CUIDADO, PODE SER GOLPE!

Aeda Valle Cavalcante[1]
Alicia Alves da Silva Matheus[2]
Amanda Rodrigues de Sousa[3]
Clara Mendes Ribeiro[4]
Emilly de Paiva Farias[5]
Felipe Xavier[6]
Jhonathan Andrade da Costa[7]
Rhaíssa Barbosa Babolin[8]
Tâmyla Oliveira de Sousa Dias[9]

Resumo

A presente pesquisa teórica foi realizada com o objetivo de embasar a atividade extensionista que será realizada no âmbito da disciplina "Direito Digital", sob a orientação do Prof. Dr. Henrique Savonitti Miranda.

Os ataques cibernéticos estão cada vez mais frequentes, apesar de alguns subestimarem pessoas vítimas de golpe digital. Hoje em dia, é essencial ter mais cuidado ao acessar a internet com inúmeras plataformas que encontramos. Vale ressaltar que grande parte das vítimas são idosos, que ao tentar se adaptar à “era digital”, são os principais afetados pela má conduta dos que praticam os crimes digitais.

A ambição financeira das pessoas que cometem tais atos é tão grande, que são diversos alertas de empresas para a população ter mais cautela ao acessar

[1] Graduanda em *Direito* pelo Centro Universitário UniProcessus.
[2] Graduanda em *Direito* pelo Centro Universitário UniProcessus.
[3] Graduanda em *Direito* pelo Centro Universitário UniProcessus.
[4] Graduanda em *Serviços Jurídicos e Cartoriais* pelo Centro Universitário UniProcessus.
[5] Graduanda em *Direito* pelo Centro Universitário UniProcessus.
[6] Graduando em *Direito* pelo Centro Universitário UniProcessus.
[7] Graduando em *Direito* pelo Centro Universitário UniProcessus.
[8] Graduanda em *Direito* pelo Centro Universitário UniProcessus.
[9] Graduanda em *Direito* pelo Centro Universitário UniProcessus.

algumas páginas, links e etc. Muitas vezes, esses indivíduos criam atalhos por meio dessas plataformas digitais e realizam roubo de senhas, cartões e informações confidenciais e pessoais.

Neste trabalho, serão abordadas questões relacionadas ao estelionato digital, as formas que são realizadas, bem como as maneiras eficazes na proteção e diminuição dos riscos e as medidas cabíveis após a vitimização.

1. Introdução

Viver em uma era digital, por vezes, pode parecer um trabalho árduo, apesar de todas as facilidades que esta proporciona ao mundo. Com o constante desenvolvimento tecno-científico na sociedade, naturalmente, grande parte dos procedimentos corriqueiros de aspecto financeiro seriam facilmente resolvidos por meio de ferramentas on-line e outros dispositivos tecnológicos. Contudo, ao mesmo tempo em que há celeridade na resolução de tratativas que antes eram burocratizadas e de caráter conhecidamente moroso, aumenta-se o enorme desafio que é tomar medidas necessárias de precaução diante da imensa variedade de golpes que são aplicados diariamente na esfera virtual.

O caráter humano e as expertises corrompidas estão inerentes a todos os usuários da tecnologia e é compreensível a cautela ao tratar-se de pessoas vulneráveis e suscetíveis ao risco. Cada vez mais, os autores por trás dessas práticas criminosas, também conhecidas como estelionato digital, utilizam-se de artilharias ilícitas e mecanismos aprimorados para violação de dispositivos e obtenção de dados essenciais da vida privada de suas vítimas, que despercebidamente entram para a estatística daqueles que se encontram como alvos abatidos diante de um golpe financeiro imprevisível.

Ocorre que grande parcela da população afetada por estes crimes virtuais é composta por consumidores tecnológicos sem o adequado “letramento digital”, ou seja, que estejam em maior probabilidade de serem ludibriadas com o surgimento dessas novas ferramentas tecnológicas, como a população idosa, por exemplo.

2. Desenvolvimento do tema pesquisado

2.1. Definição e estatísticas

O primeiro passo de nossa jornada é a definição do que é fraude eletrônica, estelionato digital ou "cyber estelionato". Quase todos nós conhecemos alguém que foi vítima de um golpe praticado por um estelionatário. O tão conhecido crime de estelionato descrito no artigo 171 do Código Penal:

"Art. 171 - Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento:

Pena - reclusão, de um a cinco anos, e multa, de quinhentos mil réis a dez contos de réis. (Vide Lei nº 7.209, de 1984)".

Com o avanço da tecnologia e popularização no uso de celulares e computadores, os criminosos passaram a utilizar vários meios eletrônicos para a aplicação dos golpes. "*(...) A fraude eletrônica ocorre quando o criminoso consegue enganar alguém, por meio de redes sociais, contatos telefônicos, correio eletrônico falso ou qualquer outro meio fraudulento, a fornecer dados confidenciais, tais como, senhas de acesso, bancos ou número de cartão de crédito ou débito*." Disponível em: https://www.tjdft.jus.br/institucional/imprensa/campanhas-e-produtos/direito-facil/edicao-semanal/estelionato-1#:~:text=Para%20tentar%20coibir%20esse%20tipo,isso%20recebe%20pena%20mais%20severa. (Acesso em: 18, mar. 2024.)

Em razão do aumento dos golpes eletrônicos e visando coibir esse tipo de crime, o Código Penal foi alterado pela Lei nº 14.155/2021, com a inclusão de alguns dispositivos:

"Art. 154-A. Invadir dispositivo informático de uso alheio, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita:

Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa.

.....

§ 2º Aumenta-se a pena de 1/3 (um terço) a 2/3 (dois terços) se da invasão resultar prejuízo econômico."

➔ FRAUDE ELETRÔNICA

"*Art. 171, § 2º-A. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se a fraude é cometida com a utilização de informações fornecidas pela vítima ou por terceiro induzido a erro por meio de redes sociais, contatos telefônicos ou envio de correio eletrônico fraudulento, ou por qualquer outro meio fraudulento análogo. (Incluído pela Lei nº 14.155, de 2021)*

§ 2º-B. A pena prevista no § 2º-A deste artigo, considerada a relevância do resultado gravoso, aumenta-se de 1/3 (um terço) a 2/3 (dois terços), se o crime é praticado mediante a utilização de servidor mantido fora do território nacional. (Incluído pela Lei nº 14.155, de 2021)"

Recentemente, a Comissão de Constituição e Justiça e de Cidadania da Câmara dos Deputados - CCJ aprovou Projeto de Lei nº 2339/23, de relatoria do Deputado Junior Mano (PL-CE), que prevê a figura do estelionato digital como crime no Código Penal brasileiro:

➔ ESTELIONATO DIGITAL (acréscimo § 2º- C ao art. 171 do CP)

"§ 2º-C. Incorre nas mesmas penas do § 2º-A quem:

I – utilizando-se de plataforma digital na rede mundial de computadores, alcança ou incrementa a projeção de atividade, marca, produto, serviço, pessoa ou interesse, induzindo ou mantendo em erro alguém interessado na obtenção de renda extra, que, embora cumpra com os compromissos assumidos, deixa de receber valor que lhe é prometido;

II – abusando da confiança de seguidor em plataforma digital, aplicativo ou rede social, alicia alguém para o ingresso em programa de renda extra fraudulento." https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=2303602&filename=Tramitacao-PL%202339/2023 (Acesso em 18, mar.2024)

A Deputada Rosângela Moro (União-SP), relatora do Projeto submetido à CCJ, exemplifica o que poderia ser considerado estelionato digital. *"Tomemos como exemplo a recente notícia do 'golpe do InstaMoney', que promete pagamento por curtidas e tem o mesmo modus operandi de fraudes em plataformas como Netflix, Tiktok Pay e Play Premiado", informa a parlamentar. "Nessa prática, o InstaMoney engana usuários que, após assistirem a anúncio fraudulento no YouTube, adquirem suposto aplicativo por R$ 147 na esperança de ganhar até R$ 200 por dia e conquistar a independência financeira apenas por curtir publicações no Instagram."*https://www.camara.leg.br/noticias/1015065-comissao-aprova-pena-de-4-a-8-anos-para-estelionato-digital/(Acesso em 18,mar.2024).

Em que pese a previsão no aumento da pena para os crimes virtuais – no estelionato comum a pena é de 1 a 5 anos de reclusão, na fraude eletrônica, é de 4 a 8 anos, fato é que as estatísticas das vítimas do referido tipo penal aumentam.

Segundo notícia divulgada na revista Veja, as fraudes digitais são consideradas "crime da moda": *"esse tipo de estelionato cravou uma marca impressionante em 2022, segundo o Anuário Brasileiro de Segurança Pública: foram 200.322 registros, 66% a mais em relação ao ano anterior. O aumento foi alavancado pelo furto e roubo de quase 1 milhão de celulares no ano, uma alta de 17% sobre 2021."*

Na reportagem afirma ainda que *"o fenômeno se deve ao maior uso da internet desde a pandemia para rotinas de trabalho, compras, movimentações financeiras e manutenção dos laços de amizade. "Isso criou um ambiente propício para que criminosos explorasse as vulnerabilidades nesses sistemas", afirma o sociólogo David Marques, Coordenador do Fórum Brasileiro de Segurança pública*." https://veja.abril.com.br/brasil/considerado-o-crime-da-moda-estelionato-digital-cresce-no-brasil (Acesso em 18, mar.2024)

De acordo com os dados do referido Anuário Brasileiro de Segurança Pública de 2023, disponibilizado na rede mundial de computadores em: https://forumseguranca.org.br/wp-content/uploads/2023/07/anuario-2023.pdf , verifica-se um grande aumento nos crimes de estelionato, em especial os praticados por meio eletrônico, conforme verificado na tabela anexa:

TABELA 15

Estelionato e Estelionato por meio eletrônico [1]

Brasil e Unidades da Federação – 2021-2022

Brasil e Unidades da Federação	Estelionato					Estelionato por meio eletrônico				
	Ns. Absolutos		Taxas [2]		Variação (%)	Ns. Absolutos		Taxas [2]		Variação (%)
	2021 [3]	2022	2021	2022		2021 [3]	2022	2021	2022	
Brasil	**1.312.964**	**1.819.409**	**649,9**	**896,0**	**37,9**	**120.470**	**200.322**	**115,0**	**189,9**	**65,2**
Acre	4.357	5.643	530,1	679,9	28,3	50	153	6,1	18,4	203,0
Alagoas	16.745	19.914	535,5	636,7	18,9	3.319	4.911	106,1	157,0	47,9
Amapá	5.875	7.596	806,8	1.035,6	28,4	78	374	10,7	51,0	376,0
Amazonas	10.385	15.397	266,1	390,7	46,8	95	404	2,4	10,3	321,2
Bahia	57.231	86.950	405,1	615,1	51,8	...	...	...	...	...
Ceará	57.089	68.754	651,4	782,0	20,0	...	...	...	...	...
Distrito Federal	40.596	51.617	1.451,7	1.832,3	26,2	10.049	15.580	359,3	553,1	53,9
Espírito Santo	29.909	37.391	785,6	975,4	24,2	10.545	15.277	277,0	398,5	43,9
Goiás	57.125	72.579	819,9	1.028,7	25,5	128	1.461	1,8	20,7	1.027,2
Maranhão	9.583	15.047	141,8	222,1	56,6	1.291	6.724	19,1	99,2	419,6
Mato Grosso	15.768	20.261	437,2	553,8	26,7	6.576	9.253	182,3	252,9	38,7
Mato Grosso do Sul	11.608	13.332	425,0	483,6	13,8	910	2.524	33,3	91,6	174,8
Minas Gerais	105.476	130.755	515,5	636,6	23,5	25.574	35.749	125,0	174,1	39,3
Pará	31.686	35.029	392,6	431,6	9,9	2.344	12.988	29,0	160,0	451,1
Paraíba	3.994	5.669	100,9	142,6	41,3	67	406	1,7	10,2	503,3
Paraná	114.951	134.154	1.011,9	1.172,3	15,9	1.890	5.685	16,6	49,7	198,6
Pernambuco	52.240	58.239	578,1	642,9	11,2	9.843	14.060	108,9	155,2	42,5
Piauí	13.269	14.184	407,4	433,9	6,5	65	246	2,0	7,5	277,0
Rio de Janeiro	71.145	123.841	443,3	771,4	74,0	...	...	...	...	...
Rio Grande do Norte	20.212	23.991	614,1	726,5	18,3	...	...	...	...	...
Rio Grande do Sul	91.792	93.864	844,8	862,7	2,1	...	...	...	...	...
Rondônia	10.770	15.568	681,9	984,7	44,4	2.787	5.932	176,5	375,2	112,6
Roraima	3.989	5.209	642,5	818,6	27,4	59	759	9,5	119,3	1.155,1
Santa Catarina	70.300	95.100	937,8	1.249,7	33,3	42.976	64.230	573,3	844,1	47,2
São Paulo [4]	382.110	638.629	865,3	1.437,7	66,1	...	...	...	...	...
Sergipe	15.754	19.216	716,8	869,7	21,3	80	432	3,6	19,6	437,1
Tocantins	9.005	11.480	600,0	759,5	26,6	1.744	3.174	116,2	210,0	80,7

Fonte: Secretarias Estaduais de Segurança Pública e/ou Defesa Social; Instituto de Segurança Pública/RJ (ISP); Polícia Civil do Estado do Amapá; Polícia Civil do Distrito Federal; Polícia Civil do Estado de Roraima; Estimativas da população residente no Brasil e Unidades da Federação - IBGE, realizadas por meio de interpolação linear; Censo 2022 - IBGE; Fórum Brasileiro de Segurança Pública.

(...) Informação não disponível.

(1) Em 2021, o crime de Estelionato - Fraude eletrônica passou a ser tipificado pelos parágrafos 2ºA, 2ºB e 3º do art. 171 do Código Penal.

(2) Taxas por 100 mil habitantes.

(3) Atualização das informações publicadas no Anuário Brasileiro de Segurança Pública, ano 16, 2022.

(4) Para a tipificação de Estelionato, o Estado registra os casos tentados ou consumados.

Uma vez que a coibição dos crimes não é eficaz com a edição de novas leis que majoram a penalidade, mais importante se torna o alerta e conscientização da comunidade para a prevenção dos crimes cometidos por estelionatários .

2.2. Dos diversos tipos de golpes e meios de prevenção

Há nesse rol de crimes virtuais subdivisões com seus devidos conceitos, que devem ser meticulosamente compreendidos para a adoção das medidas apropriadas de prevenção conforme seu tipo.

➔ O GOLPE DO PAGAMENTO POR APROXIMAÇÃO (MAQUININHAS DE CARTÕES)

Modus Operandi: O contato ocorre com a cartela de clientes de determinada empresa, que acredita estar sendo orientada por funcionários da companhia responsável pelas máquinas de cartões. Desse modo, o golpista informa a necessidade de manutenção no sistema instalado no computador da vítima. Essa falsa manutenção resulta na invasão por vírus que autoriza aos criminosos o acesso remoto à máquina de cartões. Com isso, provoca falha nos pagamentos por aproximação e aparição de mensagem de erro no procedimento, induzindo o cliente a realizar pagamentos por inserção do cartão físico, momento em que são roubados os dados do cartão e, seguidamente, sua clonagem.

Medidas de proteção:

1. Em caso de erro ao tentar realizar pagamento por aproximação, solicite ao lojista uma maquininha alternativa para nova tentativa. Em caso de negativa, realize o pagamento via pix ou dinheiro. Evite inserir o cartão físico na máquina.

2. Verifique periodicamente as faturas de seu cartão de crédito e esteja atento à possibilidade de haver algum valor indevido. Ao notar algo distinto do

planejado, entre em contato com a instituição financeira por meio do número indicado no cartão físico para obter informação verídica.

3. Em uma possível interação dos fornecedores do aparelho, os lojistas devem atentar à origem do contato. Indica-se, sobretudo, caso comunicado uma suposta manutenção a ser realizada, que busque contato direto com a empresa do cartão, se possível, por outro aparelho celular.

"BRASIL. Disponível em: https://admin.pc.rs.gov.br/upload/arquivos/202304/04121500-cartilha-golpes-na-internet-atualizada-compressed.pdf Acesso em: 18 Mar. 2024"

➔ GOLPE EM SITE DE COMPRAS ONLINE E CLONAGEM DO WHATSAPP

Modus Operandi: Trata-se de golpe que tem como finalidade enganar pessoas que publicam algum anúncio em sites de vendas como OLX, por exemplo. Geralmente, consta no anúncio um número de telefone para contato. Por meio do telefone informado, o golpista envia uma mensagem de texto e alega necessitar de uma atualização de cadastro no site em questão. A suposta validação ocorre com envio de código pelo sms. Porém, o código enviado se refere ao número de validação do whatsapp da própria pessoa que realiza o anúncio. Quando informa o código ao meliante, é liberado o acesso à conta do aplicativo do whatsapp que fica clonado. Com a posse dos dados, os golpistas utilizam o perfil da vítima para aplicar armadilhas virtuais no âmbito financeiro aos contatos de sua agenda. Solicitam empréstimos e transferências bancárias aos contatos, que realizam a transferência para a conta do criminoso, acreditando conversar com a pessoa conhecida.

Medidas de proteção:

1. Utilizar os meios de segurança disponíveis nos aplicativos de mensagens, como a verificação em mais de uma etapa, são imprescindíveis para evitar a invasão criminosa.

2. Ao ser solicitada atualização de cadastro, verificar diretamente no site em que o anúncio foi publicado para averiguar a veracidade da demanda comunicada.

3. Não encaminhar a outrem nenhum código recebido privativamente por mensagem de texto sem antes analisar os riscos de uma apropriação de dados pessoais.

4. Na eventualidade de cair nesse golpe, especificamente, encaminhar mensagem para o endereço de e-mail oficial do aplicativo whatsapp e solicitar a desativação da conta, a fim de impedir a continuidade da aplicação dos golpes aos contatos da agenda.

5. Em contrapartida, se algum contato solicitar algum empréstimo via mensagem de whatsapp, o recomendado é realizar chamada telefônica para conversar diretamente com a pessoa e confirmar sobre a procedência do pedido.

"BRASIL. Disponível em: https://admin.pc.rs.gov.br/upload/arquivos/202304/04121500-cartilha-golpes-na-internet-atualizada-compressed.pdf Acesso em: 18 Mar. 2024"

➔ GOLPE DO FALSO SITE DE INTERNET

Modus Operandi: Com a facilidade em localizar grande variedade de produtos na internet, nesse tipo de golpe são criadas cópias de sites reconhecidamente confiáveis pela população. Altera-se minimamente algum detalhe da URL de acesso ao site original. Geralmente a aparência da página é idêntica ou muito semelhante aos sites conhecidos pela vítima, de modo a ludibriar quase imperceptivelmente seu público-alvo, que apenas se dará conta tardiamente do que sucedeu. Ocorre com facilidade nos anúncios de promoções supostamente imperdíveis, principalmente na venda de eletrodomésticos e aparelhos eletrônicos.

Medidas de proteção:

1. Analisar cuidadosamente o site eletrônico de acesso, sobretudo, os de empresas conhecidas, pois elas costumam ser os principais alvos para atrair novas vítimas neste esquema impostor.

2. Buscar a localização do selo de segurança ao final da página de navegação, pois este selo é essencial para tranquilizar o consumidor acerca da autenticidade do site.

3. Desconfiar de valores promocionais discrepantes quando comparados aos valores praticados normalmente no comércio.

4. Utilizar sites que detectam a autenticidade de sites seguros como o "siteconfiavel.com.br" e "reclameaqui.com.br".

"BRASIL. Disponível em: https://admin.pc.rs.gov.br/upload/arquivos/202304/04121500-cartilha-golpes-na-internet-atualizada-compressed.pdf Acesso em: 18 Mar. 2024"

➔ GOLPE DO PIX

Modus Operandi: Nesse tipo de golpe, o agente criminoso geralmente entra em contato com a potencial vítima por telefone passando-se por um representante bancário. Após esse contato inicial, ele declara que houve o bloqueio da conta bancária por razões atreladas a diversas tentativas de invasão do dispositivo por terceiros e garante ágil resolução da suposta problemática. Uma das principais características desse golpe é a utilização de informações verdadeiras quanto às transações realizadas na conta do usuário. Porém, nessa listagem das transações informadas pelo estelionatário digital, haverá a menção de um valor não reconhecido pela vítima e que não foi realizado por ela. Esse é justamente o valor que o criminoso objetiva arrecadar. Com isso, o agente delitivo informará sobre a necessidade do cliente enviar um PIX de mesmo valor (PIX duplicado do valor não reconhecido) para que haja o cancelamento/anulação pela "instituição financeira" do suposto ato realizado pelo consumidor, valor este que será encaminhado para a conta bancária do criminoso por meio da chave PIX encaminhada para a vítima mediante mensagem.

Medidas de proteção:

1. Ao receber ligação suspeita, encerre a chamada e busque entrar em contato com telefone oficial para sanar possíveis dúvidas, de preferência por meio de outro celular.

2. Não informar quaisquer dados sigilosos por telefone, ainda que aparentam ter conhecimento de seus dados pessoais. Vale ressaltar que pode ter ocorrido o vazamento de seus dados privados por empresas fornecedoras de serviços.

3. Não entrar em links recebidos por whatsapp e sms sem saber a real procedência do link disponibilizado.

"BRASIL. Disponível em: https://admin.pc.rs.gov.br/upload/arquivos/202304/04121500-cartilha-golpes-na-internet-atualizada-compressed.pdf (Acesso em: 18 Mar. 2024)

BRASIL. Disponível em: https://www.serasa.com.br/premium/blog/golpes-do-pix-como-se-proteger/ (Acesso em: 19 Mar. 2024)"

➔ GOLPE DO FALSO BOLETO

Modus Operandi: Essa modalidade funciona com o uso de boletos bancários emitidos de forma fraudulenta com código de barras modificado por meio de um site de loja online de mesma natureza (fraudulento). O contato também pode ser realizado, por parte dos criminosos, via whatsapp, oferecendo prestação de serviços inexistentes. As características do documento supracitado são trabalhadas de forma que não haja, por parte do cliente, dúvidas ou desconfianças quanto à veracidade do boleto, pois possui aspecto visual semelhante ao padrão emitido pela loja.

Medidas de proteção:

1. Apurar cuidadosamente se os dados que constam no boleto condizem com aqueles relacionados à empresa contratada. E se o destinatário possui o CNPJ informado em meios oficiais.

2. Ao realizar a emissão de segunda via do boleto, se dirigir diretamente ao site oficial do credor para não incorrer em tentativa de fraude.

"BRASIL. Disponível em: https://admin.pc.rs.gov.br/upload/arquivos/202304/04121500-cartilha-golpes-na-internet-atualizada-compressed.pdf Acesso em: 18 Mar. 2024"

➔ GOLPE DA FALSA CENTRAL DE ATENDIMENTO

Modus Operandi: O golpe em questão tem início quando o estelionatário atua forjando ser colaborador de determinado grupo financeiro, alegando existir alguma pendência ou atualização de cadastro a ser realizada com relativa urgência na conta bancária da vítima. Este acaba por fornecer as informações que lhe foram solicitadas. A partir disso, munido desses dados confidenciais, o golpista consegue realizar operações bancárias ilegítimas.

Medidas de Proteção:

1. Desconfiar de ligações recebidas que solicitem dados pessoais ou senhas de acesso a contas bancárias, pois não são condutas usuais de instituições financeiras. Portanto, caso a ligação não tenha se originado no seu aparelho, não digite senha ou número de cartão de crédito em hipótese alguma. Ainda que o banco entre em contato para verificar alguma movimentação inusitada, não perguntarão dados sigilosos em via telefônica.

2. Não realizar chamadas para números de telefone fornecidos via mensagens. Busque através de seu cartão físico o número SAC que está contido na parte de trás do cartão para tirar suas dúvidas com os verdadeiros canais oficiais da instituição.

"BRASIL. Disponível em: https://blog.bb.com.br/golpe-0800/ Acesso em: 19 Mar. 2024"

➔ GOLPE UTILIZANDO INTELIGÊNCIA ARTIFICIAL

Modus Operandi: Na busca do aprimoramento das práticas criminosas, grupos têm atuado com maior refinamento na prática de golpes atrelados ao uso de mecanismos tecnológicos. Ou seja, utilizam-se de sites que elaboram textos dentro dos padrões gramaticais, com a coerência esperada de instituições reconhecidas. Desse modo, percebe-se maior dificuldade entre os clientes em distinguir se a comunicação recebida é oficialmente emanada de instituições financeiras ou se provém de impostores que buscam auferir vantagens lucrativas via depósito bancário e transferências diversas .

Além disso, com o advento dessa tecnologia, as possibilidades de fraude se ampliam e não se restringem ao âmbito textual, pois agora torna-se sob alcance a modificação vocal e facial, com utilização de imagens e vídeos alterados em tempo real, ampliando os recursos empregados nas condutas delitivas.

Nesse sentido, o golpe que faz uso de inteligência artificial (IA) traz entre suas possibilidades a hipótese de produção de e-mail, realização de vídeo-chamadas com cenários e personagens fictícios, adulteração de áudios, bem como vídeos, imagens e outras formas de comunicação que tenham aspectos ligados aos recursos presentes no ambiente da IA. Resumidamente, é o uso da ferramenta artificial nos elementos anteriores a ela e isso se dá com finalidade diversa do que preconiza todo o arcabouço legal brasileiro.

Medidas de proteção:

1. Verificar a autenticidade dos dados obtidos, utilizando-se de mais de uma fonte que ratifique a real procedência da informação adquirida. Em casos de suspeita de clonagem de voz por meio de áudios, buscar um contato direto com o remetente da mensagem comunicada para averiguar a veracidade.

2. Proteja dados vulneráveis, porquanto menos informações pessoais expostas nas redes sociais, melhor para a manutenção da segurança digital, e por conseguinte, a redução de possíveis ataques cibernéticos.

“BRASIL. Disponível em: https://tiinside.com.br/23/08/2023/os-riscos-do-golpe-de-clonagem-de-voz-protecao-contra-uma-ameaca-emergente/ Acesso em: 20 Mar. 2024

BRASIL. Disponível em: https://forbes.com.br/forbes-money/2023/09/por-que-a-ia-pode-tornar-os-crimes-digitais-mais-eficientes/ Acesso em: 19 Mar. 2024 ”

2.3 - Da prevenção e formas de proteção

Consoante o Instituto de Defesa de Consumidores – Idec, que fornece dicas em seu sítio eletrônico de como não cair em golpes, o primeiro cuidado que deve-se ter é com o vazamento de dados pessoais. Menciona o grande número de vazamento de dados como nome, CPF, endereço, telefone, número de cartão, etc. que ocorrem esporadicamente. Elucida que alguns dados de usuários do *WhatsApp* podem, eventualmente, ser distribuídos entre as empresas do grupo Meta (Facebook, Instagram, Messenger), que por sua vez são direcionados para publicidade de empresas. Ao autorizar o compartilhamento dessas informações, o usuário torna-se um alvo fácil de golpes. Dito isso, a primeira dica é: negar as solicitações, ou seja, não autorizar o fornecimento de dados não obrigatórios ou apagar os dados das redes sociais, que são as principais responsáveis pelo fornecimento de informações pessoais que acabam nas mãos dos golpistas. Por isso é importante sempre ler os termos das autorizações.

Outro ponto crucial da matéria é que deve-se desconfiar de tudo e manter a calma. Criminosos utilizam gatilhos psicológicos para desestabilizar as pessoas para tomar decisões e praticar ações inconscientes e desarrazoadas. Os principais gatilhos são:

Urgência: com o objetivo da pessoa tomar uma decisão rápida e sem pensar direito. Como por exemplo o golpe do cartão clonado que precisa urgentemente ser bloqueado;

Compromisso: o estelionatário estabelece algum relacionamento com a vítima para prolongar a conversa e cansá-la. Como por exemplo o golpe do falso empréstimo;

Reciprocidade: o criminoso inventa uma falsa situação em que ajuda a vítima a resolver um problema para depois negociar uma ajuda;

Autoridade: o golpista finge ser uma autoridade do tipo gerente, supervisor, servidor da Receita Federal, etc. para explorar a tendência de obediência.

Sabendo da existência dos gatilhos psicológicos utilizados pelos criminosos, é importante não tomar decisão no momento, manter a calma e não fornecer informações.

BRASIL. Disponível em: https://www.gov.br/investidor/pt-br/penso-logo-invisto/prevencao-de-fraudes-financeiras-estrategias-e-medidas-de-protecao Acesso em: 16 Mar. 2024

2.3 - Medidas cabíveis às vítimas de um golpe digital

Vimos algumas dicas acima sobre como evitar cair em golpes. No entanto, caso seja vítima, existem medidas a serem adotadas. Para isso, existem as leis, como o Código de Defesa do Consumidor, que pode ser utilizado, por exemplo, quando o golpe foi facilitado por causa de falha de segurança do banco. O site consumidor.gov.br é uma ótima ferramenta para solucionar algumas demandas.

Outra possibilidade é utilizar o site do Banco Central para fazer reclamação. Por fim, pode-se acionar o Juizado Especial, que não precisa de advogado e não há pagamento de custas processuais, para os valores de causas que não ultrapassem 20 salários mínimos.

BRASIL. Disponível em: https://www.jusbrasil.com.br/artigos/cai-em-um-golpe-e-agora/2036433685 Acesso em: 19 Mar. 2024

BRASIL. Disponível em: https://www.jusbrasil.com.br/artigos/foi-vitima-de-golpe-virtual-saiba-como-proceder/918848086 Acesso em: 20 Mar. 2024

2.4 - Dicas gerais do que pode ser feito ao descobrir que foi vítima de um golpe

1. Entre em contato imediatamente com o banco para pedir o bloqueio do cartão. Caso você tenha acesso ao aplicativo, é possível que esse bloqueio seja feito por lá também.
2. Faça um boletim de ocorrência de forma presencial ou online pelo sistema Sinesp Delegacia Virtual (DEVIR).

3. Informe a empresa responsável pela maquininha a respeito do ocorrido. (se o golpe em questão envolver maquininha de cartão de crédito).
4. Caso o golpe tenha sido pelo whatsapp, entre em contato com o suporte do aplicativo e peça para desativar sua conta temporariamente.
5. Avise seus familiares e amigos.
6. Entre em contato com o banco para tentar cancelar a compra feita.
7. Guarde todas as evidências que você tenha.Tire print de toda conversa, dos comprovantes de pagamento com os dados da transação.
8. Informe o ocorrido ao banco e peça para que eles acionem o MED, Mecanismo Especial de Devolução, criado pelo Banco Central.

“BRASIL. Disponível em: https://www.jusbrasil.com.br/artigos/cai-em-um-golpe-e-agora/2036433685 Acesso em: 19 Mar. 2024

BRASIL. Disponível em: https://www.jusbrasil.com.br/artigos/foi-vitima-de-golpe-virtual-saiba-como-proceder/918848086 Acesso em: 20 Mar. 2024”

3. Considerações Finais

Em um mundo cada vez mais virtual, os dispositivos eletrônicos são peças chaves para a prática de crimes eletrônicos. Como não é mais possível viver sem a utilização da internet, smartphones, aplicativos, whatsapp, etc., é de suma importância conhecer os mecanismos de prevenção aos diversos tipos de golpes que diuturnamente vitimam várias pessoas.

Dessa forma, nosso trabalho discorreu sobre alguns golpes que costumam causar danos financeiros à sociedade e com isso colaborar para o conhecimento das armadilhas que nos cercam. Com as orientações sobre os principais golpes aplicados na atualidade, aumentam-se as chances de defesa.

No entanto, por mais que se descreva extensivamente e minuciosamente os diversos tipos de golpes, fato é que a cada dia aparecem novas modalidades. Seria impossível estudar todos os golpes. Por isso, é importante alertar sobre os gatilhos que os criminosos utilizam para enganar, como a urgência das ações, impedindo o raciocínio lógico ou auto-controle. Grande parte das pessoas que são ludibriadas não

foram ingênuas ou pouco inteligentes. Muitas vezes não observaram os detalhes ou algo estranho, pois estavam acostumadas a realizar ações de forma automática.

Não menos importante, abordamos sobre questões práticas de como as vítimas devem agir nos casos em que sofreram alguma lesão patrimonial, como registrar um boletim de ocorrência, acionar os órgãos de defesa do consumidor e até mesmo o Poder Judiciário.

Apesar das leis relacionadas aos crimes cibernéticos serem mais rígidas, isso não é suficiente para eliminar a conduta criminosa. Os casos aumentam vertiginosamente, conforme estatísticas apresentadas. Por tudo isso, concluímos pela importância do trabalho como um serviço útil de prevenção aos golpes .

Referências

BRASIL. Disponível em: https://veja.abril.com.br/brasil/considerado-o-crime-da-moda-estelionato-digital-cresce-no-brasil#google_vignette Acesso em: 16 Mar. 2024

BRASIL. Disponível em: https://www.gov.br/investidor/pt-br/penso-logo-invisto/prevencao-de-fraudes-financeiras-estrategias-e-medidas-de-protecao Acesso em: 16 Mar. 2024

BRASIL. Disponível em: https://admin.pc.rs.gov.br/upload/arquivos/202304/04121500-cartilha-golpes-na-internet-atualizada-compressed.pdf Acesso em: 18 Mar. 2024

BRASIL. Disponível em: https://agenciabrasil.ebc.com.br/economia/noticia/2023-05/bancos-deverao-compartilhar-dados-para-prevencao-de-golpes-e-fraudes Acesso em: 18 Mar. 2024

BRASIL. Disponível em: https://www.serasa.com.br/premium/blog/golpes-do-pix-como-se-proteger/ Acesso em: 19 Mar. 2024

BRASIL. Disponível em: https://forbes.com.br/forbes-money/2023/09/por-que-a-ia-pode-tornar-os-crimes-digitais-mais-eficientes/ Acesso em: 19 Mar. 2024

BRASIL. Disponível em: https://blog.bb.com.br/golpe-0800/ Acesso em: 19 Mar. 2024

BRASIL. Disponível em: https://securityleaders.com.br/quais-desafios-a-inteligencia-artificial-traz-ao-mercado-de-prevencao-a-fraude/ Acesso em: 19 Mar. 2024

BRASIL. Disponível em: https://www.jusbrasil.com.br/artigos/cai-em-um-golpe-e-agora/2036433685 Acesso em: 19 Mar. 2024

BRASIL. Disponível em: https://www.jusbrasil.com.br/artigos/foi-vitima-de-golpe-virtual-saiba-como-proceder/918848086 Acesso em: 20 Mar. 2024

BRASIL. Disponível em:https://exame.com/inteligencia-artificial/hackers-estao-usando-inteligencia-artificial-para-aprimorar-golpes-diz-microsoft/ Acesso em: 20 Mar. 2024

BRASIL. Disponível em: https://tiinside.com.br/23/08/2023/os-riscos-do-golpe-de-clonagem-de-voz-protecao-contra-uma-ameaca-emergente/ Acesso em: 20 Mar. 2024

GONÇALVES, Jonas Rodrigo. Como escrever um Artigo de Revisão de Literatura. **Revista JRG de Estudos Acadêmicos**, Ano II, Vol. II, n.5, 2019.

GONÇALVES, Jonas Rodrigo. **Manual de Artigo de Revisão de Literatura.** 3.ed. Brasília: Processus, 2021.

GONÇALVES, Jonas Rodrigo. **Metodologia Científica e Redação Acadêmica.** 8. ed. Brasília: JRG, 2019.