUREAU. [Enforcement overview](#), Abril 2020, p. 5.

⁸⁶ FEDERAL COMMUNICATIONS COMMISSION - FCC. ENFORCEMENT BUREAU. [Enforcement overview](#), Abril 2020, p. 14.

⁸⁷ FEDERAL COMMUNICATIONS COMMISSION - FCC. ENFORCEMENT BUREAU. [Enforcement overview](#), Abril 2020, p. 20.

⁸⁸ FEDERAL COMMUNICATIONS COMMISSION - FCC. ENFORCEMENT BUREAU. [Enforcement overview](#), Abril 2020, p. 21-22.

bem como as iniciativas da maior prestadora americana de serviços de telecomunicações, a AT&T⁸⁹.

1.1. Federal Communications Commission - FCC

A FCC possui página específica em seu *site* para informar sobre fraudes, golpes e alertas. Intitulado “Frauds, Scams and Alerts” a página consta do menu “Consumer Guides” e apresenta uma relação de *links* temáticos que levam a páginas com informações específicas sobre o tipo de golpe, fraude ou alerta abordado⁹⁰. As páginas específicas dos golpes/fraudes apresentam, entre outras informações, como os golpes/fraudes ocorrem, o que se deve saber sobre eles⁹¹, o que os usuários podem fazer para se proteger/evitá-los e como registrar reclamações.⁹²

Entre os golpes/fraudes abordados pela FCC estão golpes que fazem uso de PBX/PABX⁹³, golpes solicitando doações após desastres⁹⁴, golpes de garantia/seguro automotivo⁹⁵, golpes envolvendo *spoofing*⁹⁶, fraude de celular⁹⁷, fraudes no serviço de retransmissão de IP⁹⁸, golpe de ligações a cobrar originadas no México⁹⁹, golpe da ligação de um toque¹⁰⁰, ligações e mensagens automatizadas não autorizadas¹⁰¹, golpe de mudança de prestadora sem autorização¹⁰², apropriação de caixa postal¹⁰³ e golpes relativos à pandemia do novo coronavírus¹⁰⁴.

Entre as dicas fornecidas pela FCC para evitar esses golpes estão: perguntar ao chamador por seu nome e número de telefone¹⁰⁵; desligar o telefone e não discar números ou transferir chamadas antes de fazê-lo¹⁰⁶; não atender ou retornar ligações de números desconhecidos e, se o

⁸⁹ 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](#).

⁹⁰ Vários desses golpes/fraudes foram abordados na seção sobre golpes e fraudes nos Estados Unidos no [Estudo - Golpes e fraudes contra o consumidor de telecom - Parte 1 - Identificação de casos na Europa, Estados Unidos e Brasil](#), p. 7-16.

⁹¹ Esses dois tópicos - como os golpes/fraudes ocorrem e o que se deve saber sobre eles - foram abordados na seção sobre golpes e fraudes nos Estados Unidos no [Estudo - Golpes e fraudes contra o consumidor de telecom - Parte 1 - Identificação de casos na Europa, Estados Unidos e Brasil](#), p. 7-16.

⁹² FEDERAL COMMUNICATIONS COMMISSION - FCC. [Frauds, Scams and Alerts](#).

⁹³ FEDERAL COMMUNICATIONS COMMISSION - FCC. [Don't Fall for the 90# Telephone Scam](#).

⁹⁴ FEDERAL COMMUNICATIONS COMMISSION - FCC. [After Storms, Watch Out for Scams](#).

⁹⁵ FEDERAL COMMUNICATIONS COMMISSION - FCC. [Watch out for Auto Warranty Scams](#).

⁹⁶ FEDERAL COMMUNICATIONS COMMISSION - FCC. [Caller ID Spoofing](#).

⁹⁷ FEDERAL COMMUNICATIONS COMMISSION - FCC. [Cell Phone Fraud](#).

⁹⁸ FEDERAL COMMUNICATIONS COMMISSION - FCC. [IP Relay Fraud](#).

⁹⁹ FEDERAL COMMUNICATIONS COMMISSION - FCC. [Mexico Collect Call Scam](#).

¹⁰⁰ FEDERAL COMMUNICATIONS COMMISSION - FCC. ['One Ring' Phone Scam](#).

¹⁰¹ FEDERAL COMMUNICATIONS COMMISSION - FCC. [Stop Unwanted Robocalls and Texts](#).

¹⁰² FEDERAL COMMUNICATIONS COMMISSION - FCC. [Slamming: Switching Your Authorized Telephone Company Without Permission](#).

¹⁰³ FEDERAL COMMUNICATIONS COMMISSION - FCC. [Voicemail System Hacking](#).

¹⁰⁴ FEDERAL COMMUNICATIONS COMMISSION - FCC. [Bogus COVID-19 Tests and Pharmacy Offers](#). [Coronavirus Scams - Consumer Resources](#). [Coronavirus Scams Targeting Older Americans](#). [COVID-19 Robocall Scams](#). [COVID-19 Text Scams](#). [Fear Fuels COVID-19 Contact Tracing Scams](#).

¹⁰⁵ FEDERAL COMMUNICATIONS COMMISSION - FCC. [Don't Fall for the 90# Telephone Scam](#).

¹⁰⁶ FEDERAL COMMUNICATIONS COMMISSION - FCC. [Caller ID Spoofing](#). [Don't Fall for the 90# Telephone Scam](#).

fizer, desligar imediatamente¹⁰⁷; não responder a mensagens de número desconhecidos¹⁰⁸; verificar se o código de área na verdade é um código internacional antes de ligar para números desconhecidos¹⁰⁹; bloquear a realização de chamadas internacionais junto à sua prestadora se você não tem o hábito de realizar essas ligações¹¹⁰; não responder a perguntas em ligações, especialmente as que possam ser respondidas com sim/não¹¹¹; não fornecer informações pessoais e financeiras¹¹²; alterar senhas padrão de caixas postais¹¹³; somente doar para instituições de caridade confiáveis e conhecidas, bem como verificar os números de contato e sites dessas instituições¹¹⁴; não abrir e-mails suspeitos¹¹⁵; checar posts em redes sociais¹¹⁶; suspeitar de ofertas que solicitem informações médicas ou de seguro saúde¹¹⁷ e verificar a disponibilidade de apps ou serviços de prestadoras para bloqueio de chamadas¹¹⁸.

Ademais, o órgão americano também indica que os consumidores devem, em caso de suspeitarem de golpe/fraude ou serem vítimas, informar à prestadora de serviços¹¹⁹, denunciar suspeitas de fraudes relacionadas a desastres naturais à Agência Federal de Gestão de Emergências (Federal Emergency Management Agency - FEMA)¹²⁰, registrar um alerta de fraude junto a um dos três maiores birôs de crédito do país¹²¹, entrar em contato com a polícia local¹²² ou estadual¹²³, registrar reclamações sobre golpes telefônicos na FCC¹²⁴, denunciar crimes na internet ao Birô Federal de Investigação (Federal Bureau of Investigation - FBI)¹²⁵, bem como reportar fraudes¹²⁶ e roubo de identidade à FTC¹²⁷.

¹⁰⁷ FEDERAL COMMUNICATIONS COMMISSION - FCC. [Bogus COVID-19 Tests and Pharmacy Offers](#). [Caller ID Spoofing](#). [Coronavirus Scams - Consumer Resources](#). [Coronavirus Scams Targeting Older Americans](#). [COVID-19 Robocall Scams](#). [Fear Fuels COVID-19 Contact Tracing Scams](#). [COVID-19 Text Scams](#). ['One Ring' Phone Scam](#).

¹⁰⁸ FEDERAL COMMUNICATIONS COMMISSION - FCC. [Coronavirus Scams - Consumer Resources](#).

¹⁰⁹ FEDERAL COMMUNICATIONS COMMISSION - FCC. ['One Ring' Phone Scam](#).

¹¹⁰ FEDERAL COMMUNICATIONS COMMISSION - FCC. ['One Ring' Phone Scam](#). [Voicemail System Hacking](#).

¹¹¹ FEDERAL COMMUNICATIONS COMMISSION - FCC. [Caller ID Spoofing](#).

¹¹² FEDERAL COMMUNICATIONS COMMISSION - FCC. [Bogus COVID-19 Tests and Pharmacy Offers](#). [Caller ID Spoofing](#). [Coronavirus Scams - Consumer Resources](#). [Coronavirus Scams Targeting Older Americans](#). [COVID-19 Robocall Scams](#). [Fear Fuels COVID-19 Contact Tracing Scams](#). [Watch out for Auto Warranty Scams](#).

¹¹³ FEDERAL COMMUNICATIONS COMMISSION - FCC. [Caller ID Spoofing](#). [Coronavirus Scams - Consumer Resources](#). [Voicemail System Hacking](#).

¹¹⁴ FEDERAL COMMUNICATIONS COMMISSION - FCC. [After Storms, Watch Out for Scams](#). [Coronavirus Scams Targeting Older Americans](#). [COVID-19 Robocall Scams](#). [COVID-19 Text Scams](#).

¹¹⁵ FEDERAL COMMUNICATIONS COMMISSION - FCC. [After Storms, Watch Out for Scams](#).

¹¹⁶ FEDERAL COMMUNICATIONS COMMISSION - FCC. [After Storms, Watch Out for Scams](#).

¹¹⁷ FEDERAL COMMUNICATIONS COMMISSION - FCC. [Bogus COVID-19 Tests and Pharmacy Offers](#).

¹¹⁸ FEDERAL COMMUNICATIONS COMMISSION - FCC. [Caller ID Spoofing](#).

¹¹⁹ FEDERAL COMMUNICATIONS COMMISSION - FCC. [Caller ID Spoofing](#). [Cell Phone Fraud](#). [Don't Fall for the 90# Telephone Scam](#).

¹²⁰ FEDERAL COMMUNICATIONS COMMISSION - FCC. [After Storms, Watch Out for Scams](#).

¹²¹ FEDERAL COMMUNICATIONS COMMISSION - FCC. [Cell Phone Fraud](#).

¹²² FEDERAL COMMUNICATIONS COMMISSION - FCC. [Cell Phone Fraud](#). [Don't Fall for the 90# Telephone Scam](#).

¹²³ FEDERAL COMMUNICATIONS COMMISSION - FCC. [IP Relay Fraud](#).

¹²⁴ FEDERAL COMMUNICATIONS COMMISSION - FCC. [After Storms, Watch Out for Scams](#). [Mexico Collect Call Scam](#). [Slamming: Switching Your Authorized Telephone Company Without Permission](#). [Watch out for Auto Warranty Scams](#).

¹²⁵ FEDERAL COMMUNICATIONS COMMISSION - FCC. [IP Relay Fraud](#).

¹²⁶ FEDERAL COMMUNICATIONS COMMISSION - FCC. [After Storms, Watch Out for Scams](#). [IP Relay Fraud](#). [Mexico Collect Call Scam](#). [Watch out for Auto Warranty Scams](#).

¹²⁷ FEDERAL COMMUNICATIONS COMMISSION - FCC. [Cell Phone Fraud](#).

Em especial, no que tange a ligações e mensagens automatizadas não autorizadas, a FCC indica que tem feito ações de *enforcement* resultando em multas de milhões de dólares contra *robocallers* ilegais; fornecido opções de ferramentas de bloqueio de chamadas aos consumidores; demandado, de prestadoras, a implantação de mecanismos de identificação de chamadas para reduzir práticas ilegais de *spoofing*; possibilitado, às prestadoras, com base em análise de dados aplicada às ligações, bloqueio de chamadas não solicitadas ou ilegais por padrão e disponibilizado dados de reclamações com vistas a possibilitar melhores soluções de identificação e bloqueio de chamadas.¹²⁸

Além das ligações de *telemarketing* não autorizadas, muitas ligações automatizadas são ilegais e a tecnologia faz com que essas ligações sejam cada vez mais fáceis e baratas de serem realizadas, e, conseqüentemente, mais difíceis de identificar, reduzir e bloquear¹²⁹. Ademais, segundo a FCC, “chamadas indesejadas [...] são a principal reclamação dos consumidores e a principal prioridade da Agência na proteção ao consumidor”.¹³⁰

1.2. Federal Trade Commission - FTC

No intuito de informar e manter atualizadas as informações sobre os golpes existentes, principalmente os novos, a FTC mantém página específica de alerta para golpes em seu *site* dedicado aos consumidores. Desse modo, de forma cronológica, do mais recente para o mais antigo, a FTC apresenta, ao longo de 34 páginas, título com indicação do golpe, acrescido de um breve texto descrevendo-o. De fato, cada um dos títulos é um *link* que direciona para página com informações mais detalhadas e, em geral, explicando como os esquemas funcionam e informando aos consumidores o que pode ser feito.¹³¹

Entre os golpes listados pela FTC¹³² pode-se destacar golpes solicitando doações após desastres¹³³, *catfishing* (nas variações de golpe do romance¹³⁴ e golpe da caridade¹³⁵), golpes de loterias e prêmios¹³⁶, golpes de cartões de presente¹³⁷, mula de dinheiro¹³⁸, golpes de

¹²⁸ FEDERAL COMMUNICATIONS COMMISSION - FCC. [Stop Unwanted Robocalls and Texts](#).

¹²⁹ FEDERAL COMMUNICATIONS COMMISSION - FCC. [Stop Unwanted Robocalls and Texts - Robocalls](#).

¹³⁰ Tradução nossa. No original: “Unwanted calls - including illegal and spoofed robocalls - are the FCC’s top consumer complaint and our top consumer protection priority”. FEDERAL COMMUNICATIONS COMMISSION - FCC. [Stop Unwanted Robocalls and Texts](#).

¹³¹ Tendo em vista que essa lista é crescente, foram computadas 34 páginas na data de 16/09/2020. FEDERAL TRADE COMMISSION - FTC. Consumer information. [Scams](#).

¹³² Vários dos golpes tratados pela FTC foram abordados anteriormente na seção sobre golpes e fraudes nos Estados Unidos no [Estudo - Golpes e fraudes contra o consumidor de telecom - Parte 1 - Identificação de casos na Europa, Estados Unidos e Brasil](#), p. 7-16.

¹³³ FEDERAL TRADE COMMISSION - FTC. [Dealing with Weather Emergencies](#). [Scammers prey on your kindness during disasters](#). [Tips to help you avoid post-disaster scams](#).

¹³⁴ FEDERAL TRADE COMMISSION - FTC. [It’s not true love if they ask for money](#). [Online Dating Scams Infographic](#).

¹³⁵ FEDERAL TRADE COMMISSION - FTC. [Donating in difficult times](#).

¹³⁶ FEDERAL TRADE COMMISSION - FTC. [“You’ve won! Now pay us” is always a scam](#).

¹³⁷ FEDERAL TRADE COMMISSION - FTC. [Did someone tell you to pay with gift cards? It’s a scam](#). [Paying Scammers with Gift Cards](#).

¹³⁸ FEDERAL TRADE COMMISSION - FTC. [Money Mule Scams Infographic](#). [What’s a money mule scam?](#).

criptomoedas¹³⁹, golpes da Receita Federal ou impostos¹⁴⁰ e golpes relativos à pandemia do novo coronavírus¹⁴¹.

Além de caracterizar os golpes, a FTC indica como evitá-los, podendo-se destacar as seguintes atitudes a serem tomadas pelos consumidores para que não sejam vítimas: identifique impostores (pessoas se passando por representantes de instituições/órgãos governamentais) que tentam induzir as vítimas a enviarem valores ou fornecerem informações pessoais¹⁴²; após desastres, fique alerta a ofertas de emprego¹⁴³, ofertas de aluguel¹⁴⁴ e serviços de limpeza e reparo¹⁴⁵; atente-se a solicitações de doações após desastres, especialmente se houver uma pressão para a realização da doação de forma rápida¹⁴⁶; duvide de anúncios de instituições de caridade na internet, em especial em mídias sociais¹⁴⁷; pesquise sobre a instituição antes de realizar doações¹⁴⁸; nunca faça pagamentos por transferência, dinheiro, cartões de presente¹⁴⁹ ou criptomoedas¹⁵⁰; não forneça informações pessoais¹⁵¹; não realize envio de valores a pretensas ofertas de emprego¹⁵²; habilite atualizações automáticas para seus dispositivos e sistemas operacionais¹⁵³; não realize pagamento de impostos, taxas ou despesas de manuseio e envio para

¹³⁹ FEDERAL TRADE COMMISSION - FTC. [Avoiding a cryptocurrency scam](#). [Cryptocurrency blackmail scam alert](#). [Scam emails demand Bitcoin, threaten blackmail](#).

¹⁴⁰ FEDERAL TRADE COMMISSION - FTC. [IRS Imposter Scams Infographic](#).

¹⁴¹ FEDERAL TRADE COMMISSION - FTC. [Contact Tracing Infographic](#). [Coronavirus checks: flattening the scam curve](#). [Coronavirus: Scammers follow the headlines](#). [Coronavirus stimulus payment scams: What you need to know](#). [COVID-19 contact tracing text message scams](#). [COVID-19 scam reports, by the numbers](#). [Did an ID thief steal your stimulus payment? Report it to us](#). [Economic impact payments for U.S. citizens abroad](#). [Fake emails about fake money from a fake COVID-19 fund](#). [Finding a furry friend in the era of COVID-19](#). [FTC: Coronavirus scams, Part 2](#). [FTC & FDA: Warnings sent to sellers of scam Coronavirus treatments](#). [FTC: Sellers need proof for COVID treatment claims](#). [FTC sends more warnings to sellers of scam Coronavirus treatments](#). [FTC warns 45 more sellers of scam Coronavirus treatments](#). [Help COVID-19 contact tracers, not scammers](#). [More FTC warnings about scam Coronavirus treatments](#). [Is a scammer getting unemployment benefits in your name?](#). [Not every COVID-19 testing site is legit](#). [Scammers offer facemasks but don't deliver](#). [Small businesses: Where to go for financial relief information](#). [Steer clear of work-at-home scams](#). [The IRS won't call about your stimulus money](#). [Want to get your Coronavirus relief check? Scammers do too](#).

¹⁴² FEDERAL TRADE COMMISSION - FTC. [Contact Tracing Infographic](#). [Dealing with Weather Emergencies](#). [Fake emails about fake money from a fake COVID-19 fund](#). [FTC: Coronavirus scams, Part 2](#). [Help COVID-19 contact tracers, not scammers](#). [How to avoid COVID-19 government imposter scams](#). [The IRS won't call about your stimulus money](#).

¹⁴³ FEDERAL TRADE COMMISSION - FTC. [Dealing with Weather Emergencies](#).

¹⁴⁴ FEDERAL TRADE COMMISSION - FTC. [Dealing with Weather Emergencies](#). [Tips to help you avoid post-disaster scams](#).

¹⁴⁵ FEDERAL TRADE COMMISSION - FTC. [Dealing with Weather Emergencies](#). [Tips to help you avoid post-disaster scams](#).

¹⁴⁶ FEDERAL TRADE COMMISSION - FTC. [Dealing with Weather Emergencies](#). [Donating in difficult times](#). [Scammers prey on your kindness during disasters](#). [Tips to help you avoid post-disaster scams](#).

¹⁴⁷ FEDERAL TRADE COMMISSION - FTC. [Scammers prey on your kindness during disasters](#).

¹⁴⁸ FEDERAL TRADE COMMISSION - FTC. [Donating in difficult times](#). [Scammers prey on your kindness during disasters](#).

¹⁴⁹ FEDERAL TRADE COMMISSION - FTC. [Contact Tracing Infographic](#). [Donating in difficult times](#). [It's not true love if they ask for money](#). [Money Mule Scams Infographic](#). [Online Dating Scams Infographic](#). [Scam emails demand Bitcoin, threaten blackmail](#). [Tips to help you avoid post-disaster scams](#).

¹⁵⁰ FEDERAL TRADE COMMISSION - FTC. [Contact Tracing Infographic](#). [Avoiding a cryptocurrency scam](#). [Cryptocurrency blackmail scam alert](#).

¹⁵¹ FEDERAL TRADE COMMISSION - FTC. [Contact Tracing Infographic](#). [Economic impact payments for U.S. citizens abroad](#). [FTC: Coronavirus scams, Part 2](#). [Help COVID-19 contact tracers, not scammers](#). [IRS Imposter Scams Infographic](#). [Tips to help you avoid post-disaster scams](#). [Want to get your Coronavirus relief check? Scammers do too](#).

¹⁵² FEDERAL TRADE COMMISSION - FTC. [Money Mule Scams Infographic](#).

¹⁵³ FEDERAL TRADE COMMISSION - FTC. [COVID-19 contact tracing text message scams](#).

receber prêmios¹⁵⁴; utilize autenticação em mais de uma etapa em suas contas *on-line*¹⁵⁵, bem como proteja sua identidade, esteja atento a sinais de que sua identidade foi roubada¹⁵⁶ e realize reporte de roubo de identidade¹⁵⁷.

Ademais, a FTC também preconiza que os consumidores registrem reclamação perante órgãos governamentais¹⁵⁸ e perante a própria FTC¹⁵⁹. Em especial, no caso de roubo de identidade, a agência recomenda, para realização de registro e obtenção de informações para a recuperação após se tornar vítima, a visita ao *hotsite* federal <https://www.identitytheft.gov>¹⁶⁰, que concentra esclarecimentos a vítimas desse crime específico¹⁶¹.

1.3. AT&T

A AT&T possui página específica para informar sobre golpes e fraudes. Denominada “Cyber Aware”, a página apresenta *links* para as seções “Blogs”, “Awareness”, “Alerts”, “Resources” e “Search”.¹⁶²

A seção “Search” permite realizar procura na página “Cyber Aware”, enquanto a seção “Resources”¹⁶³ traz recursos para ajudar o consumidor a alertar um birô de crédito/reportar fraude (*Alerting the Credit Bureau*)¹⁶⁴, a aderir à lista nacional de Não perturbe (*Do Not Call List*)¹⁶⁵, a compartilhar uma experiência (*Submit an Experience*)¹⁶⁶, sobre conexões de cibersegurança (*Cybersecurity Connections*)¹⁶⁷, sobre termos e definições (*Terms & Definitions*)¹⁶⁸ e, por fim, sobre dicas e informações (*Tips & Information*)¹⁶⁹.

¹⁵⁴ FEDERAL TRADE COMMISSION - FTC. [“You’ve won! Now pay us” is always a scam.](#)

¹⁵⁵ FEDERAL TRADE COMMISSION - FTC. [COVID-19 contact tracing text message scams.](#)

¹⁵⁶ FEDERAL TRADE COMMISSION - FTC. [Did an ID thief steal your stimulus payment? Report it to us. Identity Theft. Is a scammer getting unemployment benefits in your name?](#)

¹⁵⁷ FEDERAL TRADE COMMISSION - FTC. [Identity Theft.](#)

¹⁵⁸ FEDERAL TRADE COMMISSION - FTC. [Cryptocurrency blackmail scam alert. Finding a furry friend in the era of COVID-19. Help COVID-19 contact tracers, not scammers. IRS Imposter Scams Infographic. Is a scammer getting unemployment benefits in your name? Paying Scammers with Gift Cards.](#)

¹⁵⁹ FEDERAL TRADE COMMISSION - FTC. [Contact Tracing Infographic. COVID-19 contact tracing text message scams. Cryptocurrency blackmail scam alert. Dealing with Weather Emergencies. Did someone tell you to pay with gift cards? It’s a scam. Economic impact payments for U.S. citizens abroad. Fake emails about fake money from a fake COVID-19 fund. Finding a furry friend in the era of COVID-19. FTC: Coronavirus scams, Part 2. Help COVID-19 contact tracers, not scammers. It’s not true love if they ask for money. Money Mule Scams Infographic. Online Dating Scams Infographic. Paying Scammers with Gift Cards. Scam emails demand Bitcoin, threaten blackmail. Scammers prey on your kindness during disasters. Tips to help you avoid post-disaster scams. “You’ve won! Now pay us” is always a scam.](#)

¹⁶⁰ FEDERAL TRADE COMMISSION - FTC. [Did an ID thief steal your stimulus payment? Report it to us. Identity Theft. Is a scammer getting unemployment benefits in your name?](#)

¹⁶¹ FEDERAL TRADE COMMISSION - FTC. [IdentityTheft.gov.](#)

¹⁶² AT&T. [Cyber Aware.](#)

¹⁶³ AT&T. [Cyber Aware - Resources.](#)

¹⁶⁴ AT&T. [Cyber Aware - Resources - Fraud Alert Reporting/Credit Bureau Contact Information.](#)

¹⁶⁵ AT&T. [Cyber Aware - Resources - Do Not Call List.](#)

¹⁶⁶ AT&T. [Cyber Aware - Resources - Submit an Experience.](#)

¹⁶⁷ AT&T. [Cyber Aware - Resources - Cybersecurity Connections.](#)

¹⁶⁸ AT&T. [Cyber Aware - Key Terms & Definitions.](#)

¹⁶⁹ AT&T. [Cyber Aware - Awareness & Education - Help and consumer education.](#)

Na seção “Blogs” são dispostos *links* para *blogs* com temas específicos e alguns *blogs* em destaque com uma breve descrição sobre o tema a ser tratado¹⁷⁰. São os destaques:

- Não seja preguiçoso com sua segurança (*Don't Get Lazy with Your Security*): dicas de segurança que ignoramos;¹⁷¹
- Reduza os riscos cibernéticos quando você retornar ao escritório (*Reduce Cyber Risks When You Return to the Office*): dicas atuais para quem está em quarentena e vai voltar ao trabalho presencial;¹⁷²
- Dicas para que o trabalho em casa seja produtivo (*Tips to Make Working from Home Productive*): dicas para quem está trabalhando em casa;¹⁷³
- Dicas para proteger seus *chats* de vídeo (*Tips to Secure Your Video Chats*): dicas de segurança para usar os *chats* de vídeo;¹⁷⁴
- O que você precisa saber sobre golpes de troca de cartão SIM (*What You Need to Know About SIM Swap Scams*): informações sobre golpes de troca de cartão SIM;¹⁷⁵ e
- Proteja-se contra golpes de porta-a-porta (*Protect Yourself from Door-to-Door Sales Scams*): proteção contra golpes de vendas presenciais.¹⁷⁶

Além dos *blogs* em destaque a página traz também o *link* para 50 *blogs*¹⁷⁷, entre os quais se pode sublinhar alguns:

- Segurança de aplicativos (*App Security*): segurança de *apps* para *smartphones*, incluindo indicações para a não instalação de *apps* de fontes desconhecidas, instalação de um aplicativo de segurança e checagem de notificações de atualização;¹⁷⁸
- Melhores práticas (*Best Practices*): melhores práticas e recomendações em cibersegurança, incluindo questões como senhas, proteção de computadores e dispositivos, bem como configurações de privacidade e segurança em redes sociais;¹⁷⁹
- *Catfishing* - dicas para não ser vítima do golpe de *catfishing*, incluindo variações relacionadas a doações, encontros amorosos e ganhos monetários de forma fácil;¹⁸⁰
- Roubo de identidade de criança (*Child ID Theft*): dicas para evitar o roubo de identidade de crianças;¹⁸¹

¹⁷⁰ AT&T. [Cyber Aware - Cyber Aware Blogs](#).

¹⁷¹ AT&T. [Cyber Aware - Don't Get Lazy with Your Security](#).

¹⁷² AT&T. [Cyber Aware - Reduce Cyber Risks When You Return to the Office](#).

¹⁷³ AT&T. [Cyber Aware - Tips to Make Working from Home Productive](#).

¹⁷⁴ AT&T. [Cyber Aware - Tips to Secure Your Video Chats](#).

¹⁷⁵ AT&T. [Cyber Aware - What You Need to Know About SIM Swap Scams](#).

¹⁷⁶ AT&T. [Cyber Aware - Protect Yourself from Door-to-Door Sales Scams](#).

¹⁷⁷ AT&T. [Cyber Aware - Cyber Aware Blogs](#).

¹⁷⁸ AT&T. [Cyber Aware - Don't Let One Bad App Spoil the Whole Phone](#).

¹⁷⁹ AT&T. [Cyber Aware - Cybersecurity Best Practices and Recommendations](#).

¹⁸⁰ AT&T. [Cyber Aware - Stop Catfishing Before They Reel You In](#).

¹⁸¹ AT&T. [Cyber Aware - Identity Theft: Don't Let Bad Guys Steal Digital Candy from Your Baby](#).

- Golpes do coronavírus (*Coronavirus Scams*): alertas sobre golpes relacionados ao novo coronavírus;¹⁸²
- Fraude: alerta para o golpe do intermediário, indicando como funciona e o que fazer;¹⁸³
- Golpes de compras de final de ano (*Holiday Scams*): alertas sobre golpes com foco nas compras do período de final de ano;¹⁸⁴
- Golpes da Receita Federal ou impostos (*IRS/Tax Scams*): alertas sobre golpes fiscais e tributários;¹⁸⁵
- Dicas para a segurança de crianças (*Kid Security Tips*): dicas de segurança *on-line* para crianças;¹⁸⁶
- Golpes de loteria (*Lottery Scams*): alertas sobre golpes de loteria e prêmios;¹⁸⁷
- Golpe da ligação de um toque (*One-Ring Call Scams*): explicação sobre o golpe e o que fazer em caso de se tornar vítima;¹⁸⁸
- Dicas de segurança de senhas (*Password Security Tips*): dicas e recomendações para a criação de senhas fortes, incluindo a adoção de senhas no formato de frases aleatórias;¹⁸⁹
- *Phishing*: caracterização do golpe, dados sobre sua incidência e dicas para detectar esse tipo de golpe;¹⁹⁰
- Proteção de número de telefone (*Phone Number Safety*): cuidados ao compartilhar seu número de telefone;¹⁹¹
- Vídeo de *robocall* (*Robocall Video*): informações e dicas para se proteger de ligações automatizadas realizadas por robôs (*robocalls*);¹⁹²
- Golpes de troca de cartão SIM (*SIM Swap Scams*): informações sobre o golpe de troca do cartão SIM, incluindo sua caracterização, as iniciativas da prestadora para coibir esse golpe e o que o consumidor pode fazer;¹⁹³
- Golpes de mídias sociais (*Social Media Scams*): informações sobre golpes envolvendo doações em redes sociais;¹⁹⁴
- Informação sobre *spoofing* (*Spoofing Information*): explicação do golpe e dicas para se proteger;¹⁹⁵

¹⁸² AT&T. [Cyber Aware - Alerts & Reporting - Coronavirus Scam](#).

¹⁸³ Blog em espanhol. AT&T. [Cyber Aware - Alerts & Reporting - Fraude de Intermediario](#).

¹⁸⁴ AT&T. [Cyber Aware - Alerts & Reporting - Beware of Holiday Scams](#).

¹⁸⁵ AT&T. [Cyber Aware - Alerts & Reporting - IRS/Tax Scams and Similar Government Agency Scams Alert](#).

¹⁸⁶ AT&T. [Cyber Aware - For Online Safety, Keeping Up with the Kids Means Keeping Up with the Times](#).

¹⁸⁷ AT&T. [Cyber Aware - Alerts & Reporting - Lottery & Prize Scams](#).

¹⁸⁸ AT&T. [Cyber Aware - Alerts & Reporting - One-Ring Call Scams](#).

¹⁸⁹ AT&T. [Cyber Aware - Make Your p@\\$w0rDs Stronger](#).

¹⁹⁰ AT&T. [Cyber Aware - Phishing: Know Bait When You See It](#).

¹⁹¹ AT&T. [Cyber Aware - Protect Your Phone Number and Protect Your Identity](#).

¹⁹² AT&T. [Cyber Aware - 3 Things You Need to Know about Robocalls](#).

¹⁹³ AT&T. [Cyber Aware - What You Need to Know About SIM Swap Scams](#).

¹⁹⁴ AT&T. [Cyber Aware - Alerts & Reporting - Social Media Charity Scam](#).

¹⁹⁵ AT&T. [Cyber Aware - Caller ID Spoofing & What To Do About It](#).

- Autenticação em duas etapas (*Two-Factor Authentication*): recomendação da adoção de autenticação em duas etapas para proteção de contas *on-line*;¹⁹⁶ e
- Segurança de wi-fi (*Wi-Fi Security*): como se proteger ao acessar pontos públicos de wi-fi.¹⁹⁷

A seção “Awareness” fala sobre a importância de conhecer e estar alerta aos golpes e fraudes existentes. Além de um *banner* em destaque no começo da página sobre cinco dicas para evitar fraudes e aumentar a segurança¹⁹⁸; uma lista de programas e produtos da prestadora; informações sobre combate a fraudes em tempo real¹⁹⁹, bloqueio de *robocalls*²⁰⁰, relatório de anomalias²⁰¹ e análise de dados²⁰²; a página também traz uma lista de preocupações de segurança comuns, quais sejam:²⁰³

- Fraudes e golpes (*Frauds & scams*): lista fraudes e golpes bem conhecidos e como reportá-los;²⁰⁴
- *E-mails* falsos ou *phishing* (*Fake e-mail or phishing*): apresenta um panorama sobre esse tipo de golpe, como identificá-lo e como se proteger;²⁰⁵
- *SMiShing*: informa sobre golpes usando mensagens de texto;²⁰⁶
- Roubo de identidade (*ID theft*): aponta como se proteger do roubo de identidade e como reportar;²⁰⁷
- Engenharia social (*Social engineering*): dicas para se proteger desse golpe em que alguém se passando por um terceiro, tenta obter informações pessoais do usuário, bem como indicação de como reportar essa ocorrência;²⁰⁸
- *Robocalls* e ligações indesejadas (*Robocalls & unwanted calls*): informações sobre as chamadas automáticas, quando essas se configuram como golpe, como se proteger e o compromisso da prestadora em proteger os consumidores;²⁰⁹
- *Spam*: dicas para detectar e se proteger do *spam* em suas várias formas (*e-mail*, SMS e MMS);²¹⁰

¹⁹⁶ AT&T. [Cyber Aware - Better Protect Your Online Accounts with “Two-Factor Authentication”](#).

¹⁹⁷ AT&T. [Cyber Aware - Stay Private in Public: Be Wary About Wi-Fi](#).

¹⁹⁸ Esse *banner* leva à subseção *Tips & Information* da seção *Resources*, já abordada anteriormente. AT&T. [Cyber Aware - Awareness & Education - Help and consumer education](#).

¹⁹⁹ AT&T. [Cyber Aware - Real-Time Fraud Fighting](#).

²⁰⁰ AT&T. [Cyber Aware - News & Information Robocall Blocking](#).

²⁰¹ AT&T. [Cyber Aware - Awareness & Education - Anomaly Reporting](#).

²⁰² AT&T. [Cyber Aware - News & Information - Data Analytics](#).

²⁰³ AT&T. [Cyber Aware - Awareness & Education](#).

²⁰⁴ AT&T. [Cyber Aware - Awareness & Education - Fraud and scams](#).

²⁰⁵ AT&T. [Cyber Aware - Awareness & Education - Fake Email or “Phishing”](#).

²⁰⁶ AT&T. [Cyber Aware - Awareness & Education - Fake Text Messages, SMiShing and Other Text Scams](#).

²⁰⁷ AT&T. [Cyber Aware - Awareness & Education - Identity Theft](#).

²⁰⁸ AT&T. [Cyber Aware - Awareness & Education - Social engineering](#).

²⁰⁹ AT&T. [Cyber Aware - Awareness & Education - Robocalls and Unwanted calls](#).

²¹⁰ AT&T. [Cyber Aware - Awareness & Education - Spam](#).

- *Malware*: dicas para proteção contra os vários tipos de *software* malicioso, como vírus e programas espiões;²¹¹ e
- Cibersegurança para empresas (*Cybersecurity for business*): informações para fortalecer a cibersegurança de empresas.²¹²

Por fim, a seção “Alerts” é dedicada aos últimos alertas. No momento desta análise cinco tipos de golpe eram identificados nessa seção:

- Golpes de engenharia social (*Social Engineering Scams*): indicação de como funcionam golpes de engenharia social, porque funcionam e o que se pode fazer para evitá-los;²¹³
- Golpes sobre o coronavírus (*Coronavirus Scams*): golpes em que golpistas se aproveitam da pandemia do novo coronavírus para tentar tirar vantagem das pessoas;²¹⁴
- Fraudes de Número de Identificação Pessoal (*PIN Fraud Scams*): golpes envolvendo PINs (*Personal Identification Number*) e como evitá-los;²¹⁵
- Golpe do cartão pré-pago (*Prepaid Card Scam*): golpes envolvendo pagamentos por meio de cartões pré-pagos;²¹⁶ e
- Golpe “responda a uma pesquisa” (*“Take a Survey” Scam*): golpe que induz o usuário a responder a uma pretensa pesquisa para que ganhe um prêmio.²¹⁷

3. INICIATIVAS NO BRASIL

Na realidade nacional também há inúmeras iniciativas para preservar os consumidores dos serviços de telecomunicações e o público em geral. O Serasa possui um serviço de educação ao consumidor²¹⁸; o Fundo das Nações Unidas para a Infância (Unicef) no Brasil possui a iniciativa *Internet sem vacilo*²¹⁹; a Rede Nacional de Ensino e Pesquisa (RNP) possui materiais educativos sobre conscientização em segurança²²⁰ e um catálogo crescente de fraudes²²¹; a SaferNet Brasil²²²

²¹¹ AT&T. [Cyber Aware - Awareness & Education - Malware](#).

²¹² AT&T. [Cyber Aware - Awareness & Education - Cybersecurity for businesses](#).

²¹³ AT&T. [Cyber Aware - Alerts & Reporting - Social Engineering Scam](#).

²¹⁴ AT&T. [Cyber Aware - Alerts & Reporting - Coronavirus Scam](#).

²¹⁵ AT&T. [Cyber Aware - Alerts & Reporting - Prevent PIN Fraud Scams](#).

²¹⁶ AT&T. [Cyber Aware - Alerts & Reporting - Prepaid Card Scam](#).

²¹⁷ AT&T. [Cyber Aware - Alerts & Reporting - “Take a Survey” Scam](#).

²¹⁸ SERASA. [Serasa ensina](#).

²¹⁹ FUNDO DAS NAÇÕES UNIDAS PARA A INFÂNCIA - UNICEF. [Internet sem vacilo](#).

²²⁰ REDE NACIONAL DE ENSINO E PESQUISA - RNP. [Conscientização em segurança](#).

²²¹ Na data de 19/10/2020, o catálogo possuía 1.628 páginas. REDE NACIONAL DE ENSINO E PESQUISA - RNP. [Catálogo de fraudes](#).

²²² A SaferNet Brasil “é uma associação civil de direito privado, com atuação nacional, sem fins lucrativos ou econômicos, sem vinculação político partidária, religiosa ou racial [...] com foco na promoção e defesa dos Direitos Humanos na Internet no Brasil”. SAFERNET BRASIL. [Institucional](#). A organização também conta com a cooperação, entre outros, da Procuradoria Federal dos Direitos do Cidadão (PFDC) do Ministério Público Federal (MPF), do Conselho Nacional dos Procuradores-Gerais de Justiça dos Ministérios Públicos dos Estados e da União (CNPJ), da Unicef, da Secretaria de Direitos Humanos do Ministério da Mulher, da Família e dos Direitos Humanos e do Comitê Gestor da Internet no Brasil

apresenta informações, entre outras, sobre segurança digital²²³ e privacidade²²⁴; o Instituto Brasileiro de Defesa do Consumidor (Idec)²²⁵ apresenta conteúdos sobre golpes e fraudes²²⁶; bem como o Observatore²²⁷ possui cartilha antifraudes para consumidores²²⁸ e lojistas²²⁹. Ademais, há também iniciativas dos Procons²³⁰, Ministérios Públicos²³¹, Polícia Federal (PF)²³² e departamentos de polícias e Secretarias de Segurança Pública ao redor do país²³³, bem como da Secretaria Nacional do Consumidor (Senacon) do Ministério da Justiça e Segurança Pública (MJSP)²³⁴.

(CGI.br), bem como mantém parceria em projetos com o Google, o Facebook, a Vivo e o Núcleo de Informação e Coordenação do Ponto BR (NIC.BR). SAFERNET BRASIL. [Safernet](#).

²²³ SAFERNET BRASIL. [Segurança digital](#).

²²⁴ SAFERNET BRASIL. [Privacidade](#).

²²⁵ O Instituto Brasileiro de Defesa do Consumidor (Idec) “é uma associação de consumidores sem fins lucrativos, independente de empresas, partidos ou governos”. INSTITUTO BRASILEIRO DE DEFESA DO CONSUMIDOR - IDEC. [Quem Somos](#).

²²⁶ INSTITUTO BRASILEIRO DE DEFESA DO CONSUMIDOR - IDEC. [Coronavírus: fique alerta para não cair em golpes](#), 25/03/2020, 03/07/2020 (última atualização). [Dados pessoais. Golpe do WhatsApp: o que fazer?](#), 04/02/2020, 13/03/2020 (última atualização). [Golpes no WhatsApp: qual o papel das operadoras?](#), 10/10/2017. [Idec orienta consumidores sobre fraudes dos boletos bancários](#), 25/02/2016. [Vai fazer compras pela internet? Veja dicas para fugir do mau negócio](#), 26/11/2015, 21/10/2019 (última atualização). INSTITUTO BRASILEIRO DE DEFESA DO CONSUMIDOR - IDEC. A GAZETA. [Os 10 golpes contra o consumidor que avançam na pandemia](#), 23/06/2020, 01/07/2020 (última atualização). INSTITUTO BRASILEIRO DE DEFESA DO CONSUMIDOR - IDEC. G1. [Golpistas usam Instagram para aplicar fraudes em vendas on-line](#), 24/05/2020. INSTITUTO BRASILEIRO DE DEFESA DO CONSUMIDOR - IDEC. ISTOÉ DINHEIRO. [O que são, como funcionam e como se prevenir das chamadas de robôs](#), 25/10/2018, 16/08/2019 (última atualização). INSTITUTO BRASILEIRO DE DEFESA DO CONSUMIDOR - IDEC. O GLOBO. [Metade dos idosos já se sentiu enganada como cliente, mostra pesquisa](#), 17/12/2018, 16/08/2019 (última atualização). [No Dia Mundial da Internet Segura, confira 5 dicas para proteger seus dados](#), 05/02/2019. [Nova versão do golpe do boleto faz mais vítimas](#), 01/06/2020.

²²⁷ O Observatore é uma rede “de empresas da economia digital habilitada para o compartilhamento de informações-antifraude”. OBSERVATORE. [O Observatore](#).

²²⁸ OBSERVATORE. [Cartilha antifraudes para consumidores online](#).

²²⁹ OBSERVATORE. [Cartilha antifraude para lojistas](#).

²³⁰ GOVERNO DO ESTADO DO PARANÁ. SECRETARIA DA JUSTIÇA, FAMÍLIA E TRABALHO. [Procon-PR orienta consumidor aos golpes de clonagens de cartões e de contas correntes por SMS](#), 04/02/2020. PROCON/DF. [Cartilha do Procon alerta idosos sobre fraudes](#), 26/02/2014, 29/10/2018 (última atualização). [Confira as dicas para não cair no golpe do Auxílio Emergencial](#), 09/04/2020, 16/04/2020 (última atualização). [Dicas para comprar online com segurança](#), 16/04/2020, 12/05/2020 (última atualização). [Números de reclamações de compras online aumenta quase 75% em relação ao ano passado](#), 28/07/2020, 30/07/2020 (última atualização). [Procon-DF alerta consumidores sobre golpe do boleto](#), 10/03/2014, 29/10/2018. PROCON/PR. [Golpes por Mensagem de Celular](#). PROCON/SP. [Aviso ao consumidor](#), 16/04/2020. [Compras pela internet podem esconder golpes](#), 28/05/2020. [Coronavírus e as relações de consumo](#), 15/05/2020. [Dia das Crianças](#), 02/10/2020. [Espaço consumidor. Evite esses Sites. Golpe do Whatsapp](#), 31/08/2020. [Golpe envio de código pelo WhatsApp](#), 19/02/2020. [Golpe na F1](#), 20/08/2020. [Lives falsas](#), 15/05/2020. [Procon-SP alerta para golpes virtuais](#), 08/04/2020. [Site de compras falso](#), 30/09/2020.

²³¹ MINISTÉRIO PÚBLICO DO DISTRITO FEDERAL E TERRITÓRIOS - MPDFT. [MPDFT alerta contra golpes e fraudes virtuais durante a Pandemia](#), 17/04/2020. [Sugestões para o uso seguro do WhatsApp](#), 08/2020. MINISTÉRIO PÚBLICO DO ESTADO DO RIO GRANDE DO SUL - MPRS. [MP de Caxias do Sul lança campanha de alerta aos crimes de estelionato e extorsão](#), 06/12/2019. MINISTÉRIO PÚBLICO DE SANTA CATARINA - MPSC. [Cuidado com os golpes e as fraudes na Internet](#), 01/04/2015.

²³² POLÍCIA FEDERAL. [Ameaças Cibernéticas](#), 07/04/2020, 08/04/2020 (última atualização). [Polícia Federal alerta para ameaças cibernéticas](#), 08/04/2020.

²³³ G1 - PRESIDENTE PRUDENTE E REGIÃO. [Cartilha da Polícia Civil com principais golpes aplicados na região de Presidente Prudente vira aplicativo](#), 04/09/2020. POLÍCIA CIVIL DO DISTRITO FEDERAL. [Golpe do leilão falso pela internet. PCDF alerta para golpe do WhatsApp - Com perda da linha telefônica. PCDF alerta para golpe do WhatsApp - Sem perda da linha telefônica. PCDF alerta para principais golpes praticados contra a comunidade](#). POLÍCIA CIVIL DO ESTADO DO RIO GRANDE DO SUL. [Cuidado com os golpes na internet. Polícia Civil alerta para aumento nos crimes de estelionato: envolvem fraude, engenharia social e má-fé](#). SECRETARIA DE SEGURANÇA PÚBLICA DO ESTADO DO AMAZONAS. [PC alerta população sobre golpe de clonagem de linhas telefônicas em Manaus](#), 10/06/2019.

²³⁴ MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA - MJSP. SECRETARIA NACIONAL DO CONSUMIDOR - SENACON. [Dicas a. Dicas b.](#)

Além dessas iniciativas, há também aquelas da agência reguladora do setor, que é esta Anatel, do Comitê Gestor da Internet no Brasil (CGI.br) e das cinco maiores prestadoras de serviços de telecomunicações do país, que serão aprofundadas nas seções a seguir.

Antes disso cabe referenciar que no Brasil há delegacias especializadas em crimes cibernéticos em Aracaju/SE, Belém/PA, Belo Horizonte/MG, Brasília/DF, Cuiabá/MT, Curitiba/PR, Goiânia/GO, Palmas/TO, Porto Alegre/RS, Recife/PE, Rio de Janeiro/RJ, Salvador/BA, São Luiz/MA, São Paulo/SP, Teresina/PI e Vitória/ES²³⁵, bem como uma Divisão de Repressão a Crimes Cibernéticos na Polícia Federal (PF)²³⁶. Em termos de atribuição, nota enviada pela PF, em resposta a questionamentos da reportagem do UOL em 2018, indica que “sua função primordial é ‘apurar crimes cometidos contra bens, serviços e interesses da União’ e que o fato de um crime ser cometido pela internet não altera a atribuição investigativa dele, que normalmente caberá aos Estados”²³⁷. Ademais, a advogada Gisele Truzzi, especialista em direito digital, também ouvida pelo UOL na mesma reportagem, informa que um crime eletrônico “nada mais é do que um crime comum realizado em meio eletrônico”²³⁸.

Ademais, de forma geral, o Código de Defesa do Consumidor (CDC) prevê a existência de delegacias especializadas em crimes contra o consumidor nas estruturas policiais brasileiras²³⁹. Nesse sentido, possuem delegacias de proteção/defesa do consumidor o Distrito Federal²⁴⁰ e os estados do Amapá²⁴¹, Amazonas²⁴², Bahia²⁴³, Espírito Santo²⁴⁴, Goiás²⁴⁵, Maranhão²⁴⁶, Mato

²³⁵ SAFERNET BRASIL. [Delegacias Ciber Crimes](#).

²³⁶ POLÍCIA FEDERAL. [Organograma - Unidades Centrais - Com base no Decreto nº 10.365, de 22 de maio de 2020, e Portaria nº 285-MJSP, de 28 de maio de 2020](#).

²³⁷ Aspas do autor. UOL - TILT. [Por que a pessoa que te aplica golpe pelo WhatsApp nunca é presa no Brasil?](#), 05/02/2018.

²³⁸ Aspas do autor. UOL - TILT. [Por que a pessoa que te aplica golpe pelo WhatsApp nunca é presa no Brasil?](#), 05/02/2018.

²³⁹ BRASIL. [Lei nº 8.078, de 11 de setembro de 1990 - Código de Defesa do Consumidor](#), artigo 5º, III.

²⁴⁰ Coordenação de Repressão aos Crimes Contra o Consumidor, a Propriedade Imaterial e a Fraudes - CORF. POLÍCIA CIVIL DO DISTRITO FEDERAL. [Departamento de Polícia Especializada - DPE](#).

²⁴¹ Delegacia de Crimes Contra o Consumidor - DECCON. POLÍCIA CIVIL DO ESTADO DO AMAPÁ. [Unidades Policiais - Especializadas](#).

²⁴² Delegacia Especializada em Crimes contra o Consumidor - Decon. POLÍCIA CIVIL DO ESTADO DO AMAPÁ. [Delegacia do Consumidor convida empresários a conhecer plataforma digital de solução de conflitos](#), 02/04/2020.

²⁴³ Delegacia de Defesa do Consumidor - DECON. POLÍCIA CIVIL DO ESTADO DA BAHIA. [Delegacias Especializadas do Departamento de Crimes Contra o Patrimônio](#).

²⁴⁴ Delegacia Especializada de Defesa do Consumidor - Decon. POLÍCIA CIVIL DO ESTADO DO ESPÍRITO SANTO. [SPE - Divisão Especializada da Região Metropolitana](#).

²⁴⁵ Delegacia Estadual de Repressão a Crimes Contra o Consumidor - DECON. POLÍCIA CIVIL DO ESTADO DE GOIÁS. [Delegacias Especializadas](#).

²⁴⁶ Delegacia do Consumidor - DECON. POLÍCIA CIVIL DO ESTADO DO MARANHÃO. [Telefone das delegacias na capital](#), 04/2020.

Grosso²⁴⁷, Mato Grosso do Sul²⁴⁸, Minas Gerais²⁴⁹, Pará²⁵⁰, Paraíba²⁵¹, Paraná²⁵², Pernambuco²⁵³, Piauí²⁵⁴, Rio de Janeiro²⁵⁵, Rio Grande do Norte²⁵⁶, Rio Grande do Sul²⁵⁷, Rondônia²⁵⁸, Roraima²⁵⁹ e São Paulo^{260, 261}.

1.1. Anatel

A Anatel informa sobre golpes e fraudes em diversos meios eletrônicos, como em seu *site* principal, no seu Portal do Consumidor e em redes sociais como Facebook, Instagram e Twitter. Em especial, por meio da campanha #ConexãoSegura, a Agência informou e divulgou dicas de prevenção e segurança nas redes de forma direta e com elementos visuais para destacar a importância das mensagens.²⁶²

Além disso, a Agência criou em 2005 o Grupo Executivo Antifraude de Telecomunicações (GEAFT), com representantes da Anatel e das prestadoras de telecomunicações, para propor ações de prevenção, diminuição e extinção das práticas fraudulentas no setor.²⁶³

A Agência alerta aos consumidores para não fornecerem dados pessoais e ressalta que não contacta consumidores para oferecer serviços, realizar cobranças, conceder prêmios ou fazer quaisquer testes técnicos de qualidade de ligações telefônicas, bem como não solicita dados

²⁴⁷ Delegacia Especializada de Defesa do Consumidor - DECON. POLÍCIA CIVIL DO ESTADO DO MATO GROSSO. [Unidades - Delegacias Regionais de Cuiabá e Várzea Grande](#).

²⁴⁸ Delegacia Especializada de Repressão aos Crimes Contra as Relações de Consumo - Decon. POLÍCIA CIVIL DO ESTADO DO MATO GROSSO DO SUL. [Delegacia Especializada de Repressão aos Crimes Contra as Relações de Consumo](#).

²⁴⁹ Delegacia Especializada de Defesa do Consumidor - DECON. POLÍCIA CIVIL DO ESTADO DE MINAS GERAIS. [Delegacia Especializada de Defesa do Consumidor - DECON](#), 16/01/2018.

²⁵⁰ Delegacia do Consumidor - DECON. POLÍCIA CIVIL DO ESTADO DO PARÁ. [Institucional - Diretorias - DPE](#).

²⁵¹ Delegacia Especializada de Proteção e Defesa do Consumidor. G1 - PARAÍBA. [Veja mudanças nos comandos de delegacias da Polícia Civil da Paraíba](#), 16/01/2019.

²⁵² Delegacia de Crimes Contra a Economia e Proteção ao Consumidor - DELCON. POLÍCIA CIVIL DO ESTADO DO PARANÁ. [Unidades Policiais - Delegacia de Crimes Contra a Economia e Proteção ao Consumidor](#).

²⁵³ Delegacia de Polícia de Crimes Contra o Consumidor - DECON. POLÍCIA CIVIL DO ESTADO DE PERNAMBUCO. [Institucional - Estrutura](#).

²⁵⁴ Delegacia de Crimes Contra a Ordem Tributária, Econômica e Relações de Consumo - DECCOTERC. POLÍCIA CIVIL DO ESTADO DO PIAUÍ. [Gerência de Polícia Especializada](#).

²⁵⁵ Delegacia do Consumidor - DECON. POLÍCIA CIVIL DO ESTADO DO RIO DE JANEIRO. [Departamentos e Delegacias da Polícia Civil do Estado do Rio de Janeiro](#).

²⁵⁶ Delegacia Especializada de Defesa do Consumidor - DECON. POLÍCIA CIVIL DO ESTADO DO RIO GRANDE DO NORTE. [Delegacias Especializadas Grande Natal](#).

²⁵⁷ Delegacia do Consumidor - DECON. POLÍCIA CIVIL DO ESTADO DO RIO GRANDE DO SUL. [Departamento Estadual de Investigações Criminais \(DEIC\)](#).

²⁵⁸ Delegacia Especializada em Crimes contra o Consumidor - DECCON. POLÍCIA CIVIL DO ESTADO DE RONDÔNIA. [Capital - Delegacias](#).

²⁵⁹ Delegacia de Defesa do Consumidor - DDCON. POLÍCIA CIVIL DO ESTADO DO ESTADO DE RORAIMA. [Endereços da Delegacias de Roraima](#).

²⁶⁰ Divisão de Investigações sobre Infrações contra o Consumidor. POLÍCIA CIVIL DO ESTADO DO ESTADO DE SÃO PAULO. [Departamentos/Órgãos Detalhes - DPPC](#).

²⁶¹ Em pesquisa na internet e nos sites das Polícias Cíveis, não foram identificadas delegacias especializadas em consumidor nos estados do Acre, Alagoas, Ceará, Santa Catarina, Sergipe e Tocantins.

²⁶² ANATEL. [#ConexãoSegura: confira dicas para proteger seus dados pessoais](#), 25/11/2019, 05/08/2020 (última atualização).

²⁶³ ANATEL. [Anatel alerta sobre fraudes](#), 20/02/2019, 08/03/2019 (última atualização).

persoais²⁶⁴, nem envia *links* por SMS, WhatsApp²⁶⁵, *e-mail* ou Telegram²⁶⁶. Ademais, em caso de suspeita de tentativa de fraude, os consumidores devem, conforme o caso, registrar o fato junto à polícia.²⁶⁷

No tocante a golpes e fraudes de maneira geral, a Agência reforça aos consumidores que nunca forneçam informações pessoais a *sites* e aplicativos que não reconheçam; nunca abram *links* desconhecidos; fiquem atentos ao receber mensagens ou *e-mails* com faturas; desconfiem de ofertas fantásticas; sempre atualizem sistema operacional, antivírus e *firewall*; desconfiem de contatos que dizem que você foi premiado; cuidem de suas senhas, criem senhas fortes e nunca usem senhas fáceis, como números em sequência ou datas de nascimento; desconfiem de *e-mails* de desconhecidos e com assuntos apelativos ou alarmantes; utilizem todas as opções de segurança fornecidas pelos aplicativos de celular, como a verificação em duas etapas; bem como aceitem que todos somos vulneráveis, desconfiando-se até da sombra virtual. Também é indicado que o consumidor pode se informar no *site* da Agência e, se se sentir ameaçado ou for lesado, deve recorrer às autoridades policiais.²⁶⁸

Figura 1 - Peça da campanha #ConexãoSegura sobre recebimento de faturas



FONTE: ANATEL. [#ConexãoSegura: confira dicas para proteger seus dados pessoais](#), 25/11/2019, 05/08/2020 (última atualização).

²⁶⁴ ANATEL. [#ConexãoSegura: confira dicas para proteger seus dados pessoais](#), 25/11/2019, 05/08/2020 (última atualização).

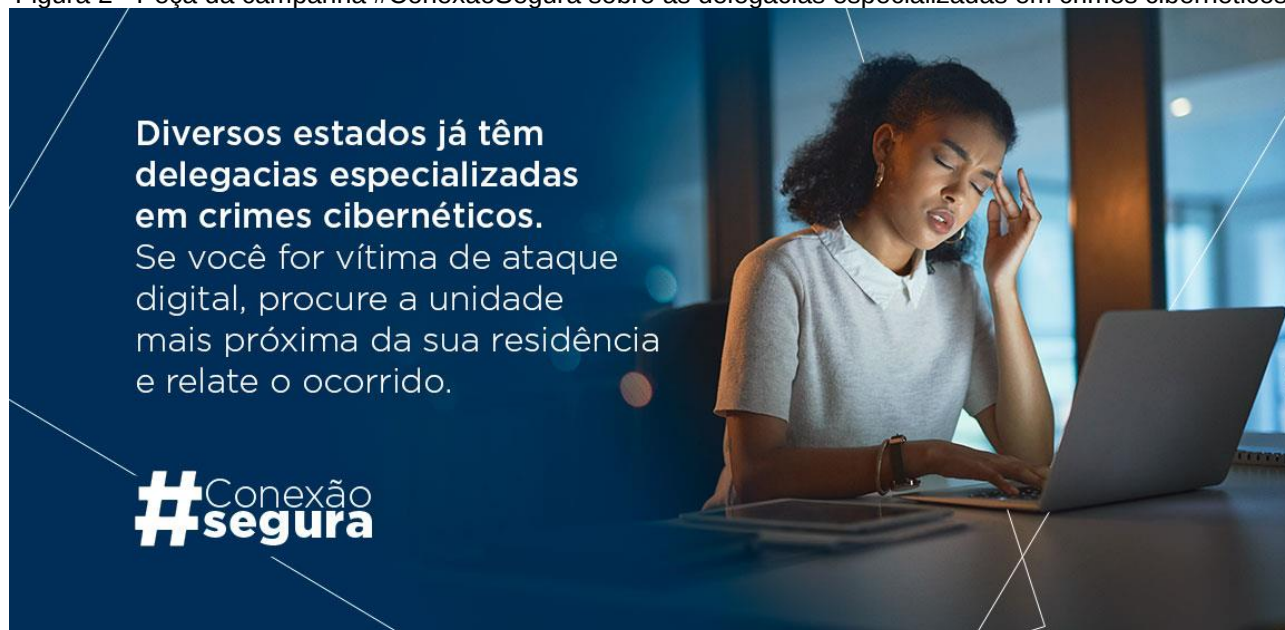
²⁶⁵ ANATEL. [Anatel alerta sobre fraudes](#), 20/02/2019, 08/03/2019 (última atualização).

²⁶⁶ ANATEL. [#ConexãoSegura: confira dicas para proteger seus dados pessoais](#), 25/11/2019, 05/08/2020 (última atualização).

²⁶⁷ ANATEL. [Anatel alerta sobre fraudes](#), 20/02/2019, 08/03/2019 (última atualização).

²⁶⁸ ANATEL. [#ConexãoSegura: confira dicas para proteger seus dados pessoais](#), 25/11/2019, 05/08/2020 (última atualização). [Tem fraude no isolamento: todo cuidado é pouco](#), 24/03/2020, 13/04/2020 (última atualização).

Figura 2 - Peça da campanha #ConexãoSegura sobre as delegacias especializadas em crimes cibernéticos



FONTE: ANATEL. [#ConexãoSegura: confira dicas para proteger seus dados pessoais](#), 25/11/2019, 05/08/2020 (última atualização).

A Agência também está atenta aos desenvolvimentos correntes, tendo alertado aos consumidores sobre golpes e fraudes se aproveitando da atual situação da pandemia do novo coronavírus. Nesse sentido, a Anatel advertiu aos consumidores sobre golpes utilizando seu nome e prometendo oferecer internet grátis ou solicitando dados pessoais por *e-mail*, SMS, ligação, Telegram ou WhatsApp²⁶⁹, bem como golpes oferecendo distribuição de álcool gel e falsos serviços de filmes e séries gratuitos.²⁷⁰

²⁶⁹ ANATEL. [#ConexãoSegura: confira dicas para proteger seus dados pessoais](#), 25/11/2019, 05/08/2020 (última atualização). [Tem fraude no isolamento: todo cuidado é pouco](#), 24/03/2020, 13/04/2020 (última atualização).

²⁷⁰ ANATEL. [#ConexãoSegura: confira dicas para proteger seus dados pessoais](#), 25/11/2019, 05/08/2020 (última atualização).

Figura 3 - Peça sobre golpes digitais na pandemia usando o nome da Agência para falsamente oferecer internet grátis ou solicitar dados pessoais



The poster features a dark background with a blue and green digital theme. On the right, a silhouette of a person in a hoodie holds a smartphone. On the left, a smartphone displays a fake Anatel message. The message text includes: 'Anatel', 'PARA CONSIENTIZAR O POVO', 'FICAR EM CASA, NÃO', 'TOTAL', '7GB de', 'VÁLIDO PARA A', 'vivo', 'nextel', 'ANTEL em conscientização', 'contra o Corona Vírus, esta', 'GRATUITAMENTE 7GB de', 'RECEBER INTERNET:', and a URL 'https://bit.ly/7GbdeInternet'. A large red 'FALSO' (False) stamp is diagonally placed over the fake message. The main title 'GOLPES DIGITAIS' is in large white letters at the top left. To its right is the hashtag '#Conexão segura' in white. Below the title, white text states: 'A Anatel não oferece pacotes de internet, ou qualquer produto, e jamais solicita dados pessoais por mensagem de Whatsapp, Telegram, SMS, e-mail ou ligação.' At the bottom, there are social media icons for Facebook (anatel.oficial), Twitter (anatel_oficial), and LinkedIn (anatel), along with the website 'www.anatel.gov.br'.

GOLPES DIGITAIS

#Conexão segura

A Anatel **não oferece pacotes de internet**, ou qualquer produto, e **jamais solicita dados pessoais** por mensagem de Whatsapp, Telegram, SMS, e-mail ou ligação.

anatel.oficial anatel_oficial anatel www.anatel.gov.br

FONTE: ANATEL. [#ConexãoSegura: confira dicas para proteger seus dados pessoais](#), 25/11/2019, 05/08/2020 (última atualização).

Ademais, entre vários exemplos, podem-se destacar algumas peças veiculadas pela Agência:

a) Matérias publicadas no Portal Institucional da Agência

- *Tem fraude no isolamento: todo cuidado é pouco*: alerta que o momento atual da pandemia do novo coronavírus está sendo aproveitado por pessoas mal-intencionadas que se utilizam de golpes e fraudes para roubar dados pessoais. Entre esses golpes a Anatel chama a atenção para golpe em que os criminosos, utilizando-se do nome da

Agência e das prestadoras de serviços de telecomunicações, supostamente oferecem internet grátis;²⁷¹

- *Campanha #ConexãoSegura*: motivada por reclamações de consumidores sobre tentativas de golpes e fraudes, a Agência realizou campanha com 14 *posts*, entre novembro e dezembro de 2019, com informações aos consumidores, entre outras, sobre a criação de senhas fortes e o não compartilhamento de dados pessoais ou senhas ao falar com desconhecidos.²⁷²

b) Campanhas e matérias do Portal do Consumidor da Agência

- Crimes cibernéticos: descubra como você pode se proteger de ataques na internet;²⁷³
- Anatel alerta usuários sobre tentativa de fraude usando nome da Agência;²⁷⁴
- #ConexãoSegura: confira dicas para proteger seus dados pessoais;²⁷⁵
- ANATEL EXPLICA - Edição 83 - *Cuidado com Dados Pessoais*: traz cinco dicas (proteger a privacidade, tomar cuidado com o que posta, conferir se sites que se vai acessar são seguros, atentar-se aos dados a serem acessados por aplicativos de celular e não divulgar informações bancárias) para que o consumidor cuide dos dados pessoais ao navegar pela internet, bem como alerta aos consumidores para que evitem compartilhar dados pessoais na rede;²⁷⁶
- ANATEL EXPLICA - Edição 84 - *Fraudes e Golpes, não caia nessa!*: orienta os consumidores a ficarem atentos a links enviados por SMS, e-mail ou WhatsApp; a notícias de que foi premiado e ao recebimento de pessoas em casa, pois podem ser criminosos se passando por representantes das prestadoras pretensamente realizando uma visita técnica, bem como indica que a Anatel não manda mensagens de texto ou realiza ligações informando sobre sorteios ou premiações.²⁷⁷

c) Postagens no Instagram

- A Anatel reproduziu nessa rede social as peças informativas sobre os golpes se aproveitando da pandemia do novo coronavírus, comunicando aos consumidores que se tratam de golpes a distribuição de álcool gel grátis²⁷⁸ e o oferecimento de internet

²⁷¹ ANATEL. [Tem fraude no isolamento: todo cuidado é pouco](#), 24/03/2020, 13/04/2020 (última atualização).

²⁷² ANATEL. [Anatel realiza campanha educativa de proteção de dados pessoais](#), 26/11/2019, 28/11/2019 (última atualização).

²⁷³ ANATEL. [Crimes cibernéticos: descubra como você pode se proteger de ataques na internet!](#), 02/01/2018, 27/08/2019 (última atualização).

²⁷⁴ ANATEL. [Anatel alerta usuários sobre tentativa de fraude usando nome da Agência](#), 25/07/2017, 27/08/2019 (última atualização).

²⁷⁵ ANATEL. [#ConexãoSegura: confira dicas para proteger seus dados pessoais](#), 25/11/2019, 05/08/2020 (última atualização).

²⁷⁶ Todas as edições do Anatel Explica estão disponíveis no Portal do Consumidor da Agência em ANATEL. [Anatel Explica](#), e a edição 83 está disponível em ANATEL. [Cuidado com dados pessoais](#).

²⁷⁷ Todas as edições do Anatel Explica estão disponíveis no Portal do Consumidor da Agência em ANATEL. [Anatel Explica](#), e a edição 84 está disponível em ANATEL. [Fraudes e Golpes, não caia nessa!](#).

²⁷⁸ ANATEL - INSTAGRAM. [Golpes Digitais - Álcool em gel grátis](#).

grátis ou solicitação de dados pessoais utilizando-se do nome da Agência²⁷⁹. Também é orientando aos consumidores para nunca clicarem em *links* enviados por desconhecidos via SMS, e-mail, Telegram ou WhatsApp²⁸⁰;

d) Postagens no Twitter

- A Agência reproduziu no Twitter, em janeiro do corrente ano, as postagens da campanha #ConexãoSegura, alertando aos consumidores sobre como usar todas as opções de segurança dos aplicativos de celular, como a verificação em duas etapas²⁸¹; criar senhas fortes²⁸²; encerrar sessões e bloquear a tela de computadores em locais públicos²⁸³; não abrir *links* e *pop-ups* chamativos²⁸⁴; checar a reputação de vendedores antes de realizar compras na internet²⁸⁵; atualizar antivírus e sistema operacional²⁸⁶; cuidado ao receber e-mails ou mensagens com faturas²⁸⁷; recorrer às delegacias especializadas em crimes cibernéticos²⁸⁸ e não fornecer dados pessoais ou senhas em ligações de desconhecidos²⁸⁹.
- Entre março e maio de 2020, também foram reproduzidas nessa rede social as peças alertando aos consumidores sobre golpes e fraudes durante o período da pandemia²⁹⁰, conforme já abordado anteriormente nessa seção; e
- A Agência também realizou *retweets* de *tweets*, sobre golpes e fraudes, desenvolvidos pelo Núcleo de Informação e Coordenação do Ponto BR (NIC.br), ligado ao Comitê Gestor da Internet no Brasil (CGI.br)²⁹¹.

Ademais, a Anatel, em sede de processo de fiscalização regulatória, demandou às prestadoras de serviços de telecomunicações a realização de uma campanha antifraude. Lançada em 14 de outubro, a campanha #FiqueEsperto, agora com um escopo ampliado, incluindo os setores financeiro, comercial e de governança da internet, estender-se-á por quatro meses e compreende postagens em redes sociais, o envio de SMSs e e-mails, bem como o *hotsite* <https://fe.seg.br/>.²⁹² Em especial, o *site* contém dicas de segurança para que os consumidores

²⁷⁹ ANATEL - INSTAGRAM. [Golpes Digitais - Oferta ou solicitação da Anatel](#).

²⁸⁰ ANATEL - INSTAGRAM. [Golpes Digitais - Nunca clique em links enviados por desconhecidos](#).

²⁸¹ ANATEL - TWITTER. [#ConexãoSegura](#), 02/01/2020. [#ConexãoSegura](#), 03/01/2020. [#ConexãoSegura](#), 06/01/2020.

²⁸² ANATEL - TWITTER. [#ConexãoSegura](#), 04/01/2020. [#ConexãoSegura](#), 05/01/2020. [#ConexãoSegura](#), 07/01/2020.

²⁸³ ANATEL - TWITTER. [#ConexãoSegura](#), 08/01/2020.

²⁸⁴ ANATEL - TWITTER. [#ConexãoSegura](#), 09/01/2020.

²⁸⁵ ANATEL - TWITTER. [#ConexãoSegura](#), 10/01/2020.

²⁸⁶ ANATEL - TWITTER. [#ConexãoSegura](#), 11/01/2020.

²⁸⁷ ANATEL - TWITTER. [#ConexãoSegura](#), 12/01/2020.

²⁸⁸ ANATEL - TWITTER. [#ConexãoSegura](#), 13/01/2020.

²⁸⁹ ANATEL - TWITTER. [#ConexãoSegura](#), 14/01/2020.

²⁹⁰ ANATEL - TWITTER. [Golpes digitais](#), 24/03/2020. [Golpes digitais](#), 25/03/2020. [Golpes digitais](#), 26/03/2020. [Golpes digitais](#), 27/03/2020. [Golpes digitais](#), 25/05/2020.

²⁹¹ NIC.br - TWITTER. [Internet Segura](#), 26/03/2020. [#InternetSeguraCoronavírus](#), 30/03/2020. [#InternetSeguraCoronavírus](#), 31/03/2020. [Internet Segura](#), 08/04/2020a. [Internet Segura](#), 08/04/2020b. [Internet Segura](#), 27/04/2020. [Internet Segura](#), 06/05/2020. [Internet Segura](#), 07/05/2020.

²⁹² ASSOCIAÇÃO BRASILEIRA DE INTERNET - ABRANET. [Abranet adere à iniciativa multisetorial #FiqueEsperto](#), 14/10/2020. CORREIO BRAZILIENSE. [Campanha informativa #FiqueEsperto alerta para segurança digital](#), 14/10/2020.

protejam-se de vários tipos de golpes e fraudes que ocorrem no ambiente digital²⁹³. Entre as dicas já apresentadas na página estão as de não utilizar a mesma senha em vários serviços e habilitar a verificação em duas etapas, bem como orientações para a elaboração de senhas²⁹⁴.

1.2. Comitê Gestor da Internet no Brasil - CGI.br

O Comitê Gestor da Internet no Brasil (CGI.br) é um órgão multissetorial com representantes do governo, do setor empresarial, do terceiro setor, da comunidade científica e tecnológica e um representante de notório saber em assuntos de internet.²⁹⁵ O órgão é responsável por estabelecer diretrizes relacionadas à internet no país.²⁹⁶ O CGI.br mantém, dentro de sua estrutura o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.Br), que tem entre suas atribuições o trabalho de conscientização sobre problemas de segurança. Dessa forma, o CERT.br elaborou a Cartilha de Segurança para Internet, que, além da descrição de golpes corriqueiros na internet, apresenta também formas de prevenção a eles.²⁹⁷

Em linhas gerais, a Cartilha indica, então, as seguintes medidas de prevenção para cada golpe que relaciona:

- Furto de identidade (*identity theft*): evitar que o golpista tenha acesso aos seus dados e às suas contas de usuário, bem como ser cuidadoso com senhas, tanto na elaboração, quanto na guarda. Ademais é necessário atenção a possíveis sinais de roubo de identidade, entre os quais, acesso a redes sociais em horários e locais incomuns para o padrão de uso do usuário, problemas com órgãos de proteção de crédito e extrato bancário ou de cartão de crédito com movimentações não usuais;
- Fraude de antecipação de recursos (*advance fee fraud*): aprender a identificar as mensagens contendo tentativas de golpes, como aquelas que envolvem largas quantias de dinheiro, pagamento antecipado para recebimento de maiores valores futuramente e que solicitam sigilo e/ou urgência na resposta. Ademais nunca se deve responder a tais mensagens, pois isso serve de confirmação que o *e-mail* é válido, acabando por ser repassado a listas de *spam* ou encaminhado a golpistas que praticam outros tipos de golpes;
- *Phishing*: ficar atento e desconfiar de mensagens recebidas, identificando características típicas de mensagens fraudulentas, como aquelas contendo solicitação

NÚCLEO DE INFORMAÇÃO E COORDENAÇÃO DO PONTO BR - NIC.br. [Com apoio do NIC.br e CGI.br, campanha #FiqueEsperto amplia conscientização sobre o uso seguro da Internet](#), 14/10/2020. TELE TIME. [Campanha multissetorial alerta para proteção de dados no ambiente virtual](#), 14/10/2020.

²⁹³ #FIQUEESPERTO. [Página inicial](#).

²⁹⁴ #FIQUEESPERTO. [Proteção de contas](#).

²⁹⁵ COMITÊ GESTOR DA INTERNET NO BRASIL - CGI.br. [Composição do CGI.br](#).

²⁹⁶ COMITÊ GESTOR DA INTERNET NO BRASIL - CGI.br. [Atribuições](#).

²⁹⁷ CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL - CERT.br. [Cartilha de Segurança para Internet - Golpes na Internet](#).

de dados pessoais, solicitação de clique em *links*, solicitação de instalação ou execução de programas, que tenham assuntos chamativos e que tenham como remetentes instituições com as quais você não tem relação e solicitam algum tipo de atualização de módulo de segurança ou cadastramento. Além disso, deve-se utilizar mecanismos de segurança, como filtros *antiphishing*, *antimalware* e *firewall*; verificar se as páginas na internet possuem certificado de segurança válido e utilizam conexão segura, bem como se acostumar a fazer verificações nos *sites* originais das instituições em que as mensagens supostamente se originam, sem clicar em *links* enviados nas mensagens;

- *Pharming*: desconfiar de redirecionamento de *sites* e de *sites* de *internet banking* ou comércio eletrônico que não utilizem conexão segura, além de verificar os certificados dos *sites*;
- Golpe do *site* de comércio eletrônico fraudulento: fazer pesquisa de mercado e aprender a identificar preços suspeitos, checar *sites* especializados em tratar reclamações de consumidores, ligar o alerta em relação a publicidade recebida por *spam*, validar os dados de cadastro da empresa no *site* da Receita Federal, entre outros;
- Golpe envolvendo *sites* de compras coletivas: evitar comprar no impulso, ser cauteloso e sempre realizar pesquisas sobre os *sites* envolvidos e sobre o produto/serviço que se pretende comprar;
- Golpe do *site* de leilão e venda de produtos: sempre checar o valor de mercado do produto e desconfiar de valores muito bons, pesquisar *sites* especializados em reclamações, utilizar sistemas de gerenciamento de pagamento, verificar a reputação dos usuários, etc; e
- Boato (*hoax*): sempre conferir a procedência e a veracidade das mensagens, desconfiando de mensagens, mesmo que o remetente seja conhecido. Ademais, o boato geralmente apresenta algumas características como ameaçar consequências para a vítima caso não realize algo, promessa de ganhos financeiros, erros gramaticais e de ortografia, informações contraditórias, urgência no repasse da mensagem para outros, etc. Adicionalmente, uma simples pesquisa na internet com o tema da mensagem já pode ser suficiente para identificar que a suposta informação é na verdade um boato.²⁹⁸

A cartilha aponta ainda, como dicas gerais para a prevenção de golpes: ao identificar uma tentativa de golpe, informe à instituição cujo nome foi utilizado e, tendo em vista que os golpes são dinâmicos, esteja sempre informado e atualizado (indicando-se ainda alguns *sites* especializados em que o usuário pode se informar).

²⁹⁸ CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL - CERT.br. [Cartilha de Segurança para Internet - Golpes na Internet](#).

Ademais, a cartilha também apresenta uma parte de fascículos em que há material específico sobre os temas: privacidade, boatos, redes sociais, comércio eletrônico, senhas, verificação em duas etapas, *backup*, códigos maliciosos, *internet banking* e segurança em dispositivos móveis, computadores e em redes.²⁹⁹ Nesses fascículos há informações, orientações e dicas, entre as quais:

- Impactos, na privacidade, da divulgação de informações pessoais na internet, bem como os riscos associados a essa divulgação e golpes e ataques na internet;
- Principais riscos do comércio eletrônico, incluindo o não recebimento de produtos e uso indevido de dados pessoais e financeiros;
- Principais riscos e cuidados a serem tomados ao se realizar transações por *internet banking*;
- Atenção a mensagens e ligações que solicitem dados pessoais, senhas, dados financeiros e números de cartão de crédito;
- Verificação de política de privacidade de *sites*;
- Verificação das condições de compra e de reputação de *sites*/lojas/vendedores atuantes no comércio eletrônico;
- Utilizar conexões seguras, que podem ser verificadas, por exemplo, pelo começo do endereço *on-line* com *https* e o ícone de um cadeado fechado na barra de endereço do navegador de internet;
- Cuidado na divulgação de dados de localização;
- Cuidado no aceite de contatos e associação a grupos em redes sociais;
- Definição de boato, como identificá-lo, os problemas que os boatos trazem e como combatê-los;
- Caracterização de vários tipos de códigos maliciosos, entre os quais cavalo de Tróia (*trojan*), *rootkit*, *bot*, *backdoor*, *spyware*, *ransomware*, *worm* e vírus;
- Cuidado especial com as crianças, incluindo não exposição excessiva de filhos e informação, às crianças, sobre os riscos das redes sociais;
- Como proteger contas de *e-mail* e redes sociais, incluindo criação de senhas fortes e verificação em duas etapas;
- Como manter equipamentos seguros, incluindo instalação de antivírus, *antispam*, *antimalware* e *firewall*; proteção com senha em computadores e dispositivos móveis, bem como manutenção de aplicativos e sistemas operacionais atualizados e com programação de atualização automática;

²⁹⁹ Lista de temas presentes em 14/10/2020. CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL - CERT.br. [Cartilha de Segurança para Internet - Fascículos](#).

- Como criar senhas fortes, o que evitar na criação de senhas, uso de frases em senhas, alteração de senhas, utilização de mecanismos de recuperação e dicas para a criação de boas senhas, bem como riscos associados à não proteção de senhas, incluindo acessos não autorizados a contas bancárias, redes sociais, *e-mails* e computador;
- Proteção de equipamentos de rede, incluindo atualização de *firmware* e alteração de senha de administração;
- Realizar *backups* e mantê-los em locais seguros e com acesso restrito, bem como alerta de cuidados ao se usar serviços de *backup on-line*;
- Cuidados ao se conectar a redes móveis e redes Wi-Fi, em especial Wi-Fi público, bem como ao utilizar conexões *bluetooth*;
- Utilizar verificação em duas etapas sempre que possível; e
- Indicação de cuidado ao abrir anexos e clicar em *links*.³⁰⁰

O Comitê Gestor da Internet no Brasil também mantém outras iniciativas entre as quais as páginas InternetSeguraBR³⁰¹ e Antispam.br³⁰². A primeira reúne “iniciativas de conscientização sobre segurança e uso responsável da Internet no Brasil, auxiliando os internautas a localizar as informações de interesse e incentivando o uso seguro da Internet”³⁰³ e a segunda “tem o compromisso primordial de informar o usuário e o administrador de redes sobre o *spam*, suas implicações e formas de proteção e combate”³⁰⁴.

1.3. Prestadoras de serviços de telecomunicações

a) CLARO

A CLARO possui página dedicada sobre segurança, na qual informa sobre situações específicas que demandam atenção e cuidado, em especial indicando que fraudadores podem tentar se passar por prestadores de serviço de forma geral.

Inicialmente, nessa página, há um demonstrativo de uma fatura da empresa, com indicações sobre como verificar a autenticidade da mesma. Informa-se ainda nessa seção qual é o *e-mail* e o

³⁰⁰ CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL - CERT.br. [Backup - Slides para a divulgação das boas práticas](#). [Boatos - Slides para a divulgação das boas práticas](#). [Códigos Maliciosos - Slides para a divulgação das boas práticas](#). [Fascículo Backup](#), Dezembro 2017. [Fascículo Boatos](#), Abril 2018. [Fascículo Códigos Maliciosos](#), Março 2017. [Fascículo Comércio Eletrônico](#), Março 2017. [Fascículo Computadores](#), Março 2017. [Fascículo Dispositivos Móveis](#), Março 2017. [Fascículo Internet Banking](#), Março 2017. [Fascículo Privacidade](#), Março 2017. [Fascículo Redes](#), Março 2017. [Fascículo Redes Sociais](#), Março 2017. [Fascículos Senhas](#), Março 2017. [Fascículo Verificação em Duas Etapas](#), Março 2017. [Privacidade - Slides para a divulgação das boas práticas](#). [Redes sociais - Slides para a divulgação das boas práticas](#). [Segurança em Comércio Eletrônico - Slides para a divulgação das boas práticas](#). [Segurança em Computadores - Slides para a divulgação das boas práticas](#). [Segurança em Dispositivos Móveis - Slides para a divulgação das boas práticas](#). [Segurança em Internet Banking - Slides para a divulgação das boas práticas](#). [Segurança em Redes - Slides para a divulgação das boas práticas](#). [Segurança em Senhas - Slides para a divulgação das boas práticas](#). [Verificação em Duas Etapas - Slides para a divulgação das boas práticas](#).

³⁰¹ NÚCLEO DE INFORMAÇÃO E COORDENAÇÃO DO PONTO BR - NIC.BR. [Internet Segura BR](#).

³⁰² NÚCLEO DE INFORMAÇÃO E COORDENAÇÃO DO PONTO BR - NIC.BR. [Antispam.br](#).

³⁰³ NÚCLEO DE INFORMAÇÃO E COORDENAÇÃO DO PONTO BR - NIC.BR. [Sobre o Internet Segura](#).

³⁰⁴ Grifos nossos. NÚCLEO DE INFORMAÇÃO E COORDENAÇÃO DO PONTO BR - NIC.BR. [Sobre o antispam.br](#).

número de WhatsApp oficial da prestadora, bem como informações sobre a linguagem utilizada nos *e-mails* referentes à fatura e a proteção do boleto enviado. Adicionalmente há outras dicas importantes sobre boletos, caracterizando detalhes típicos de mensagens fraudulentas.³⁰⁵

Também nessa página há dicas de proteção no WhatsApp, como não compartilhar código de confirmação, ativar verificação em duas etapas, não instalar *apps* de terceiros ou compartilhar informações pessoais a pedido de ninguém por meio do aplicativo e desconfiar de ligações de empresas com linguagem informal. Adicionalmente, há referência a página de perguntas e respostas mantida pelo próprio aplicativo³⁰⁶, bem como há informações sobre providências a serem adotadas em caso de a conta desse *app* ter sido *hackeada*, além de outras dicas de segurança específicas para o aplicativo.³⁰⁷

Na seção “Dicas antifraude”, há *link*³⁰⁸ para página da própria prestadora com informações específicas sobre o projeto da Anatel de cadastramento e consulta de celulares pré-pagos, há indicação de que a prestadora não solicita dados de cartão de crédito por telefone ou *e-mail* e que não tem contrato com a empresa Electroneum para disponibilizar pagamento da fatura ou realização de recargas via criptomoeda, bem como é reforçada a sugestão de não se instalar aplicativos, de reputação duvidosa, que prometem bonificações ou navegação gratuita.³⁰⁹

Enfim, a página indica aos consumidores que entrem em contato com a prestadora caso suspeitem de informações veiculadas em seu nome, bem como apresenta mais algumas referências sobre como se proteger no tocante a caixa postal, ligações e mensagens suspeitas, visitas técnicas e biometria e senhas.³¹⁰

b) OI

A OI também possui página específica com avisos e dicas sobre segurança. Nela a prestadora apresenta quatro golpes (falsas promoções, falsos sequestros-relâmpagos, falsas solicitações de reparo e falsos *e-mails*), indicando ao consumidor como o golpe é feito, como se pode identificá-lo e o que fazer para se prevenir. Também é fornecido alerta específico, indicando que a prestadora não tem qualquer relação com uma empresa de *marketing* multinível.³¹¹

De forma geral a prestadora orienta os consumidores a não fornecerem informações pessoais e instruir os familiares da mesma maneira, a não abrir *e-mails* suspeitos ou clicar em *links* ou arquivos constantes dessas mensagens, bem como a manter antivírus e *antispam* atualizados. A prestadora também indica que o consumidor deve estar atento, pois ela não realiza ligações a

³⁰⁵ CLARO. [Segurança](#).

³⁰⁶ WHATSAPP. [Como podemos ajudar você?](#).

³⁰⁷ CLARO. [Segurança](#).

³⁰⁸ CLARO. [Projeto cadastro pré-pago](#).

³⁰⁹ CLARO. [Segurança](#).

³¹⁰ CLARO. [Segurança](#).

³¹¹ OI. [Avisos e dicas de segurança](#).

cobrar, não solicita senhas de cartões de recarga e que em caso de dúvida sobre promoções, deve-se entrar em contato com a prestadora.³¹²

Ademais, ao final da página ainda há *link*³¹³ para uma cartilha sobre o tema da segurança da informação, trazendo alguns conceitos, dicas e perguntas e respostas³¹⁴. A seção de conceitos traz, entre outras, as definições de *spam*, *antivírus*, *antispam*, *spyware*, *phishing*, *criptografia* e *firewall*³¹⁵, enquanto a seção sobre perguntas e resposta endereça as questões de porque alguém tentaria invadir o computador do consumidor, como proteger as informações enviadas por *e-mail*, porque realizar *backup* e como saber se um antivírus é bom³¹⁶. Por seu turno, a seção de dicas traz informações sobre como não ser vítima de *phishing*, como evitar vírus de computador, o que fazer em caso de suspeita de *e-mail* falso, como acabar com o *spam* e a importância da troca e redefinição de senhas³¹⁷.

c) SKY

Na SKY, a página dedicada a fraudes é bem simples, somente indicando ao consumidor, por meio de quatro pontos, como distinguir faturas falsas e mensagens suspeitas.³¹⁸

d) TIM

Em página dedicada a dicas de segurança, a TIM indica tanto aos clientes, quanto às pessoas em geral, que há tentativas de golpes que tentam se apropriar tanto do nome da TIM, quanto de outras prestadoras e, nesse sentido, a TIM aponta golpes corriqueiros e dicas de segurança na referida página.³¹⁹

Entre os golpes, a TIM lista *e-mails* falsos (*phishing*)³²⁰, falsos sequestros³²¹, golpe do siga-me (programação de encaminhamento de chamadas recebidas para outro número)³²² e falsas promoções³²³, promoções de aniversário³²⁴ e de bônus de recarga³²⁵.

Entre as dicas, a prestadora indica ao consumidor que adote a verificação em duas etapas no WhatsApp³²⁶; tenha antivírus e *firewall* atualizados no computador³²⁷; desconfie de ligações sobre

³¹² OI. [Avisos e dicas de segurança](#).

³¹³ OI. [Avisos e dicas de segurança. Leia mais sobre segurança da informação e saiba como se manter protegido na internet](#).

³¹⁴ OI. [Book com terminologias de segurança da informação](#).

³¹⁵ OI. [Book com terminologias de segurança da informação](#), p. 3 e 4.

³¹⁶ OI. [Book com terminologias de segurança da informação](#), p. 4 e 5.

³¹⁷ OI. [Book com terminologias de segurança da informação](#), p. 5 e 6.

³¹⁸ SKY. [Aprenda a se proteger de fraudes](#).

³¹⁹ TIM. [Dicas de segurança](#).

³²⁰ TIM. [E-mails falsos \(phishing\)](#).

³²¹ TIM. [Falso sequestro](#).

³²² TIM. [Golpe do siga-me](#).

³²³ TIM. [Falsas promoções](#).

³²⁴ TIM. [Falsa promoção de aniversário](#).

³²⁵ TIM. [Falsa promoção do bônus de recarga](#).

³²⁶ TIM. [Duplo fator de segurança WhatsApp](#).

³²⁷ TIM. [E-mails falsos \(phishing\)](#).

promoções, prêmios ou bônus de crédito³²⁸; não execute arquivos recebidos na internet³²⁹; não forneça dados pessoais e documentos a pessoas desconhecidas³³⁰ e oriente familiares a fazer o mesmo³³¹; não abra mensagens de remetentes desconhecidos³³²; evite atender ligações a cobrar³³³; registre ocorrência policial³³⁴; não ligue para número de origem desconhecida informado em mensagem de texto³³⁵ e verifique o número do remetente de mensagens de texto para ter certeza que se trata da prestadora³³⁶.

A prestadora também informa os endereços de seus perfis em redes sociais³³⁷, indica que não solicita dados pessoais por *e-mail*³³⁸, bem como alerta à população sobre possíveis fraudes se aproveitando do tridígito 136 destinado ao Ministério da Saúde para realização de ligações sobre a Covid-19³³⁹.

e) VIVO

Na Vivo, as informações sobre golpes e fraudes estão em página dedicada, dentro da seção de ajuda do *site* da prestadora. Nessa página são destacados seis itens com *links* que abrem uma nova página sobre o assunto, sendo eles: ligações; *e-mails*; mensagens de texto; boletos; visitas técnicas; e WhatsApp.³⁴⁰

De forma geral, os itens apresentam caracterização de golpes, exemplos e indicação de formas de prevenção, conforme indicado abaixo:

a) Ligações

- *Redução de custos telefônicos*: falsa empresa promete redução de custos telefônicos mediante fornecimento de dados pessoais e pagamento de falso boleto;
- *Falsa troca de aparelho*: golpista se passa pela prestadora indicando ou que o consumidor ganhou uma promoção para troca de aparelho celular ou que a troca é obrigatória. Em ambos os casos o preço do novo aparelho é convidativo e o golpista diz que para efetuar a troca é necessário fornecer dados de cartão de crédito. A prestadora alerta que não obriga a troca de aparelho, não liga a cobrar e que caso o consumidor suspeite, deve encerrar a ligação. Ademais, se o consumidor tiver sido vítima, orienta a

³²⁸ TIM. [Golpe do siga-me](#).

³²⁹ TIM. [E-mails falsos \(phishing\)](#).

³³⁰ TIM. [Falsas promoções](#). [Golpe do siga-me](#).

³³¹ TIM. [Falso sequestro](#).

³³² TIM. [E-mails falsos \(phishing\)](#).

³³³ TIM. [Golpe do siga-me](#).

³³⁴ TIM. [Falso sequestro](#).

³³⁵ TIM. [Falsas promoções](#).

³³⁶ TIM. [Falsa promoção de aniversário](#). [Falsa promoção do bônus de recarga](#).

³³⁷ TIM. [Perfis TIM nas redes sociais](#).

³³⁸ TIM. [E-mails com links TIM](#).

³³⁹ TIM. [Ligações 136 - COVID-19](#).

³⁴⁰ VIVO. [Vivo Dúvidas: Fraudes](#).

recorrer à polícia, e, em caso de ter informado dados bancários ou de cartão de crédito, entrar em contato com a administradora do cartão ou o banco imediatamente;

- *Fraude por chip clonado*: novamente golpistas se passando pela prestadora informam falsamente ao consumidor que seu *chip* foi clonado, solicitando ao consumidor que desligue o telefone por uma hora. Nesse ínterim os golpistas ligam para familiares do consumidor, simulando um sequestro. A prestadora indica que nunca solicita aos consumidores que realizem o desligamento de aparelhos por longos períodos sob a justificativa de atualização ou manutenção;
- *Obtenção do código Meu Vivo*: golpistas tentam induzir o consumidor a informar o código do aplicativo da prestadora, que ressalta que não solicita tal código ou senha do consumidor; e
- *Instalação de Internet Fixa*: golpistas oferecem instalação de internet fixa mediante pagamento. A prestadora indica que não solicita dados de cartão de crédito e nem cobra serviços em boletos separados para além da fatura do consumidor.³⁴¹

b) *E-mails*

- *Pendências financeiras*: *e-mails* falsos apontam que o consumidor está com pendências financeiras, sendo necessário quitá-las sob pena de adoção de medidas legais. Os *links* dessas mensagens visam capturar informações pessoais; e
- *Falsas contas digitais*: *e-mails* com falsas faturas da prestadora, indicando a mesma que o consumidor deve sempre verificar o remetente, sendo que aqui são informados os endereços exclusivos da prestadora, bem como deve ser checada também as saudações da mensagem e os dados da fatura (nome, endereço, linha, plano e outros dados do titular).³⁴²

c) *Mensagens de texto*

- *Mensagens de texto falsas*: em geral essas mensagens indicam falsamente que o consumidor ganhou prêmios ou apontam curas milagrosas. A prestadora aponta aqui que o consumidor pode averiguar se um SMS é pirata por meio de consulta ao site <http://www.smspirata.com.br/smsoficial.php>;
- *SMS Oficial e SMS Pirata*: aqui a prestadora caracteriza esses tipos de SMS;
- *Exemplos reais de mensagens de textos falsas*: traz exemplos desse tipo de mensagem;
- *Mensagens de texto com fraude em boleto*: são SMSs falsos que enviam *links* com assuntos como, entre outros, desbloqueio, atualização cadastral e contestação de valores; e

³⁴¹ VIVO. [Vivo dúvidas: Ligações falsas](#).

³⁴² VIVO. [Vivo dúvidas: E-mails falsos](#).

- *Recebeu um SMS falso ou suspeito? Denuncie e ajude a acabar com essa prática:* por fim, a prestadora encoraja os consumidores a reportarem casos.³⁴³

d) Boletos

- Aqui a prestadora ressalta aos consumidores que fiquem atentos ao receberem boletos, observando especialmente dados de nome, endereço, linha, plano e dados do código de barra (sempre começam ou com 846 ou 848), bem como outros dados do titular presentes tanto no *e-mail* de envio do boleto, quanto no próprio boleto. Também é indicado aos consumidores que em caso de dúvidas, solicitem segunda via pelo aplicativo da prestadora ou pelo WhatsApp.³⁴⁴

e) Visitas técnicas

- A prestadora informa que nunca envia técnicos sem antes ter agendado junto ao consumidor. Adicionalmente a prestadora recomenda a instalação de seu aplicativo para que o consumidor possa visualizar informações mais detalhadas sobre os atendimentos agendados.³⁴⁵

f) WhatsApp

- *Conheça o WhatsApp Vivo:* a prestadora informa aqui o número oficial de seu WhatsApp, bem como os serviços que o consumidor pode solicitar por meio desse aplicativo;
- *Como se proteger de golpes no WhatsApp:* indica que os consumidores devem sempre desconfiar de ligações que se dizem de empresas, mas que utilizam linguagem informal; devem ativar a verificação em duas etapas; não devem fornecer o código de confirmação do aplicativo e não devem instalar aplicativos de terceiros ou informar dados pessoais a pedido de ninguém por meio do *app*;
- *Se sua conta foi roubada, Como ativar a confirmação em 2 etapas e O que fazer se sua conta foi hackeada:* dá instruções sobre como recuperar ou desativar a conta em caso de perda/roubo, como ativar a verificação em duas etapas e instruções para as providências a serem tomadas em caso de a conta ser *hackeada*. Também é indicado a seção de perguntas e repostas da próprio aplicativo³⁴⁶ para mais informações.³⁴⁷

Ademais, a prestadora também mantém o *site Dialogando Vivo*, para discussão de “diversos temas ligados ao uso consciente da tecnologia e seus impactos na vida das pessoas”, com matérias produzidas por pesquisadores, jornalistas e publicitários³⁴⁸. O portal da Vivo tem parceria com a

³⁴³ VIVO. [Vivo dúvidas: Mensagens de texto falsas.](#)

³⁴⁴ VIVO. [Vivo dúvidas: Boletos falsos.](#)

³⁴⁵ VIVO. [Vivo dúvidas: Falsas visitas técnicas.](#)

³⁴⁶ WHATSAPP. [Como podemos ajudar você?](#)

³⁴⁷ VIVO. [Vivo dúvidas: Golpes via WhatsApp.](#)

³⁴⁸ VIVO - DIALOGANDO VIVO. [Sobre o Dialogando.](#)

SaferNet Brasil³⁴⁹ e é dividido nas seções “Comportamento”³⁵⁰, “Inovação”³⁵¹, “Segurança”³⁵², “Educação”³⁵³ e “Sustentabilidade”³⁵⁴, além de contar com campanhas³⁵⁵ e cartilhas³⁵⁶. Em especial na seção “Segurança” são apresentadas dicas, entre outras, sobre senhas³⁵⁷, como se proteger de golpes e fraudes³⁵⁸, como funciona a autenticação em dois fatores³⁵⁹, como atualizar o sistema operacional do celular³⁶⁰, *fake news* e sua identificação³⁶¹, o que fazer em caso de ter o aparelho celular roubado³⁶², compartilhamento de dados nas redes sociais de forma segura³⁶³ e proteção de crianças na *web*³⁶⁴.

4. INICIATIVA INTERNACIONAL - ECONSUMER.GOV

O econsumer.gov é uma iniciativa da Rede Internacional de Proteção e Fiscalização do Consumidor (International Consumer Protection and Enforcement Network - ICPEN). A ICPEN indica ser uma rede de organizações governamentais unidas na aplicação de leis de práticas justas no comércio e outras atividades de proteção ao consumidor.³⁶⁵

A página é uma parceria entre mais de 35 agências de proteção de consumidores ao redor do mundo e contempla dois componentes³⁶⁶:

³⁴⁹ Como já explicitado anteriormente, a SaferNet Brasil “é uma associação civil de direito privado, com atuação nacional, sem fins lucrativos ou econômicos, sem vinculação político partidária, religiosa ou racial [...] com foco na promoção e defesa dos Direitos Humanos na Internet no Brasil”. SAFERNET BRASIL. [Institucional](#).

³⁵⁰ VIVO - DIALOGANDO VIVO. [Comportamento](#).

³⁵¹ VIVO - DIALOGANDO VIVO. [Inovação](#).

³⁵² VIVO - DIALOGANDO VIVO. [Segurança](#).

³⁵³ VIVO - DIALOGANDO VIVO. [Educação](#).

³⁵⁴ VIVO - DIALOGANDO VIVO. [Sustentabilidade](#).

³⁵⁵ VIVO - DIALOGANDO VIVO. [Campanhas](#).

³⁵⁶ VIVO - DIALOGANDO VIVO. [Cartilhas](#).

³⁵⁷ VIVO - DIALOGANDO VIVO. [A importância de ter senhas seguras](#), 22/04/2016.

³⁵⁸ VIVO - DIALOGANDO VIVO. [Entenda como se prevenir contra fraudes e mensagens enganosas](#), 19/09/2017. [Crimes online: denuncie, não ignore!](#), 20/04/2016

³⁵⁹ VIVO - DIALOGANDO VIVO. [Como funciona a autenticação em dois fatores?](#), 10/08/2020. [Descomplicando a Tecnologia: senhas e autenticação em dois fatores](#), 09/10/2020.

³⁶⁰ VIVO - DIALOGANDO VIVO. [Descomplicando a tecnologia: como atualizar o software do celular](#), 19/10/2020.

³⁶¹ VIVO - DIALOGANDO VIVO. [Checagem de fake news](#), 26/03/2018. [Como a tecnologia ajuda jornalistas a não espalharem fake news?](#), 04/06/2019. [Debate sobre fake news em novo formato de conteúdo](#), 21/08/2018. [Fake News: como descobrir se uma notícia é verdadeira ou não](#), 14/02/2020. [Fake news: e quando sua própria mente tenta te enganar?](#), 17/09/2019. [Fake news está em ‘quase’ todo clique](#), 22/08/2018. [Fake News no Twitter: riscos vão além da desinformação](#), 27/03/2018. [Fake news: não repasse!](#), 21/03/2018. [Fake news, o mal da era digital](#), 31/08/2018. [Mensagens falsas e boatos tomam conta da internet](#), 13/03/2018. [Notícias falsas, ameaças reais](#), 19/03/2018. [Olho vivo: passo a passo para identificar fake news](#), 03/08/2018. [Ouça o podcast: debate sobre fake news](#). [Perigos digitais: como reconhecer uma fake news](#), 06/01/2017. [Plataformas sociais no combate às fake news](#), 20/09/2019. [Terceira idade conectada também está no alvo das fake news](#), 24/08/2018. [Você sabe o que é fake news?](#), 09/03/2018.

³⁶² VIVO - DIALOGANDO VIVO. [Smartphones: saiba o que fazer após ter o celular roubado](#), 28/10/2019.

³⁶³ VIVO - DIALOGANDO VIVO. [Exposição online: como compartilhar conteúdos nas redes sociais de maneira segura?](#), 28/02/2020.

³⁶⁴ VIVO - DIALOGANDO VIVO. [Como ter cuidado com o que meu filho acessa?](#), 13/10/2016. [Crianças na internet, cuidado redobrado](#), 21/02/2018. [Cuidados com a exposição dos filhos na internet](#), 04/04/2016. [Cyberbullying não é brincadeira de criança](#), 05/08/2016. [Existem riscos ao divulgar fotos dos filhos na internet?](#), 26/07/2017. [Exposição na internet: na medida, consciente e sem riscos](#), 11/10/2018. [Você publica fotos dos seus filhos na internet?](#), 27/04/2016.

³⁶⁵ INTERNATIONAL CONSUMER PROTECTION AND ENFORCEMENT NETWORK - ICPEN. econsumer.gov.

³⁶⁶ INTERNATIONAL CONSUMER PROTECTION AND ENFORCEMENT NETWORK - ICPEN. econsumer.gov.

- a) Um *site* público, atualmente disponível em alemão, coreano, espanhol, francês, inglês, japonês, polonês e turco, que permite a consumidores fazerem reclamações sobre fraudes internacionais³⁶⁷; e
- b) Um *site* seguro, hospedado por meio da plataforma Consumer Sentinel Network, da FTC, dos Estados Unidos, que permite, às autoridades policiais de todo o mundo, compartilhar e acessar dados de reclamações de consumidores e outras informações³⁶⁸.

Atualmente a iniciativa contempla 39 países membros de todos os continentes:

Tabela 2 - Países membros do *econsumer.gov*

PAÍSES			
Austrália	Espanha	Israel	Polônia
Bélgica	Estados Unidos	Itália	Quênia
Bulgária	Estônia	Japão	Reino Unido
Canadá	Filipinas	Letônia	República Dominicana
Chile	Finlândia	Lituânia	Suécia
Coreia do Sul	Gâmbia	México	Suíça
Costa Rica	Grécia	Nigéria	Suriname
Dinamarca	Holanda	Noruega	Turquia
Egito	Hungria	Nova Zelândia	Zâmbia
El Salvador	Irlanda	Peru	-

FONTE: INTERNATIONAL CONSUMER PROTECTION AND ENFORCEMENT NETWORK - ICPEN. econsumer.gov - Member Countries.

Na página principal, além de um vídeo instrutivo sobre como o sistema funciona, é disponibilizada uma relação de nove botões/*links* com acesso a páginas para efetuar as reclamações, cada um dentro de um tipo de golpe, conforme as seguintes definições:³⁶⁹

- Compras *on-line*/Serviços de internet/Computadores;
- Crédito e dívida;
- *Telemarketing* e *spam*;
- Empregos e ganhando dinheiro;
- Golpes de impostor: família, amigo, governo, negócios ou romance;
- Loteria, sorteios ou golpes de prêmios;
- Viagem e férias;
- Telefones/Dispositivos móveis e serviços de telefone; e

³⁶⁷ INTERNATIONAL CONSUMER PROTECTION AND ENFORCEMENT NETWORK - ICPEN. econsumer.gov - About US.

³⁶⁸ INTERNATIONAL CONSUMER PROTECTION AND ENFORCEMENT NETWORK - ICPEN. econsumer.gov - About US.

³⁶⁹ INTERNATIONAL CONSUMER PROTECTION AND ENFORCEMENT NETWORK (ICPEN). econsumer.gov.

- Outros.³⁷⁰

Ao acessar a página de reclamação do golpe específico, o usuário do sistema passará por uma árvore de filtros ou por uma breve pesquisa, a depender do caso, para classificar e especificar sua reclamação.

Além da área de reclamações, o *econsumer.gov* oferece informações na seção “News and data”, na qual é possível consultar notícias (*News*), alertas (*Alerts*) e tendências de reclamações (*Complaint Trends*)³⁷¹. Nesse último item são apresentados *links* para uma página externa ao *econsumer.gov*³⁷², na qual a FTC apresenta um relatório interativo com informações gerais sobre fraude internacional. O relatório apresenta, no formato de infográfico interativo, entre outras, informações sobre os principais tipos de golpes, os países de maior incidência e o valor de perdas monetárias, além de permitir a aplicação de alguns filtros, em especial de ano e trimestre.

Figura 4 - Visualização parcial do relatório sobre fraudes internacionais do *econsumer.gov* elaborado pela FTC



FONTE: TABLEU PUBLIC - FEDERAL TRADE COMMISSION. [econsumer.gov International Fraud Report](https://econsumer.gov/International-Fraud-Report). Acesso em: 14/09/2020.

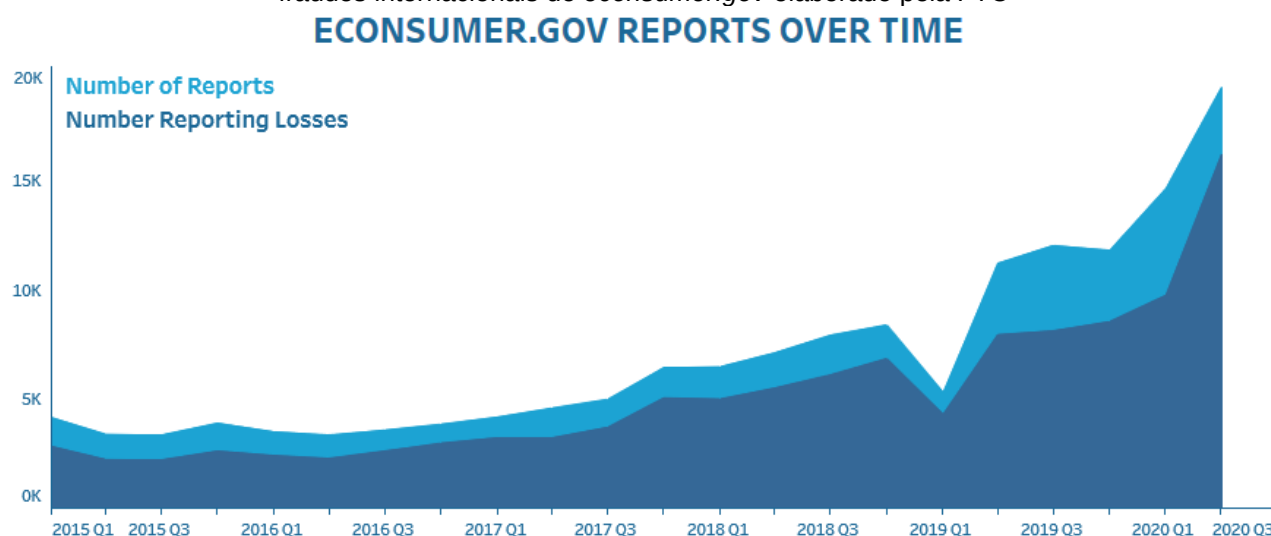
³⁷⁰ INTERNATIONAL CONSUMER PROTECTION AND ENFORCEMENT NETWORK - ICPEN. econsumer.gov.

³⁷¹ INTERNATIONAL CONSUMER PROTECTION AND ENFORCEMENT NETWORK (ICPEN). [econsumer.gov - News and data](https://econsumer.gov/News-and-data).

³⁷² TABLEU PUBLIC - FEDERAL TRADE COMMISSION. [econsumer.gov International Fraud Report](https://econsumer.gov/International-Fraud-Report).

Há também no relatório um gráfico com a evolução temporal, desde 2015, do número de reclamações e do número de reclamações que resultaram em perda financeira para as vítimas. Nesse gráfico pode-se perceber uma tendência de aumento no número de reclamações a partir do terceiro trimestre de 2016³⁷³. A partir do primeiro trimestre de 2020 essa alta parece intensificar-se³⁷⁴, o que pode ser resultado da pandemia do novo coronavírus, momento em que o mundo inteiro tem visto o aumento de golpes e fraudes, principalmente através da internet.

Figura 5 - Visualização do gráfico de evolução das reclamações do relatório sobre fraudes internacionais do *econsumer.gov* elaborado pela FTC



FONTE: TABLEU PUBLIC - FEDERAL TRADE COMMISSION. [econsumer.gov International Fraud Report](https://www.ftc.gov/econsumer.gov/International-Fraud-Report). Acesso em: 14/09/2020.

D. CONSIDERAÇÕES FINAIS

Tratou o presente estudo de analisar a prática de golpes e fraudes contra os consumidores de serviços de telecomunicações. Foi investigado como eles ocorrem³⁷⁵ e o que instituições governamentais e empresas privadas do setor têm feito na prevenção e repressão a essas práticas ilícitas e, principalmente, como vêm educando os consumidores para que não se tornem vítimas de aproveitadores.

Os golpes e fraudes se aproveitando dos consumidores dos serviços de telecomunicações, incluindo telefonia e internet, são universais e encontrados em maior ou menor escala em todos os países. No Reino Unido e Irlanda, tanto órgãos reguladores, quanto as maiores prestadoras de

³⁷³ No primeiro trimestre de 2019 há uma queda acentuada no número de reclamações, mas o relatório traz a observação que entre 28 de dezembro de 2018 e 26 de janeiro de 2019 os portais de recebimento de reclamações estiveram indisponíveis devido a paralisação do governo dos Estados Unidos. TABLEU PUBLIC - FEDERAL TRADE COMMISSION. [econsumer.gov International Fraud Report](https://www.ftc.gov/econsumer.gov/International-Fraud-Report).

³⁷⁴ TABLEU PUBLIC - FEDERAL TRADE COMMISSION. [econsumer.gov International Fraud Report](https://www.ftc.gov/econsumer.gov/International-Fraud-Report).

³⁷⁵ Tema do primeiro estudo desta série: [Estudo - Golpes e fraudes contra o consumidor de telecom - Parte 1 - Identificação de casos na Europa, Estados Unidos e Brasil](#).

serviços de telecomunicações trazem informações ao consumidor, em variados graus de aprofundamento, enquanto, na Dinamarca, a informação ao consumidor está concentrada no setor privado e não no órgão regulador. Nos Estados Unidos, são várias as instituições mobilizadas no combate e disseminação de informações sobre golpes e fraudes, com destaque, no setor de telecomunicações, para a Federal Communications Commission (FCC) e a Federal Trade Commission (FTC). No Brasil, esta Agência Nacional de Telecomunicações tem ativamente se engajado em educação para o consumo abordando essa temática, havendo também iniciativas de outros órgãos governamentais, como Senacon, Procons e Ministérios Públicos; de órgão multissetorial, o Comitê Gestor da Internet no Brasil (CGI.br); da sociedade civil, como a SaferNet Brasil e o Idec; bem como das cinco maiores prestadoras de serviços de telecomunicações do país.

No que tange ao arranjo institucional de controle e repressão a golpes e fraudes, analisado de forma breve no presente trabalho, pode-se ver que no Reino Unido e nos Estados Unidos há uma concentração sobre reporte de golpes e fraudes. No caso do Reino Unido, o Action Fraud (<https://www.actionfraud.police.uk/>) recebe os relatos de golpes, fraudes e crimes cibernéticos em geral, enquanto nos Estados Unidos a FTC recebe comunicações em página específica sobre roubo de identidade (<https://www.identitytheft.gov/>) e o Federal Bureau of Investigation (FBI) o faz sobre golpes e fraudes perpetrados por meio da internet (<https://www.ic3.gov/>). No Brasil, por seu turno, não se verificou uma iniciativa centralizada de reporte desses tipos de embustes.

Relativamente à investigação e repressão, no Reino Unido, na perspectiva nacional, o National Fraud Intelligence Bureau (NFIB), que gere o Action Fraud junto com a polícia de Londres, foca-se em gerar inteligência sobre os relatos recebidos por meio do Action Fraud e os encaminhar a agências/forças policiais para investigação. O órgão também possui poderes de *enforcement* para realizar algumas ações contra fraudadores. Nos Estados Unidos, no panorama nacional, o FBI tem *enforcement* para fazer cumprir as leis criminais do país, tendo entre suas atribuições a investigação de fraudes em geral e fraudes cometidas por meio da internet³⁷⁶. A FTC, que é a única agência federal com jurisdição geral sobre a fraude contra o consumidor, e a FCC, que é responsável pela implementação e aplicação das leis e regulamentos de comunicações, têm poderes investigativos, mas não de imputação criminal. Todavia, essas agências cooperam de forma próxima com órgãos governamentais e forças policiais que têm esse poder de *enforcement* criminal. No Brasil, sem se adentrar em pormenORIZAÇÕES, as polícias estaduais são primariamente as responsáveis pela condução de investigações e, como se viu, nem todas as Unidades da Federação possuem delegacias especializadas em crimes cibernéticos e crimes contra o consumidor.

De forma geral, nas realidades aqui estudadas - Reino Unido, Irlanda, Dinamarca, Estados Unidos e Brasil - pode-se ver que as agências governamentais estão, à exceção da Dinamarca,

³⁷⁶ Não se analisou aqui o papel das forças policiais e locais nos Estados Unidos, mas pelas informações pesquisadas sobre o FBI, pode-se inferir que há um nível de cooperação entre o Birô e esses órgãos policiais.

atentas ao cenário dinâmico de golpes e fraudes que visam o consumidor de telecomunicações, bem como as maiores prestadoras desses serviços também tem se atentado para esse campo. Nesse sentido, nos países aqui pesquisados há medidas em curso para prevenir, reprimir e informar os consumidores sobre essas práticas. A própria iniciativa internacional do *econsumer.gov*, integrado por 39 países espalhados pelos cinco continentes, é um demonstrativo do esforço que os golpes e fraudes têm mobilizado, bem como é uma indicação de que essas práticas ilícitas são um flagelo disseminado internacionalmente.