FRAUDES EM TRANSAÇÕES ONLINE ENVOLVENDO CARTÃO DE CRÉDITO

Julia Castro Alves de Salles Cunha (Departamento de Empreendedorismo e Gestão da Universidade Federal Fluminense (UFF)- jucastro@id.uff.br;

Renan Vinagre Camara (Departamento de Empreendedorismo e Gestão da Universidade Federal Fluminense (UFF) - renan_vinagre@id.uff.br.

Resumo:

O presente trabalho tem como objetivo geral buscar um melhor entendimento sobre fraudes eletrônicas, especificamente quanto ao uso indevido e malicioso de cartão de crédito. Para tal, o relatório em questão valeu-se de cinco objetivos específicos. O primeiro objetivo tratou da descrição de como acontecem as fraudes em cartão de crédito, também foram abordados os principais métodos empregados pelos hackers para acessar informações sensíveis, mecanismos bancários de combate à fraudes, perfil de compra do titular do cartão e os sistemas que mais são fraudados. O objetivo principal foi a aplicação de uma pesquisa quantitativa com enfoque no público jovem para confrontar com dados da população brasileira economicamente ativa, levantados pela Confederação Nacional de Dirigentes Lojistas (CNDL).

Palavras Chaves: fraude, cartão de crédito, hacker, golpe, comércio eletrônico.

1- Introdução:

É notório que a praticidade tem ditado as novas formas de consumo, a situação atual de Pandemia e a paralisação temporária das lojas físicas tem contribuído ainda mais para uma migração crescente para as compras eletrônicas. Segundo estudo apresentado pela Abcomm, o comércio online teve um aumento de 81% em Abril de 2020 comparado ao mesmo mês do ano anterior, mês onde diversas cidades do país estiveram em isolamento social devido a pandemia. Kotler e Keller (2011) escrevem que o varejo sem loja física está dominando negócios do varejo tradicional e que de fato, alguns varejistas de lojas tradicionais viram no varejo online uma grande ameaça.

É justamente essa migração em massa para a compra on-line e a vulnerabilidade de informações disponibilizadas nessas transações que tornam o assunto de fraudes em cartão de crédito mais presente na vida dos consumidores. Tendo como base o desconhecimento dos

consumidores sobre o tema, e a limitada gama de informações que abordam a temática em pauta, o presente artigo tem como papel contribuir para a instrução e combate às fraudes em cartão de crédito de forma eletrônica.

Segundo a pesquisa feita por Abdallah (2016) as principais áreas de fraude on-line são telecomunicações, leilão on-line, comércio eletrônico, sistema de seguro de saúde e em primeiro lugar cartão de crédito. Por ser a área de fraude mais recorrente e gerar grandes prejuízos, adotamos esse ponto focal para análise.

2- Revisão de Literatura:

2.1- Elevação no número de fraudes

Segundo dados da Confederação Nacional de Dirigentes Lojistas (CNDL) e do Serviço de Proteção ao Crédito (SPC Brasil), entre Agosto de 2018 e no mesmo mês do ano seguinte mais de 12 milhões de brasileiros relataram ter sofrido alguma espécie de fraude online, equivalente a 46% dos internautas ativos nesse período, gerando um prejuízo de 1.8 bilhão de reais.

Ainda apresentando dados da CNDL, com números tão altos de fraudes e prejuízos, a confiança dos consumidores nas compras online é muito baixa, onde 8 a cada 10 brasileiros acreditam que estão sujeitos a sofrerem fraudes online. A pesquisa foi realizada com 917 pessoas residentes em todas as capitais do país, homens e mulheres, com idade igual ou maior a 18 anos e de todas as classes sociais e obteve uma idade média de 37 anos entre as pessoas que sofreram fraudes.

Corroborando com essas informações, dados da Federação Brasileira de Bancos (Febraban) apontam um aumento de 44% em golpes envolvendo o nome de bancos ou instituições financeiras com intuito de roubar dados e movimentar o dinheiro de forma indevida. Ainda com base em dados da Febraban, desde o início de março de 2020 o volume de tentativas de ataque de phishing bancário falsos por e-mail aumentou 80%.

Na visão de Pinheiro e Cunha (2003, p.35) a realização de estudos sobre fraudes, “não tem sido objeto de investigação metodológico-científica na mesma ordem de grandeza que o fenômeno tem sido mensurado em recentes pesquisas através de conceituadas instituições que atuam nos meios empresariais”.

2.2- Introdução de chip em cartão de crédito

Inicialmente é importante entendermos como acontecem as fraudes em cartão de crédito. Os fraudadores não precisam do cartão de forma física para fazer compras em nome de outra pessoa. As operações em sites, aplicativos e comércio eletrônico permitem que pessoas mal intencionadas busquem dados e por meio deles façam a compra.

A tecnologia anterior ao chip era a de trilhas magnéticas, após a adoção do chip nos cartões de crédito, o modelo de fraude no mundo físico foi consideravelmente reduzido. Diferente dos cartões magnéticos, os cartões com chip possuem um meio de codificação que protege as informações contra gravação. Essa tecnologia impede que informações sensíveis sejam acessadas.

A maior dificuldade de acessar o cartão fez com que os fraudadores migrassem seus esforços para o meio digital. A dinâmica adotada consiste em hackear os dados do portador do cartão, testar o cartão em uma compra de pequeno valor, cientes da validade e limite do cartão os fraudadores partem para compras de maior valor.

Segundo Futema (2018), em nosso país, possuímos uma das bases mais fortes de cartões com chip, o que reduziu dramaticamente o número de fraudes com cartões. Naturalmente as financeiras possuem total conhecimento dos padrões de compras do cliente e analisam potenciais fraudes baseadas nesses dados.

2.3- Perfil de Compra como artifício de combate à fraude

Segundo Futema (2018) as empresas de cartão de crédito tem adotado como mecanismo de combate a fraudes, o envio de SMS para os titulares do cartão avisando sobre as compras realizadas, o que permite uma análise do próprio consumidor e ajuda a isentar os emissores do cartão de culpa em certos casos de fraude.

Os bancos registram o perfil de compra de cada consumidor com base nos valores normalmente gastos, estabelecimentos onde são feitas compras de forma recorrente, e horários de compra. Quando algo incomum acontece, um valor muito expressivo é gasto ou uma compra é feita em um estabelecimento nunca antes acessado o banco notifica o portador do cartão antes de autorizar a compra.

Moraes (2008) afirma que estamos mais suscetíveis a fraudes em cartão de crédito quando o ambiente é online, já que é mais difícil verificar a identidade do comprador e se ele é um possível fraudador ou não. Quando se trata de perdas geradas pelas fraudes, a mesma afirma que apesar dos custos mensuráveis serem altos, custos não mensuráveis também devem ser levados em conta, tais como redução da satisfação do cliente, o sentimento de violação e vulnerabilidade em relação à empresa do cartão, além da perda de lealdade do cliente sobre a marca.

2.4- Tipos de Fraude

Segundo Turban et al., (2004) as fraudes podem ser executadas por pessoas de fora da organização que invadem um sistema, ou por pessoas de dentro da organização, autorizadas a usar o sistema, porém fazendo mau uso dessa autorização. Pessoas de fora da organização bancária podem agir em conluio com membros das companhias, que atuam como facilitadores de informações.

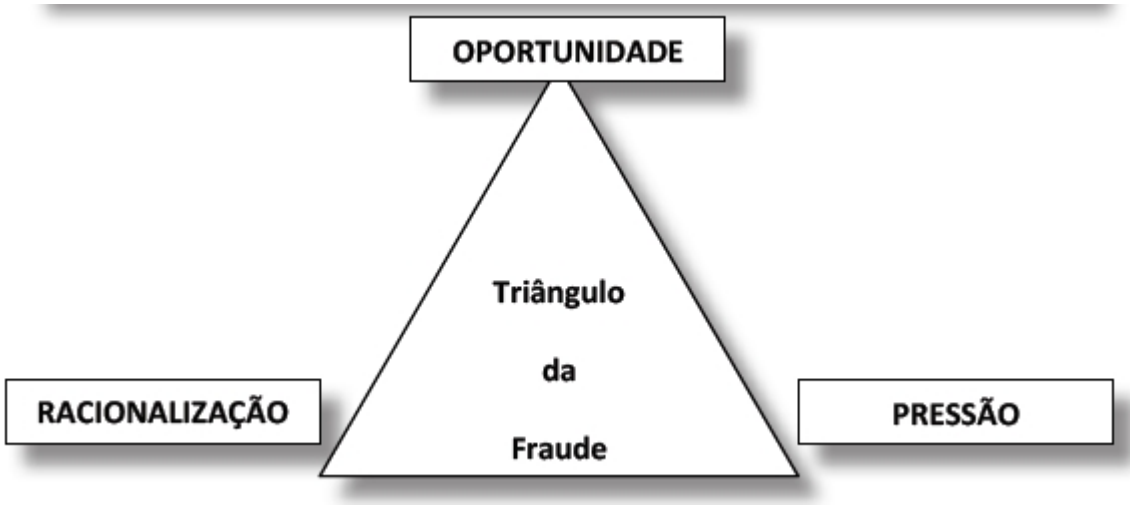
Gil (1999) classifica as fraudes informatizadas quanto à sua formação em três tipos: fraude de funcionários, fraudes de quadrilhas e fraudes de chefia. O mesmo explica que as fraudes de funcionários são as mais fáceis de serem detectadas e que apresentam a maior quantidade de ocorrências.

As fraudes por quadrilha são as mais difíceis de serem identificada, têm ocorrência mais rara e geralmente causam grandes impactos nas empresas. Por fim, as fraudes de chefia normalmente são praticadas por executivos empresariais, causam grandes prejuízos financeiros e geralmente culminam em impunidade. Os cargos elevados de chefia fazem com que os fraudadores sintam-se no direito de justificar seus atos ilícitos alegando desvios concretizados pelas organizações por ocasião de seus negócios.

Segundo a Associação Brasileira de Comércio Eletrônico (ABComm), o e-commerce brasileiro registra uma tentativa de fraude a cada cinco segundos. Em 2017 foram feitas mais de 203 milhões de compras online ao longo do ano. Sendo, 3,03% delas de origem fraudulenta. Logo, mais de 6 milhões de transações foram feitas por estelionatários utilizando cartões clonados durante os 365 dias do ano. Cressey (1953) desenvolveu a Teoria do Triângulo da

Fraude que permite identificar os motivos que dão origem e incentivam a ocorrência de fraude, por parte de um ou mais indivíduos.

Na tríade de motivos encorajadores está a pressão, geralmente associada a questões financeiras, ou pretensão de vida acima da sua realidade. A oportunidade, geralmente associada a fragilidade do sistema de controle das organizações e por fim a racionalização, que está atrelada as razões que o fraudador procura para justificar a fraude.



Fonte: eosconsultores

3- Metodologia da Pesquisa:

Foi aplicada uma pesquisa quantitativa. O público alvo escolhido foi de universitários de 18 a 30 anos de ambos os sexos majoritariamente da cidade de Niterói, localizada na região metropolitana do Rio de Janeiro.

O público foi escolhido com objetivo de confrontar os dados regionais de um público alvo específico com dados apresentados na sessão anterior, representando todo o público brasileiro sem uma faixa etária definida.

O questionário aplicado foi composto pelas questões abaixo:

1	Você tem cartão de crédito?
2	Você realiza compra online com cartão de crédito?
3	Você já sofreu algum tipo de fraude online?
4	Quantas fraudes de cartão de crédito você já sofreu?
5	Você costuma comprar em sites nacionais ou internacionais?

6	Qual a sua frequência de compra online?
7	A quarentena impactou na sua frequência de compra online?
8	Utiliza computador ou smartphone?
9	Qual o sistema operacional do dispositivo utilizado?
10	Você salva seu cartão nos sites que realiza suas compras?
11	Você costuma checar o endereço dos sites que realiza suas compras?
12	Você sabe como agir caso seu cartão seja clonado?
13	Você costuma consultar sites de reclamação?
14	Você considera sua senha forte?
15	Você troca sua senha nos sites com frequência?
16	Você costuma verificar se a conexão do site é segura?

Tabela 1. Questionário aplicado aos entrevistados

4- Resultados:

Os dados obtidos abaixo são referentes a 135 respondentes, da faixa etária em estudo e tratam de indicadores relevantes e específicos que serão empregados no tópico Discussão para fins comparativos.

A pergunta “Você tem cartão de crédito?” foi feita com intuito de avaliar a aderência dos jovens a esse método de pagamento. A pergunta “Você realiza compras online com cartão de crédito?” permitiu compreender se as compras online estão presentes no perfil de compra do público alvo, se os mesmo são adeptos de métodos modernos de consumo ou preferem efetuar compras de forma presencial.

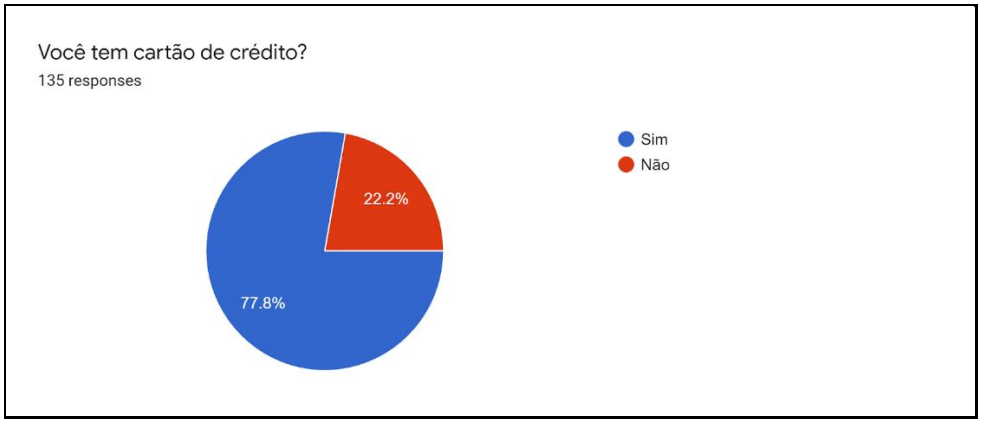


Figura 1. - "Você tem cartão de crédito?"

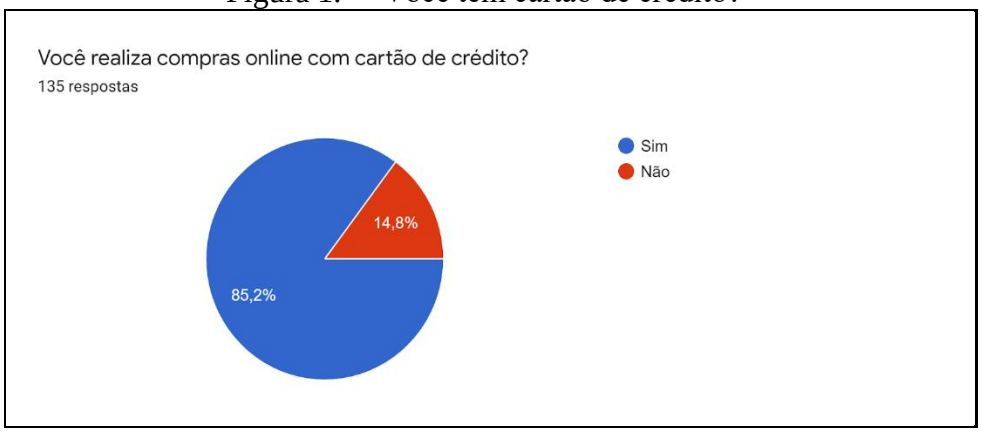


Figura 2 - "Você realiza compras online com cartão de crédito?"

A pergunta "Você já sofreu algum tipo de fraude online?" foi feita com intuito de compreender a incidência de fraude online entre o público jovem. A pergunta "Quantas fraudes de cartão de crédito você já sofreu?" permitiu compreender se os jovens aprendem com falhas de segurança ou são alvos recorrentes dos fraudadores eletrônicos.

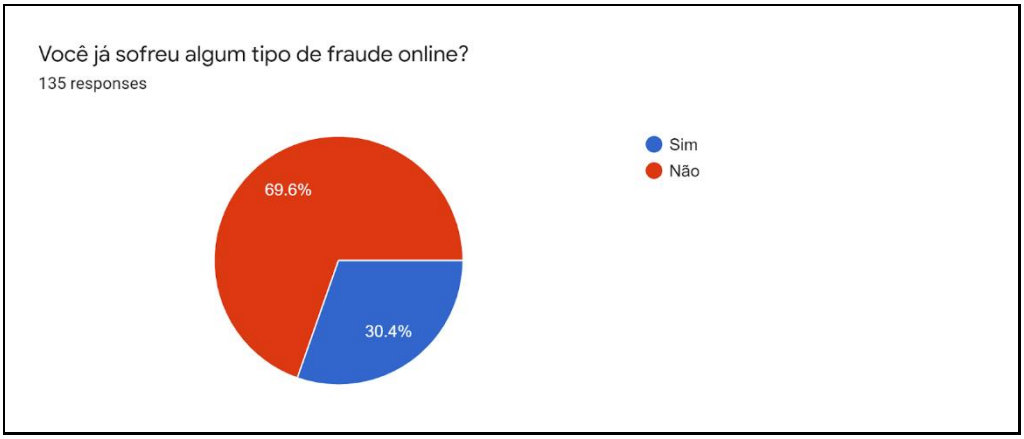


Figura 3. “Você já sofreu algum tipo de fraude online?”

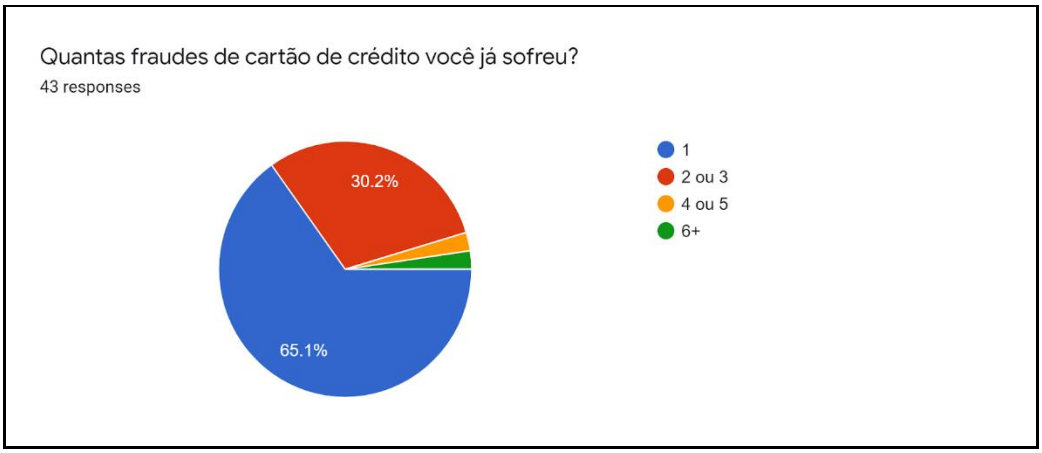


Figura 4. “Quantas fraudes de cartão de crédito você já sofreu?”

A pergunta “Você costuma comprar em sites nacionais ou internacionais?” objetivou identificar onde as fraudes ocorrem com maior frequência.

Figura 5. “Você costuma comprar em sites nacionais ou internacionais?”

A pergunta “Qual a sua frequência de compra online?” visou entender qual o padrão de consumo anual do público em estudo, enquanto a pergunta “A quarentena impactou na sua frequência de compra online?” buscou identificar o impacto do isolamento social e fechamento do comércio na modalidade de consumo. Assim é possível compreender se os jovens já consumiam de forma online ou se o contexto de Pandemia iniciou um novo hábito.

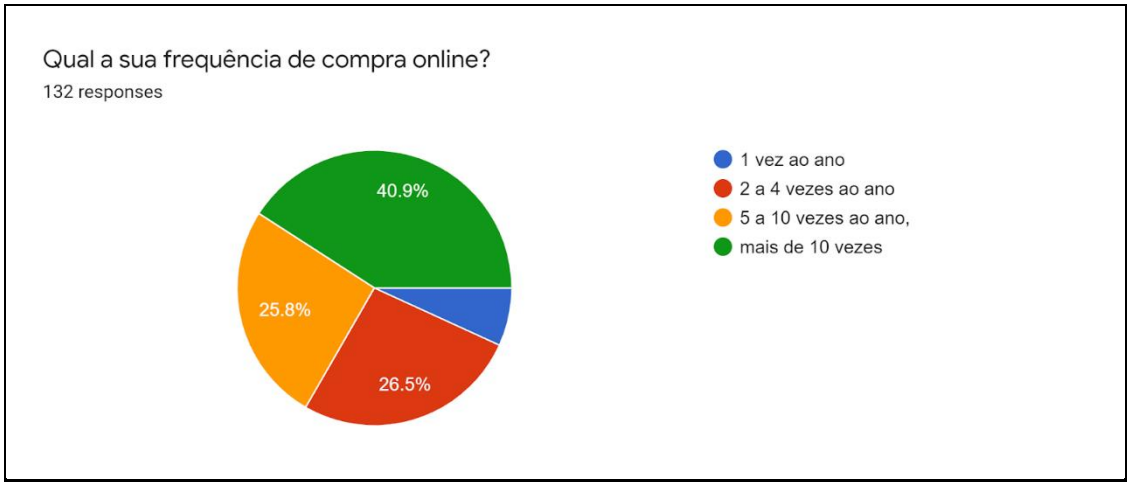


Fig. 6. “Qual a sua frequência de compra online?”

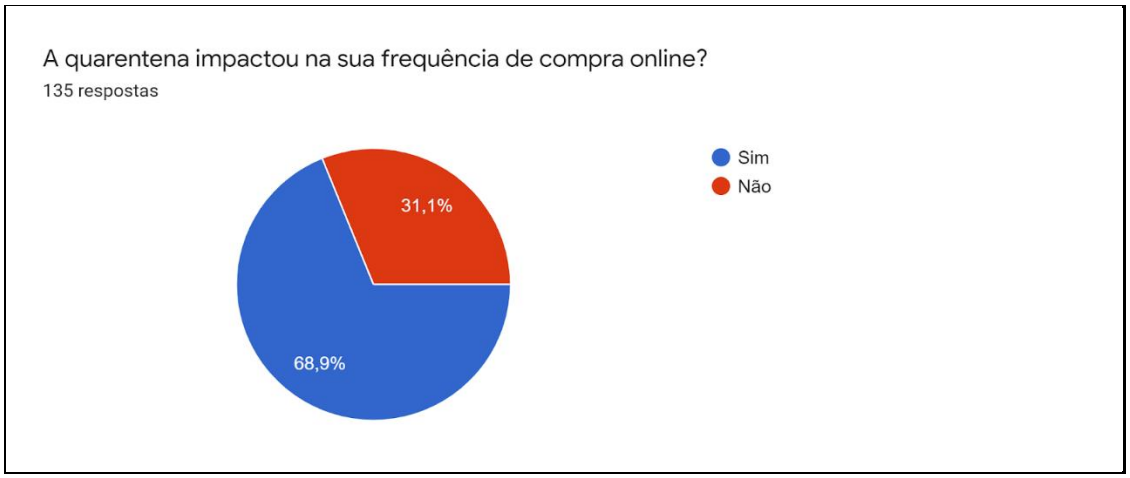


Fig. 7. “A quarentena impactou na sua frequência de compra online?”

A pergunta “ Você utiliza computador ou Smartphone para fazer compras online?” foi feita com intuito de coletar informações sobre o aparelho utilizado, se o mesmo exerce alguma influência nos índices de fraude eletrônica entre os jovens de 18 a 30 anos.

Complementando essa análise, a pergunta “ Qual é o sistema operacional do seu dispositivo?” foi feita para comparar a forma de acesso e sua vulnerabilidade proporcional a resposta anterior.

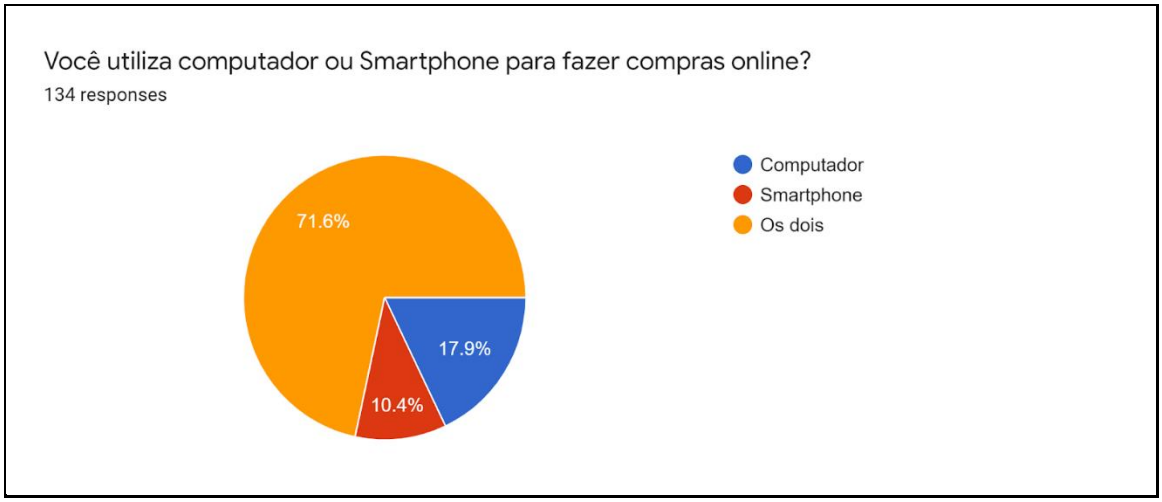


Fig. 8.“Você utiliza computador ou Smartphone?”

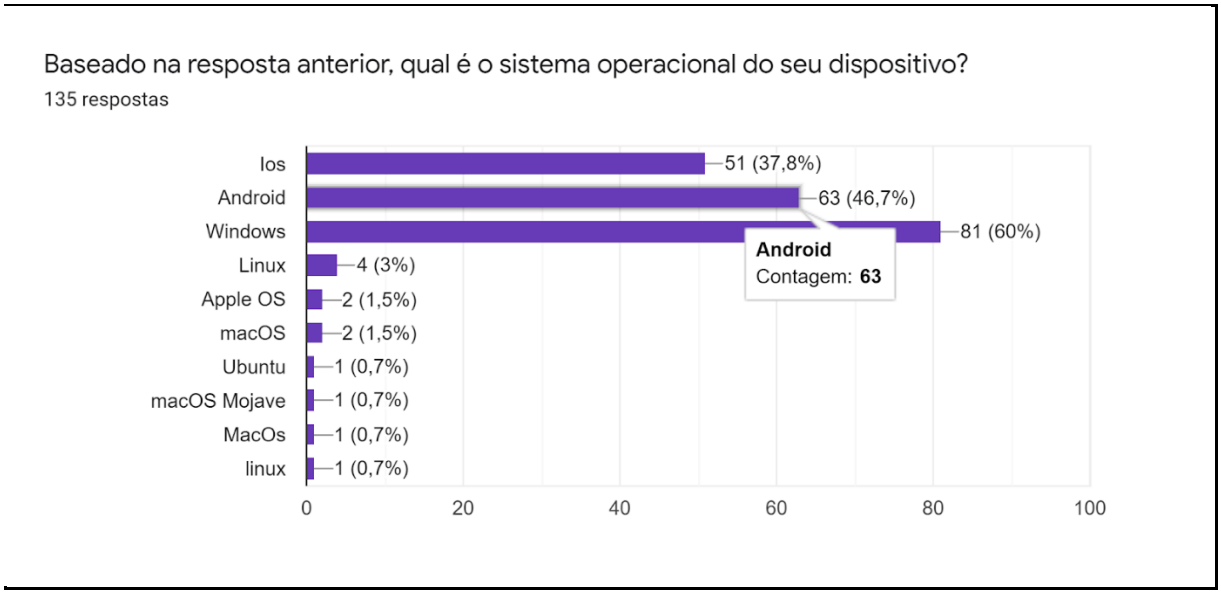


Fig. 9. “Qual é o sistema operacional do seu dispositivo?”

A pergunta “Você salva seu cartão nos sites que realiza suas compras” esteve entre as diversas perguntas que buscou identificar a preocupação com segurança dos respondentes.

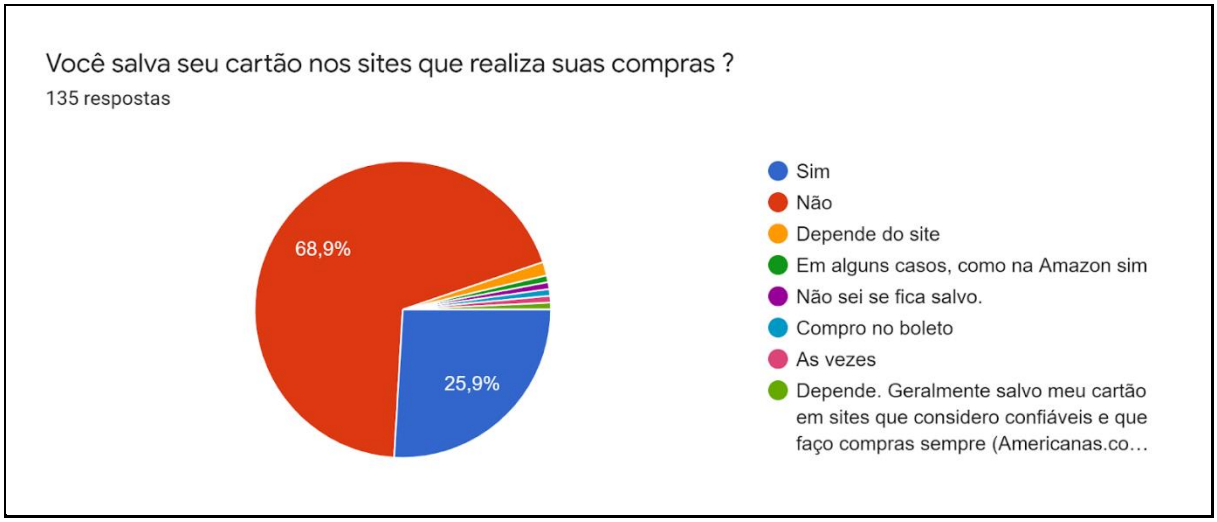


Figura 10. “Você salva seu cartão nos sites que realiza suas compras?”

As perguntas “Você costuma checar o endereço dos sites que realiza suas compras?” e “Você sabe como agir caso seu cartão seja clonado?” foram realizadas com intuito de compreender o conhecimento dos jovens em relação às medidas de prevenção e correção.

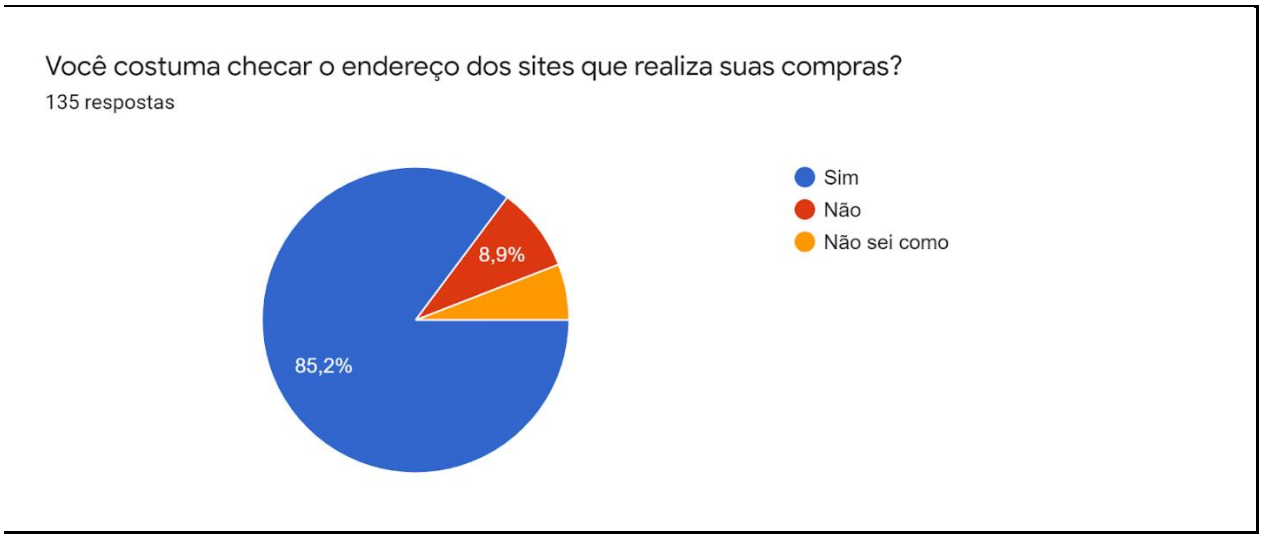


Figura 11. “Você costuma checar o endereço dos sites que realiza suas compras?”

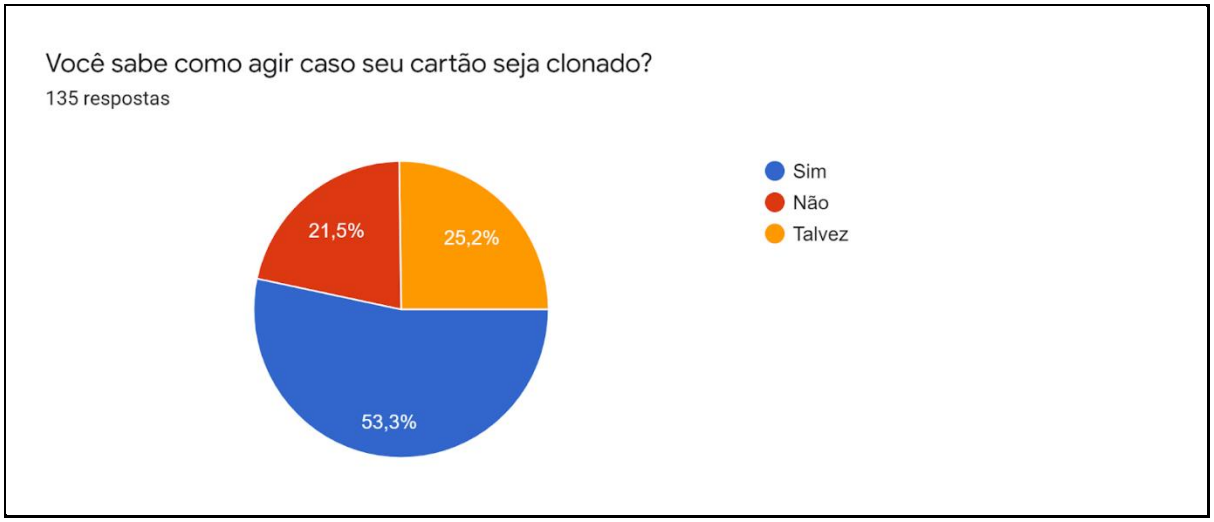


Figura 12. “Você sabe como agir caso seu cartão seja clonado?”

A pergunta “Você costuma consultar sites de reclamação antes de fazer compras online?” buscou identificar se os jovens são induzidos pela experiência de compra alheia ou se apresentam um perfil mais arriscado de consumo. A pergunta “Você troca a sua senha nos sites com frequência?” foi realizada com intuito de compreender a preocupação dos jovens quanto ao sigilo de senhas. Se o público tem o hábito de modificar as senhas ou se mantém as mesmas para fins de praticidade.

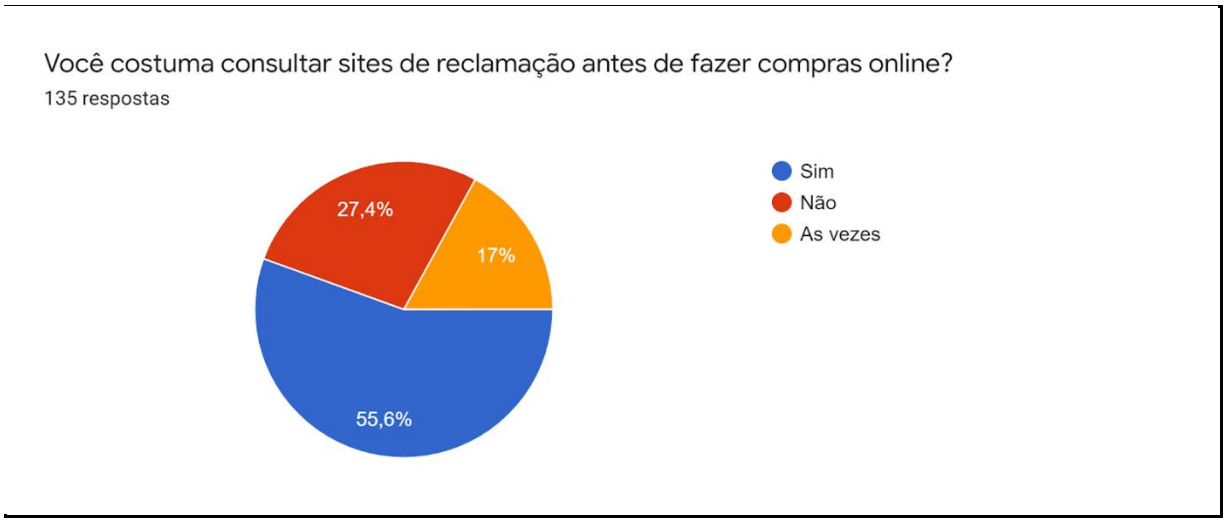


Figura 13. “Você costuma consultar sites de reclamação antes de fazer compras online?”

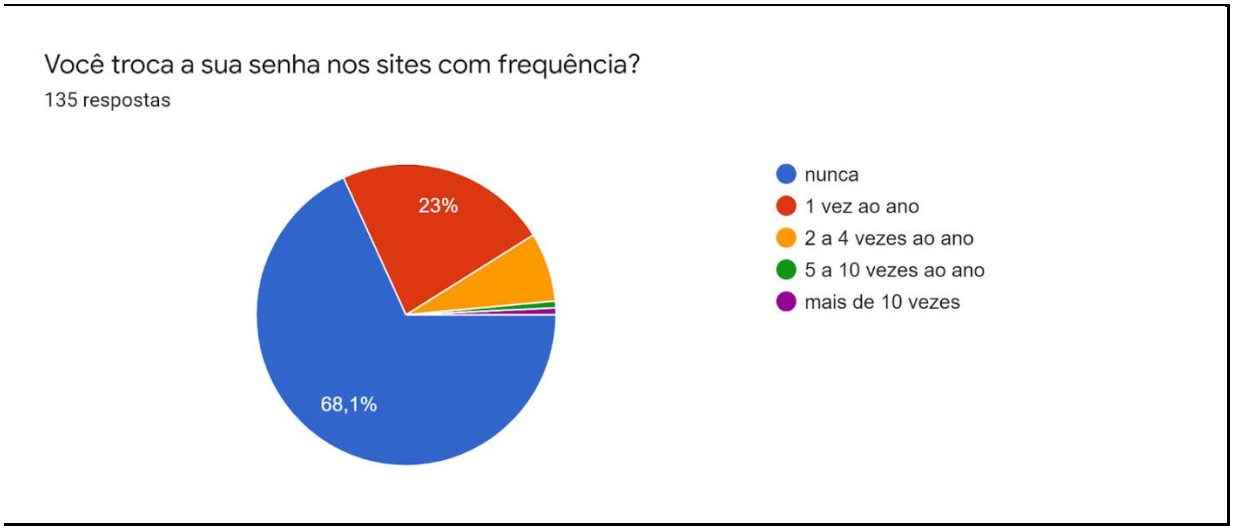


Figura 14. “Você troca a sua senha nos sites com frequência?”

A pergunta “Você considera suas senhas fortes?” foi feita com o objetivo de identificar o quão forte são as senhas empregadas e se há uma preocupação dos jovens quanto a esse quesito. A pergunta “Você costuma verificar se a conexão do site é segura?” buscou identificar se os jovens têm conhecimento e consideram importante a presença do cadeado de segurança nos sites que costumam acessar e efetuar compras.

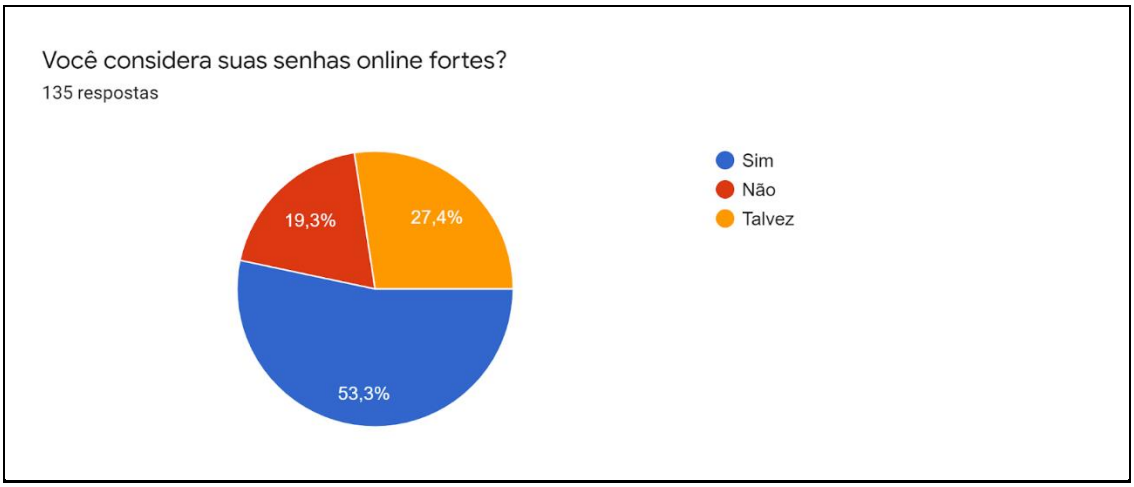


Figura 15.“Você considera suas senhas online fortes?”

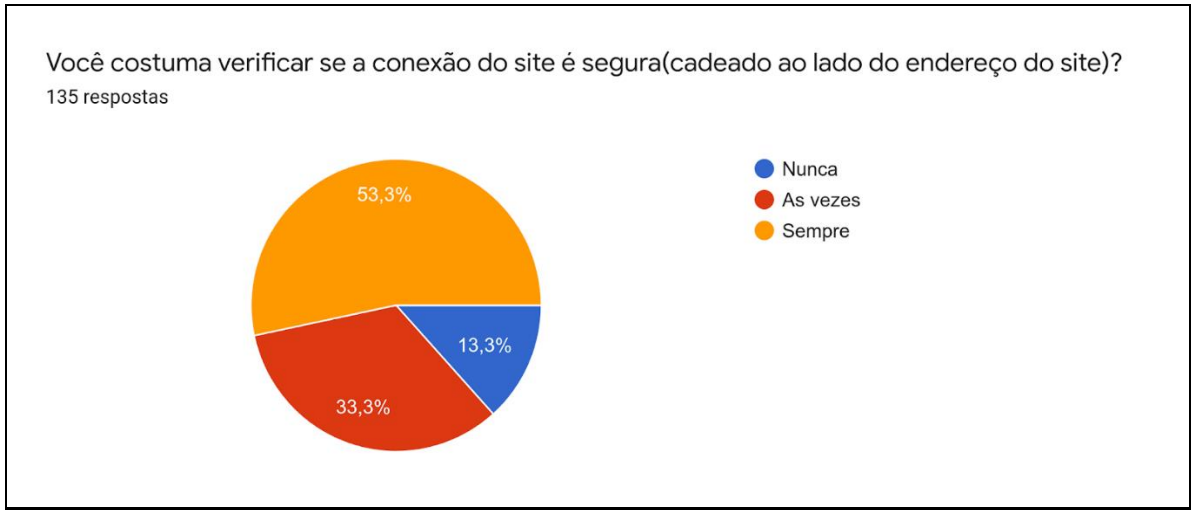


Figura 16. "Você costuma verificar se a conexão do site é segura?"

5- Discussão:

Nesse tópico do relatório os resultados da pesquisa quantitativa serão discutidos e relacionados aos dados da pesquisa do CNDL, para fins comparativos e expositivos. Serão apresentadas as perspectivas dos autores sobre os dados estudados, conclusões e indícios das suas análises.

É notório entre o público estudado que a parcela de utilizadores de cartão de crédito é bastante alta, atingindo 77.8% dos jovens. O que podemos concluir como reflexo de uma crescente de fintechs e facilitações de crédito. De acordo com estudo da CNDL, nos últimos anos as fintechs expandiram-se abruptamente, alcançando uma parcela significativa da população Brasileira, somando 21,5% do total de cartões de créditos utilizados no Brasil, e aproximadamente um terço desse público são de jovens, entre 18 e 35 anos, o que sustenta o número elevado de usuários de cartão de crédito entre a faixa etária estudada.

Quando se trata de compras online a porcentagem de adeptos é maior que a de detentores de cartão de crédito, evidenciando que 7.4% dos pesquisados compram através de cartão de crédito de outras pessoas ou utilizam opções de cartões pré-pago, o que pode evidenciar dois fatores para estudos futuros: que essa parcela do público utiliza cartões de terceiros, provavelmente de familiares ou pessoas próximas, representando uma dependência financeira ou que se preocupam com a segurança dos seus cartões e preferem opções pré-pagas.

Um dado relevante obtido pela pesquisa é que apenas 30.4% do público alvo já sofreu

fraudes online entre a faixa etária estudada, em oposição aos 46% do total de brasileiros apenas no último ano. Tais dados sobressaem fortemente aos dados nacionais da CNDL, indicando que os jovens estão menos suscetíveis às fraudes.

Outro fator que destaca um menor índice de fraudes com o público alvo é que majoritariamente os fraudados só sofreram esse tipo de golpe uma única vez em sua vida. Dado que reafirma uma maior preocupação do público de 18 a 30 anos no quesito segurança eletrônica, visto que a população estudada reincidente em golpes é minoria entre os respondentes.

Sobre a frequência de compras online a pesquisa aplicada demonstra que a maior parcela dos jovens compra mais de dez vezes ao ano. Esse dado reflete uma maior confiança do público nos meios de venda digitais o que foi fortalecido com o contexto de isolamento social.

Com Pandemia do Covid-19, as lojas físicas foram fechadas e a alternativa para continuar os negócios foi a criação do e-commerce. A pesquisa comprovou que a quarentena mudou a frequência de compra de grande parte dos respondentes, os preços promocionais e a necessidade de venda das lojas para sua sobrevivência ocasionou uma elevação no consumo eletrônico, 68,9% dos respondentes alegaram uma mudança de hábitos.

Quanto ao aparelho utilizado para efetuar a compra, a maioria dos entrevistados utiliza tanto o computador quanto o celular, o que descarta inicialmente um padrão específico de atuação dos fraudadores em relação ao dispositivo utilizado. Os sistemas operacionais mais utilizados pelo público alvo foram em 1º lugar com 60% o Windows, seguido pelo Android e IOS. De acordo com Flávio Tasinaffo os sistemas que mais sofrem fraudes são o Windows, Android e iPhone, respectivamente. Já, Google Chrome e Safari são os navegadores utilizados em mais de 90% das tentativas de golpe. Dados esses que ratificam os resultados obtidos.

Ao perguntarmos pro nosso público se eles têm o costume de salvar o cartão nos sites que fazem compras, a resposta majoritária foi não, apenas 25% deles alegaram salvar seus cartões. Com isso, conseguimos fortalecer a afirmação de que a faixa etária estudada tende a ter mais cuidado ao fazer compras online. Outro ponto que comprova isso, é a resposta de 85% dos entrevistados, afirmando checar se os sites em que fazem suas compras são seguros.

A pesquisa apontou um dado muito importante, uma parcela minoritária, mas muito expressiva dos pesquisados, alegou ter dúvidas ou não saber lidar com a fraude eletrônica. O assunto é uma espécie de tabu entre os bancos e não é mencionado por medo de propaganda negativa para as instituições financeiras que oferecem cartões de crédito como serviço.

Na pesquisa aplicada 55% do público pesquisado disse se preocupar em consultar sites de reclamação antes de concluírem suas compras online. Porém, quando questionados sobre a troca periódica de senhas, a maioria deles respondeu que “nunca” trocam suas senhas online e que as consideram fortes. O comportamento identificado pode trazer brechas para que os fraudadores atuem em sites de compras, principalmente quando os usuários optam por gravar dados referentes ao cartão.

Tais brechas são identificadas e por meio de técnicas de obtenção de dados as fraudes bancárias são executadas. Existem vários métodos de obtenção de dados, o primeiro é o de captura do teclado digital, nessa técnica os hackers acessam o que o usuário está digitando e assim conseguem informações de senhas. Para combater essa fraude os bancos têm disposto os números de forma aleatória e em vez de digitar a senha, o usuário clica nos campos que apresentam os números que compõem sua senha.

Outro método é o falso navegador, inicialmente os hackers criavam páginas que se assemelhavam aos sites dos bancos mas nem sempre eram convincentes. Essas páginas apresentavam erros e tinham suas limitações o que dava pistas ao usuário de que não se tratava de uma página de acesso seguro. Os fraudadores aprimoraram suas técnicas e passaram a injetar códigos nos navegadores reais, assim os próprios sites oficiais eram manipulados e as informações eram obtidas.

O redirecionamento também se tornou um método fraudulento comum entre os hackers. São feitas alterações na configuração do navegador ou do arquivo do Windows. Os sistemas mais sofisticados ainda conseguem instalar uma falsa certificação que permite que o site clonado apresente o cadeado de segurança.

Os hackers também obtêm informações por meio de vírus. Os vírus modificam o destinatário de transferências, manipulam extratos para que as compras não sejam notadas,

fazem uso de códigos de segurança digitados e fazem modificações em boletos. Nesse caso a senha não é necessária, a fraude é feita diretamente do computador da vítima.

6- Conclusão:

A pesquisa concluiu, que o público alvo pesquisado é menos vulnerável a sofrer fraudes online, quando comparado à totalidade do público brasileiro. Trata-se de uma parcela da população que valoriza a praticidade e facilidade na ocasião de compra.

Há uma tendência crescente de migração do perfil de compra das novas gerações para o e-commerce, que não se limitará ao contexto de isolamento social. Trata-se de uma nova realidade que foi muito bem aceita pelos jovens e dá indícios da geração de uma tendência de plataforma para consumo. Tal tendência deve estimular ainda mais fraudadores a buscarem aberturas para atuar neste meio, o que se apresenta como um grande desafio para as financeiras que oferecem os serviços de cartão de crédito.

Para garantir a segurança do consumidor no processo de compra on-line, os bancos devem instalar sistemas de prevenção (FPS's) e de detecção (FDS's). Esses sistemas podem atuar separadamente, mas quando combinados surtem melhores efeitos. As estratégias de defesa são cinco: prevenção e detenção, detecção, limitação, recuperação e correção, segundo Turban et al (2004).

Os sistemas de segurança contra fraude demandam investimento e investigação. Como pôde ser visto no relatório, assim como as empresas e especialistas vêm estudando os métodos empregados e como detê-los, os próprios fraudadores vem concomitantemente aprimorando suas técnicas. Por isso, todo o investimento aplicado no combate a fraude eletrônica é não só necessário como pode representar a longo prazo um diferencial ligado a um menor prejuízo com fraudes e maior prestígio no que diz respeito ao sentimento de segurança dos consumidores.

Não foi possível no escopo deste trabalho identificar o motivo do baixo nível de compras online internacionais, como trabalho futuro os autores pretendem se aprofundar nesse contexto e identificar eventuais perfis mais suscetíveis à fraudes de acordo com os e- commerces frequentados e seus locais de origem.

Referências:

ABDALLAHN, Aisha, MAAROF, M. Aizaini, ZAINAL, Anazida. (2016). Fraud detection system: A survey. Journal of Network and Computer Applications.

FILGUEIRAS, Isabel. (15 de agosto 2019). Valor Investe. 12 milhões de brasileiros são vítimas de golpes na internet. Disponível em Valor Investe: https://valorinveste.globo.com/objetivo/gastar-bem/noticia/2019/08/15/12-milhoes-de-brasileiros-sao-vitimas-de-golpes-na-internet-veja-os-mais-comuns.ghtml. – Acessado em (27 de Julho de 2020).

FUTEMA, Fabiana. (15 de março de 2018). Como funcionam as novas fraudes com cartão de crédito. Disponível em Veja: <https://veja.abril.com.br/economia/como-funcionam-as-novas- fraudes-com-cartao-de-credito/>. – Acessado em (27 de Julho de 2020).

Tipos de cartões magnéticos. Disponível em Os Tipos de: https://www.ostiposde.com/tipos-de-cartoes-magneticos/. – Acessado em (27 de Julho de 2020).

ROHR, Altieres. (28 de junho de 2013). Entenda como os hackers brasileiros realizam fraudes bancárias. G1. Disponível em G1: http://g1.globo.com/tecnologia/blog/seguranca-digital/post/entenda-como-os-hackers-brasileiros-realizam-fraudes-bancarias.html. – Acessado em (27 de Julho de 2020).

FIORI, Diniz. (27 de junho 2020). E-commerce cresce, mesmo durante a pandemia. Disponível em ABComm: https://abcomm.org/noticias/e-commerce-cresce-mesmo-durante-a-pandemia/. – Acessado em (27 de Julho de 2020).

NAKAMURA, A. Massami. (2011). Comércio Eletrônico - Riscos nas compras pela Internet. FATECSP.

MORAES, Dalila. (2008). Modelagem de Fraude em Cartão de Crédito. Arquivo da Universidade Federal de São Carlos.

BASTOS, P. S. Siqueira. (2017). Fraudes Eletrônicas: O que há de novo? Revista de Contabilidade do Mestrado em Ciências Contábeis da UERJ.

(31 de janeiro de 2018). E-commerce brasileiro sofre uma tentativa de fraude a cada cinco segundos. Disponível em E-commerce Brasil: https://www.ecommercebrasil.com.br/noticias/e-commerce-brasileiro-sofre-uma-tentativa-de-fraude-cada-cinco-segundos/. – Acessado em (27 de Julho de 2020).

STIVANI, Mirella. (31 de dezembro de 2018). Os sete maiores golpes online de 2018. Disponível em TechTudo: https://www.techtudo.com.br/noticias/2018/12/os-sete-maiores-golpes-online-de-2018.ghtml. – Acessado em (27 de Julho de 2020).

Redação Vindi. (19 de setembro 2017). Conheça os principais sistemas antifraude para e-commerce do mercado. Disponível em Redação Vindi: https://blog.vindi.com.br/sistemas-antifraude-ecommerce/ – Acessado em (27 de Julho de 2020).

TASINAFFO, Flávio. (27 de fevereiro de 2020). A cada 5 segundos, há uma tentativa de fraude cibernética, aponta estudo. Disponível em Blogosfera Uol: https://tudogolpe.blogosfera.uol.com.br/2020/02/27/a-cada-5-segundos-ha-uma-tentativa-de-fraude-cibernetica-aponta-estudo/. – Acessado em (27 de Julho de 2020).

Redação Nubank (16 de junho de 2020). Golpes financeiros crescem 44% na pandemia. Como se proteger? Disponível em Blog Nubank: https://blog.nubank.com.br/golpes-financeiros-como-se-proteger. – Acessado em (28 de setembro de 2020).

BRAUN, Daniela. (18 de setembro de 2020). Golpes bancários pela internet crescem 80%

durante a pandemia, diz Febraban. Disponível em Valor Investe: https://valorinveste.globo.com/produtos/servicos-financeiros/noticia/2020/09/18/golpes-bancarios-pela-internet-crescem-80percent-durante-a-pandemia-diz-febraban.ghtml. – Acessado em (28 de setembro de 2020).

ECKERT, Alex. – Fraudes Contábeis: Caracterização e análise das publicações em periódicos e eventos nacionais de contabilidade. Revista Universo Contábil. 2020

GIL, A. de Loureiro. – Como Evitar Fraudes, Pirataria e Conivência. 2. ed. São Paulo: Atlas, 1999.

WELLS, Joseph T. – Fraude na empresa: prevenção e detecção. 2ª ed. Coimbra: Edições Almedina. SA, 2009.

MARCONDES, J. S. (13 de fevereiro de 2017). Fraude – Fraude Organizacional, Empresarial – Tipos de Fraudes. Disponível em Blog Gestão de Segurança Privada: https://gestaodesegurancaprivada.com.br/conceito-de-fraude-o-que-e-definicao/. – Acessado em (28 de setembro de 2020).