revista principia
Vol. 59, N. 4
REVISTA DE DIVULGAÇÃO CIENTÍFICA E TECNOLÓGICA DO INSTITUTO FEDERAL DE CIÊNCIA, EDUCAÇÃO E TECNOLOGIA DA PARAÍBA

DOI: http://dx.doi.org/10.18265/1517-0306a2021id5834
ARTIGO ORIGINAL

SUBMETIDO 27/04/2021
APROVADO 28/06/2021
PUBLICADO ON-LINE 22/08/2021
PUBLICADO 30/12/2022
EDITORA ASSOCIADA
Crishane Azevedo Freire

Vulnerabilidade à Engenharia Social: um estudo com alunos do Instituto Federal da Paraíba (IFPB)

José Augusto Lopes Viana [1] *
Antônio José Costa Alves [2]
Pedro Gustavo Santos de Lima [3]

[1] augusto.viana@ifpb.edu.br
[2] antoniojosecostaalves@gmail.com
[3] pedrogustavo0520@gmail.com.

Instituto Federal de Educação, Ciência e Tecnologia da Paraíba (IFPB), Campus Guarabira, Brasil.

*Autor para correpondência.

RESUMO: A Engenharia Social representa uma das maiores ameaças à segurança da informação. Por meio da manipulação de pessoas, agentes mal intencionados subtraem informações e bens de suas vítimas. Nesse contexto, este estudo foi desenvolvido com o objetivo de verificar como se apresenta a vulnerabilidade à Engenharia Social entre os discentes dos cursos técnicos integrados ao Ensino Médio (Informática, Contabilidade e Edificações) do Instituto Federal da Paraíba, Campus Guarabira. Para tanto, foram aplicados 170 questionários on-line compostos por itens que verificavam o nível de vulnerabilidade desses alunos em três dimensões: persuasão, coleta de dados e fabricação. Os resultados mostraram que, de forma geral, os alunos apresentam um nível de vulnerabilidade baixo, porém com diferenças de comportamento entre grupos. Alunos do Curso Técnico em Informática e residentes na área urbana apresentaram, estatisticamente, um nível mais baixo de vulnerabilidade. Embora no contexto geral se observe tal resultado, quando se analisaram os itens do questionário separadamente, verificou-se que dois deles mostravam níveis acima do ponto médio da escala utilizada. Esses dois itens apresentavam situações relacionadas à retribuição de favores na internet e à criação de senhas de acesso a sistemas.

Palavras-chave: ameaças virtuais; crimes cibernéticos; persuasão; segurança da informação.

Vulnerability to Social Engineering: a study with students from the Instituto Federal da Paraíba (IFPB)

ABSTRACT: *Social engineering represents one of the biggest threats to information security. Through the manipulation of people, malicious agents subtract information and assets from their victims. In this context, this study was developed with the objective of verifying the vulnerability to social engineering among students of technical courses (Informatics, Accounting and Building) at the Instituto Federal da Paraíba, Campus Guarabira. To this end, 170 online questionnaires were applied, consisting of items that checked the*

ISSN (on-line): 2447-9187

vulnerability level of these students in three dimensions: persuasion, data collection and fabrication. The results showed that, in general, students have a low level of vulnerability, however, with differences in behavior between groups. Students in the technical course of Informatics and residents in the urban area showed, statistically, a lower level of vulnerability. Despite this result in the general context, the students showed low levels of vulnerability, when the items that made up the questionnaire were analyzed separately, two of them showed levels above the midpoint of the scale used. These two items presented situations related to the return of favors on the internet and the creation of passwords for accessing systems.

Keywords: *cybercrimes; information security; persuasion; virtual threats.*

1 Introdução

A mudança de paradigma imposta pela popularização do uso da rede mundial de computadores – a internet – nas mais diversas atividades humanas tem levado as pessoas a uma conectividade permanente com um mundo de conhecidos e desconhecidos, trazendo facilidades e também preocupações, já que a popularização de suas vias de acesso também oferece àqueles que praticam crimes novas oportunidades para atividades ilegais (MARTIN; RICE, 2013).

Embora o senso comum nos dias atuais considere o uso das Tecnologias de Informação e Comunicação (TICs) uma atividade trivial, quando se busca um maior entendimento dos seus aspectos técnicos e de segurança, é preciso considerar que a maioria das pessoas se sente ignorante sobre o uso das TICs (MANN, 2011). Isso facilita a criação de situações de vulnerabilidade para os usuários da grande rede mundial de computadores no acesso a sistemas, na interação com pessoas e na proteção dos seus dados pessoais e informações mais diversas, especialmente quando a informação tem assumido o papel de um dos ativos mais importantes na atualidade. A informação é o novo petróleo na economia mundial (COULDRY; MEJIAS, 2019).

Nesse sentido, a vulnerabilidade passa a existir quando se tem uma interação, em um determinado contexto, de um usuário da rede, na condição de vítima, com um agressor cujo objetivo é obter acesso indevido a informações que lhe permitam subtrair bens ou valores da vítima, situação da qual, quando estabelecida, depreende-se que houve uma violação na segurança da informação.

A segurança da informação consiste na proteção da informação contra vários tipos de ameaças (ABNT, 2007). Esse tipo de segurança pode ser abordado a partir de vários aspectos e contempla os recursos físicos, lógicos e humanos que se relacionam e se sobrepõem (CÔRTES, 2008). Os recursos abordados por este estudo são os recursos humanos, mais especificamente o comportamento humano nas interações em que informações, muitas vezes negligenciadas por pessoas e organizações, possam ser subtraídas para uso escuso.

Várias técnicas são utilizadas por hackers e agressores, virtuais ou não, com a intenção de burlar a proteção da informação. Uma das técnicas mais eficientemente utilizadas, sendo considerada uma das maiores ameaças relacionadas à segurança da informação, é a da engenharia social (HADNAGY, 2011; MANN, 2011; MITNICK; SIMON, 2003). Segundo Hadnagy e Ekman (2014), trata-se de qualquer ato que influencie alguém a

tomar uma ação que pode ser ou não em seu melhor interesse. A engenharia social se torna especialmente perigosa porque nem todas as técnicas utilizadas por ela podem ser detectadas por sistemas computacionais, já que normalmente são aplicadas na interação entre pessoas, e as pessoas representam o elo mais fraco quando se trata da prevenção de fraudes (HADNAGY, 2011; MANN, 2011; MITNICK; SIMON, 2003).

A melhor arma contra essa ameaça é a própria informação, sua matéria-prima, a educação sobre seus métodos e consequências (CONHEADY, 2014). Assim, esta pesquisa se mostra relevante quando busca traçar um cenário trazendo à discussão uma prática que pode causar grande impacto naqueles que são vitimados por ela. Uma prática que se mostra pouco conhecida e, mesmo quando conhecida, muitas vezes negligenciada.

Os Institutos Federais formam jovens por todo o país, para atuarem como profissionais em diversos mercados. Jovens que iniciam o contato com a internet cada vez mais cedo e precisam estar atentos aos riscos aos quais estão sujeitos na interação com outras pessoas, no uso de sistemas e no acesso à grande rede mundial de computadores. Riscos para eles mesmos e para as organizações, quando eles estiverem atuando como profissionais no mercado de trabalho. Nesse contexto, esta pesquisa buscou verificar como se apresenta a vulnerabilidade à engenharia social entre os discentes dos cursos técnicos integrados ao Ensino Médio do Instituto Federal de Educação, Ciência e Tecnologia da Paraíba (IFPB), Campus Guarabira.

As demais seções deste artigo estão organizadas da seguinte forma: a seção 2 discute a engenharia social em seus principais aspectos, a seção 3 explicita os procedimentos metodológicos para a execução da pesquisa, a seção 4 apresenta a discussão sobre os resultados alcançados e a seção 5 traz as considerações finais sobre o estudo realizado, com sugestões de trabalhos futuros.

2 Engenharia Social

Do ponto de vista da Segurança da Informação, entende-se a Engenharia Social como o uso malicioso de métodos sociais que resultam na invasão de um sistema de informação (TETRI; VUORINEN, 2013). Desse ponto de vista, o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br, 2017) define a engenharia social como a técnica por meio da qual uma pessoa procura persuadir outra a executar determinadas ações – uma prática de má-fé, motivada pela ganância e pela vaidade, abusando da ingenuidade e da confiança das pessoas, com a finalidade de obter informações sigilosas e importantes, para aplicar golpes.

Atualmente, a expressão engenharia social é frequentemente associada ao mundo virtual. Rhees (1947), no entanto, a descreve como um processo de organização social, no qual se atribui ao engenheiro social a tarefa de solucionar problemas em uma sociedade, destacando que, como esta não é racional, cabe ao engenheiro social racionalizá-la. Essa tarefa remete ao poder que a figura central da engenharia social pode exercer na condução do comportamento das pessoas.

Segundo Mitnick e Simon (2013), a engenharia social consiste na manipulação casual ou calculada de pessoas, com a intenção de influenciá-las a praticar ações que normalmente não fariam, convencendo-as sem levantar suspeita. As técnicas utilizadas na engenharia social funcionam porque, em geral, os indivíduos confiam em qualquer pessoa que estabeleça credibilidade, tanto no convívio pessoal como no ambiente profissional.

Para Mann (2011), a engenharia social não se resume a uma prática utilizada para acesso aos sistemas de computadores; ela é uma forma de manipular pessoas, com o

intuito de enganá-las para que forneçam informações ou executem ações benéficas tão somente ao agressor. Seguindo o mesmo raciocínio, Hadnagy e Ekman (2014) confirmam que essa prática objetiva mais do que a obtenção de informação; muitas vezes tem como finalidade a execução de uma ação desejada pelo agressor, a qual, na maioria das vezes, não é de interesse do usuário, mera vítima de um golpe (HADNAGY; EKMAN, 2014).

Luo *et al*. (2011) destacam que, geralmente, as pessoas desconhecem o valor das informações, e, embora as pessoas representem o elo mais fraco na prevenção de fraudes, o fator humano tem sido sistematicamente negligenciado quando se aborda a segurança da informação (HADNAGY, 2011; MANN, 2011; MITNICK; SIMON, 2003). A fragilidade estaria relacionada às características humanas identificadas com a tendência natural a seguir instruções, à ignorância, à credulidade, ao desejo de ser amado, ao desejo de ser prestativo (MANN, 2011), assim como à necessidade de aprovação social (HADNAGY, 2011). E no que diz respeito a esse último traço – o da aprovação social –, quanto maior o número de pessoas que acham uma ideia correta, mais um indivíduo irá considerá-la correta (CIALDINI, 2012). Destaca-se que não necessariamente a ideia em questão precisa ser correta, o que importa, nesse caso, é como ela é vista por um grande número de pessoas.

Para obter sucesso, um engenheiro social agressor investe tempo desenvolvendo um relacionamento com a provável vítima do seu ataque. Esse relacionamento normalmente se estabelece estimulado por frequentes interações (PELTIER, 2006), criando-se uma relação de confiança, uma conexão amigável e harmoniosa (WORKMAN, 2007). Há casos, entretanto, em que se faz uso da autoridade, apoiado na tendência natural das pessoas em obedecer a ordens de quem pareça poder emaná-las (CIALDINI, 2012).

O sucesso de ataques de engenharia social é mais facilmente observado quando as pessoas são ingênuas ou desconhecem as boas práticas relacionadas à segurança (MITNICK; SIMON, 2003). Por outro lado, há diversos ataques dessa engenharia que funcionam pela predisposição da vítima em atuar iludida pelo ganho fácil ou até mesmo pela ganância. Qualquer que seja o motivo, independentemente da condição da vítima, essa prática tem se mostrado muito eficiente para os agressores, sendo, por isso, considerada pelas instituições especializadas nesse assunto uma das grandes ameaças aos usuários da internet (CONHEADY, 2014; HADNAGY, 2011; MANN, 2011), já que não é possível criar defesas contra ela apenas com hardware e software (PELTIER, 2006).

2.1 Dimensões de um ataque de engenharia social

Com o objetivo de simplificar o entendimento de como se dá um ataque de engenharia social, Tetri e Vuorinen (2013) destacam que tal problema não deve ser analisado a partir de uma visão unidimensional em que o sucesso das ações do agressor seria atribuído a uma vulnerabilidade específica da vítima, mas sim sob um ponto de vista multidimensional, mais especificamente em três dimensões: persuasão, fabricação e coleta de dados.

A *persuasão* seria o ato de fazer com que uma pessoa execute algo que normalmente não faria, atendendo a uma solicitação inadequada, mesmo contra normas e regulamentos. Para isso, o agressor faz uso de técnicas como o uso de autoridade, apelo emocional, simpatia, estabelecimento de relacionamento, reciprocidade e exploração do sentimento de aprovação social inerente aos seres humanos.

A *fabricação* seriam as ações desenvolvidas na criação de situações, como a interpretação de papéis que confundem a vítima e legitimam a posição do agressor. A fabricação pode ser *soft*, com o uso de palavras e mensagens, e podem ser *hard*, com o

uso de uniformes e crachás, por exemplo. As técnicas utilizadas na fabricação incluem fingir que se age em nome de alguém com autoridade para tal, a representação de alguém com autoridade, o uso de jargões do meio ao qual a vítima pertence e o uso de credenciais falsas.

A *coleta de dados* consiste na aquisição de informações sobre a possível vítima, para se lançar um ataque com maiores chances de sucesso. Em geral, a coleta de dados é realizada antes de se iniciar a interação com a vítima e não é realizada em interações diretas com ela. Muitas vezes uma coleta de dados serve de ponto de partida para uma nova coleta de dados e assim continua até que a informação desejada seja alcançada. Um agressor coleta todas as informações necessárias antes de iniciar um ataque de engenharia social, para aprimorar os detalhes de sua fabricação ou a eficácia de sua persuasão. As técnicas comumente utilizadas na coleta de dados consistem na busca por informações abertas (em sites e redes sociais), busca de informações no lixo da vítima ou organização, escuta de conversas, observação do comportamento da vítima, *phishing* e roubo.

Tetri e Vuorinen (2013) argumentam que as três dimensões raramente aparecem sozinhas em uma técnica de ataque – o mais provável é que a técnica utilizada se manifeste nas três dimensões simultaneamente.

O trabalho de Tetri e Vuorinen (2013) mostra uma visão geral de como pode ser interpretado um ataque de engenharia social a partir das três dimensões propostas e, embora a proposta foque originalmente o ambiente organizacional, essa visão pode ser utilizada em qualquer ambiente em que a engenharia social possa ser aplicada, ou seja, em qualquer interação humana.

Nessa perspectiva, Viana (2017) desenvolveu um estudo baseado no modelo multidimensional de Tetri e Vuorinem (2013). No estudo, foram comparados o comportamento de idosos e o comportamento de pessoas mais jovens, no uso das TICs. O estudo validou as escalas utilizadas na verificação das dimensões propostas e identificou diferenças de comportamento entre os dois grupos pesquisados.

3 Método da pesquisa

Para se atingirem os objetivos deste estudo foi empreendida uma pesquisa com abordagem quantitativa, que se baseia na medição numérica e análise estatística para estabelecer padrões e comprovar teorias (SAMPIERI; COLLADO; LUCIO, 2013), do tipo descritiva, que observa, registra, analisa e correlaciona fenômenos sem manipulá-los (CERVO; BERVIAN; SILVA, 2007).

A população estudada na pesquisa foram os alunos de três cursos técnicos do IFPB Campus Guarabira: Técnico em Informática, Técnico em Edificações e Técnico em Contabilidade integrados ao Ensino Médio. Foi obtida uma amostra de 170 alunos entre os matriculados que frequentavam regularmente as aulas.

Como instrumento de pesquisa, foi utilizado um questionário adaptado de Viana (2017). O questionário foi composto por questões quanto ao perfil dos entrevistados (idade, gênero, área de residência e curso), suas percepções sobre a possibilidade de ser vítima de um golpe na internet e quanto ao nível de vulnerabilidade à engenharia social. Para essa última questão, foram apresentadas 15 afirmações em escala de concordância Likert de onze pontos (0 a 10), cuja marcação corresponderia ao que cada respondente assinalou como seu nível de concordância. As 15 afirmações representavam as três dimensões relacionadas à vulnerabilidade à engenharia social (Coleta de dados, Fabricação

e Persuasão), segundo Tetri e Vuorinen (2013). Para cada dimensão investigada foram propostas cinco afirmações (Quadro 1).

Quadro 1 ▶ Dimensões da vulnerabilidade à engenharia social. *Fonte: elaborado pelos autores, adaptado de Viana (2017)*

Dimensão	Afirmação
Persuasão	1. Na internet, quando alguém faz alguma coisa por mim, sinto que eu deveria fazer o mesmo por ele(a).
	2. Na internet, se eu gosto de alguém, irei ajudá-lo(a) mesmo em situações em que eu provavelmente não deveria.
	3. Eu acho importante seguir o comportamento do grupo do qual eu participo e de pessoas que eu admiro.
	4. Eu forneço a minha senha de e-mail para alguém que demonstre ter autoridade para solicitá-la.
	5. Eu assumo riscos com frequência, se há chance de eu ganhar alguma coisa com isso.
Coleta de dados	1. Eu não me preocupo com os dados pessoais que eu publico nas redes sociais.
	2. Eu publico com frequência, nas redes sociais, fotos de tudo o que eu faço, para deixar minha família e amigos informados.
	3. Eu costumo abrir links que recebo na internet, de origem desconhecida, para saber mais sobre o assunto mencionado.
	4. Para não esquecer a minha senha, eu costumo utilizar palavras conhecidas que me façam lembrá-la com mais facilidade.
	5. Para não esquecer a minha senha, eu costumo escrevê-la em um lugar de fácil acesso.
Fabricação	1. Eu passo informações pessoais em bate-papo com alguém que conheci na internet se a pessoa com quem converso faz o mesmo.
	2. Eu costumo abrir os anexos de e-mails que chegam me oferecendo alguma oportunidade que eu considero vantajosa.
	3. Eu costumo clicar em janelas que aparecem na minha tela (pop-up) solicitando informações ou oferecendo oportunidades.
	4. Na internet, eu confio nas pessoas que mostram que gostam das mesmas coisas de que eu gosto.
	5. Na internet, pessoas que se mostram amigáveis são, normalmente, confiáveis.

O questionário adaptado foi submetido a um pré-teste, o qual foi respondido por 15 alunos – 5 alunos de cada um dos cursos. Como resultado, o questionário se mostrou adequado, sem a necessidade de modificações. Em seguida, o instrumento de pesquisa foi disponibilizado no formato on-line para ser preenchido pelos alunos dos três cursos técnicos integrados ao Ensino Médio do Campus Guarabira do Instituto Federal da Paraíba (Técnico em Informática, Técnico em Edificações e Técnico em Contabilidade). Para sua divulgação, foram utilizadas as redes sociais virtuais dos pesquisadores, assim como foram utilizados grupos em aplicativos de mensagens, com o intuito de se obter o maior número possível de respondentes.

A análise dos dados foi realizada considerando a média geral dos níveis assinalados pelos respondentes (nas escalas Likert de 0 a 10), por dimensão, no confronto com os objetivos propostos (nível de vulnerabilidade, diferença de comportamento quanto ao curso que estudam, quanto ao porte da cidade e área que residem). Para a verificação

de diferença de comportamento dos alunos quanto ao porte da cidade de residência, as cidades registradas por eles no questionário foram inicialmente classificadas em ordem crescente, de acordo com os números de habitantes estimados, obtidos no Instituto Brasileiro de Geografia e Estatística (IBGE). A Tabela 1 traz a relação das cidades e sua classificação quanto ao porte.

Tabela 1 ▶
Classificação das cidades quanto ao porte.
Fonte: IBGE (2020)

Classificação	Cidade	População
1	Serra da Raiz	3131
2	Riachão	3619
3	Pilõezinhos	4955
4	Sertãozinho	5089
5	Caldas Brandão	6046
6	Pilões	6576
7	Caiçara	7191
8	Mulungu	9932
9	Dona Inês	10413
10	Pirpirituba	10584
11	Tacima	10969
12	Alagoinha	14560
13	Araçagi	16921
14	Belém	17705
15	Itapororoca	18823
16	Mari	21866
17	Solânea	26227
18	Alagoa Grande	28439
19	Sapé	52804
20	Guarabira	59115

Após a classificação, foi aplicado um teste estatístico de correlação, com o intuito de observar se há, de fato, correlação entre o porte da cidade e o comportamento dos alunos residentes em relação à vulnerabilidade à engenharia social. Como referência para os níveis de intensidade de correlação foram adotados os valores do Quadro 2. Além do teste de correlação, foram utilizados testes para verificar a normalidade dos dados (Shapiro-Wilk) e testes para a comparação de grupos (Mann-Whitney).

Quadro 2 ▶
Níveis de intensidade de correlação.
Fonte: dados da pesquisa

Resultado da correlação (+ ou -)	Intensidade da correlação
De 0,00 a 0,19	Inexistente ou muito fraca
De 0,20 a 0,39	Fraca
De 0,40 a 0,69	Moderada
De 0,70 a 0,89	Forte
De 0,90 a 1,00	Muito forte ou perfeita

Para a tabulação dos dados, análises quantitativas e testes estatísticos, foram utilizados os softwares Statistical Package for the Social Sciences (SPSS 20) e a planilha eletrônica CALC, do pacote LibreOffice®.

4 Resultados e discussão

No tratamento inicial dos dados, foi observado que dois respondentes confundiram os campos de respostas, preenchendo o campo criado para idade com o nome da cidade na qual residiam. Como solução, esses campos foram substituídos pela idade com maior frequência para o curso do respectivo respondente, não interferindo, dessa forma, nos resultados das análises estatísticas empreendidas, obtendo-se, ao final, 170 respondentes.

Do total de respondentes, 45,29% (77) eram do gênero masculino e 54,71% (93) do gênero feminino. A faixa etária com o maior número de respondentes foi a de "14 a 19 anos", 97,65% (166), obtendo-se apenas 2,35% (4) dos respondentes na faixa etária de "mais de 20 anos". Sobre a área onde os respondentes residiam, foi registrada a maior presença na área urbana, com 80,59% (137), ficando a zona rural com 19,41% (33) dos respondentes. Observou-se também que o curso com maior número de respondentes foi o de Informática, com 41,76% (71), seguido de Edificações com 30% (51) e Contabilidade com 28,24% (48).

Com o instrumento de pesquisa, também foi registrado o número de alunos em relação ao ano que cursavam. O ano com maior número de respondentes foi o 1º, com 28,82% (49), logo em seguida o 2º ano, com 27,06% (46), depois o 3º ano, com 22,94% (39) e, por último, o 4º ano, com 21,18% (36). Esses dados podem ser visualizados agrupados na Tabela 2.

Tabela 2 ▶
Gênero, idade, área, curso e ano.
Fonte: dados da pesquisa

Aspecto	Caracterização	n	%
Gênero	Masculino	77	45,29
	Feminino	93	54,71
Faixa etária	14 a 19 anos	166	97,65
	20 anos ou mais	4	2,35
Zona	Urbana	137	80,59
	Rural	33	19,41
Curso	Informática	71	41,76
	Contabilidade	48	28,24
	Edificações	51	30
Ano	1°	49	28,82
	2°	46	27,06
	3°	39	22,94
	4°	36	21,18

Para atingir o primeiro objetivo da pesquisa, foi necessário conhecer a percepção de vulnerabilidade dos alunos sobre a possibilidade de ser vítima de um golpe na internet. Para tanto, no questionário foi disponibilizada uma questão (Q1 - *Acredito que a*

possibilidade de eu cair em um golpe na internet é:), para que o respondente assinalasse a possibilidade de cair em um golpe na internet em uma escala variando de 0 (zero) a 10 (dez) – quanto mais próximo de dez, mais o aluno acredita estar vulnerável a um golpe. Essa questão apresentou como média geral 4,21, valor abaixo do ponto médio da escala (5,0).

Para o desenvolvimento das demais análises de dados, as questões correspondentes a cada uma das dimensões estudadas (Persuasão, Coleta de dados e Fabricação) foram agrupadas com o uso da média, formando, assim, a média da dimensão persuasão (variável MP), a média da dimensão coleta de dados (variável MC) e a média da dimensão fabricação (variável MF). A Tabela 3 exibe as médias correspondentes às dimensões e a Q1 em relação ao curso e área de residência dos alunos. Todas as médias apresentaram valor abaixo do ponto médio da escala (5,0).

Tabela 3 ▶
Médias obtidas para as variáveis da pesquisa.
Fonte: dados da pesquisa

Variável	Médias para cursos e zonas de residência					
	Geral	I	C	E	U	R
Q1	4,21	3,77	4,75	4,29	4,06	4,82
MP	3,50	3,22	3,85	3,56	3,39	3,93
MC	3,04	2,26	3,64	3,57	2,86	3,81
MF	1,43	1,17	1,68	1,54	1,34	1,78

Legenda: I – Informática; C – Contabilidade; E – Edificações; U – Urbana; R – Rural.

Após o agrupamento das dimensões em suas respectivas variáveis, foi realizado o teste de normalidade de Shapiro-Wilk. Como resultado, todas as dimensões apresentaram um *p*-valor menor que 0,05, indicando que as dimensões não apresentavam uma distribuição normal. Os resultados do teste de Shapiro-Wilk podem ser visualizados na Tabela 4.

Tabela 4 ▶
Teste de normalidade.
Fonte: dados da pesquisa

Teste de Shapiro-Wilk	
Dimensão	p-valor
MP	0,004
MC	0,001
MF	0,000

Como não foi verificada a ocorrência de distribuição normal em nenhuma das variáveis, utilizou-se o teste não paramétrico de Mann-Whitney e as medianas obtidas para cada variável na comparação do comportamento dos respondentes separados em grupos.

O teste Mann-Whitney apontou comportamentos diferentes entre os alunos, separados por curso, em duas das três dimensões (variáveis) estudadas. Nos testes, foram obtidos valores de *p*-valor inferiores a 0,05 para as dimensões MC (*p*-valor = 0,000) e MF (*p*-valor = 0,029) entre os cursos de Informática e Contabilidade, indicando comportamentos distintos entre eles. Também foi observada diferença de comportamento para a dimensão MC (*p*-valor = 0,000) entre os cursos de Informática e Edificações.

Quando levadas em consideração as medianas obtidas, pode-se observar que os alunos do curso de Informática apresentaram um nível de vulnerabilidade menor para a dimensão MC (mediana = 2,00) em relação aos alunos do curso de Contabilidade (mediana = 3,8) e aos do curso de Edificações (mediana = 3,4). Para a dimensão MF, os alunos do curso de Informática também apresentaram um nível de vulnerabilidade inferior (mediana = 0,8) ao dos alunos do curso de Contabilidade (mediana 1,6).

Na comparação entre os alunos separados em grupos de acordo com a região onde residiam, área urbana ou área rural, foi observada diferença de comportamento apenas para a dimensão MC (*p*-valor = 0,011), em que os alunos residentes na zona urbana exibiram um nível de vulnerabilidade inferior (mediana = 2,6) ao dos alunos residentes na zona rural (mediana = 4,0).

Ainda na comparação entre grupos, dos testes relacionados à variável Q1, apenas o comportamento dos alunos dos cursos de Informática e de Contabilidade mostraram diferença estatística significativa (*p*-valor = 0,036) – os alunos do curso de Informática apresentaram um menor nível de percepção de vulnerabilidade (mediana = 4,0) comparado ao nível de percepção registrado pelos alunos do curso de Contabilidade (mediana = 5,0). Esses dados podem ser visualizados na Tabela 5.

Tabela 5 ▶
Comparação entre grupos.
Fonte: dados da pesquisa

Medianas					
Variável	I	C	E	U	R
MP	3,2	4,2	3,4	3,2	4,2
MC	2,0	3,8	3,4	2,6	4,0
MF	0,8	1,6	1,2	1,0	1,4
Q1	4,0	5,0	4,0	4,0	5,0
Mann-Whitney (p-valor)					
Variável	I x C	I x E	C x E	U x R	
MP	0,112	0,389	0,587	0,183	
MC	0,000	0,000	0,861	0,011	
MF	0,029	0,085	0,652	0,230	
Q1	0,036	0,478	0,242	0,058	

Legenda: I – Informática; C – Contabilidade; E – Edificações; U – Urbana; R – Rural.

Para verificar se o porte da cidade onde os respondentes residiam exercia alguma influência no nível de vulnerabilidade apresentado, foi realizado o teste de correlação de Spearman (*rs*) entre a variável Cidade (cidades classificadas quanto ao porte) e as variáveis (dimensões) MP, MC, MF e Q1. Adicionalmente, verificou-se se havia correlação entre a variável Q1 e as variáveis MP, MC e MF. Os resultados podem ser visualizados na Tabela 6.

Tabela 6 ▶
Correlações entre as variáveis.
Fonte: dados da pesquisa

Teste de Spearman	
Variáveis	*rs*
Cidade x Q1	-0,047
Cidade x MP	-0,060
Cidade x MC	-0,079
Cidade x MF	0,015
Q1 x MP	0,236
Q1 x MC	0,182
Q1 x MF	0,266

Com os testes de Spearman, verificou-se correlações estatisticamente significativas apenas entre a variável Q1 e a dimensão MP e entre a variável Q1 e a dimensão MF, ambas correlações positivas, indicando que quanto maior a percepção de vulnerabilidade (Q1), maior o nível de vulnerabilidade para as dimensões Persuasão (MP) e Fabricação (MF), embora tenham mostrado correlações fracas.

Uma última análise foi realizada com a verificação, por meio da média, do nível de vulnerabilidade dos alunos para cada uma das 15 afirmações (Quadro 1) que compunham as três dimensões estudadas. Os resultados são apresentados na Tabela 7.

Tabela 7 ▶
Médias para as afirmações das dimensões.
Fonte: dados da pesquisa

Dimensão	A. 1	A. 2	A. 3	A. 4	A. 5
Persuasão	5,65	4,25	4,46	1,37	1,75
Coleta de dados	1,62	1,35	2,55	5,58	4,11
Fabricação	4,11	1,11	1,66	1,12	1,62

As médias obtidas mostraram um nível de vulnerabilidade acima do ponto médio da escala (5,0) para dois comportamentos: a Afirmação 1 da dimensão Persuasão, que corresponde a "*Na internet, quando alguém faz alguma coisa por mim, sinto que eu deveria fazer o mesmo por ele(a)*", com média 5,65; e a Afirmação 4 da dimensão Coleta de Dados, que corresponde a "*Para não esquecer a minha senha, eu costumo utilizar palavras conhecidas que me façam lembrá-la com mais facilidade*", com média 5,58.

5 Considerações finais

Os resultados obtidos com a pesquisa realizada mostraram um nível de vulnerabilidade à engenharia social baixo entres os alunos dos cursos técnicos em Informática, Contabilidade e Edificações integrados ao Ensino Médio do Instituto Federal da Paraíba – Campus Guarabira, quando considerado o instrumento utilizado e o ponto médio das escalas apresentadas aos respondentes. Também foi verificado um nível baixo em relação à percepção dos alunos sobre a possibilidade de caírem em um golpe na internet.

Quando comparados os resultados separados em grupos, por curso e área de residência, observou-se que os alunos do curso de Informática apresentaram, com significância estatística, um menor nível de vulnerabilidade à engenharia social na dimensão Coleta

de Dados em relação aos alunos dos cursos de Contabilidade e Edificações, e um menor nível de vulnerabilidade na dimensão Fabricação em relação aos alunos do curso de Contabilidade. Também foi observada (com significância estatística) diferença entre a percepção de vulnerabilidade sobre a possibilidade de cair em um golpe na internet entre os alunos do curso de Informática e Contabilidade, situação em que os discentes do curso de Contabilidade apresentaram uma maior percepção de risco. Já em relação à zona de residência, apenas na dimensão Coleta de Dados foi observada diferença com significância estatística, com um maior nível de vulnerabilidade para os alunos residentes na área rural.

Nos resultados não foram encontradas correlações estatisticamente significativas entre o porte da cidade e o nível de vulnerabilidade à engenharia social apresentado pelos alunos. Apenas quando comparadas as respostas sobre a percepção de vulnerabilidade dos alunos em cair em um golpe na internet e as dimensões da engenharia social analisadas é que foram observadas correlações positivas entre essa percepção e as dimensões Persuasão e Fabricação, todavia em níveis baixos, indicando correlações fracas.

Embora o nível geral de vulnerabilidade à engenharia social tenha se mostrado baixo entre os alunos, quando as afirmações são observadas isoladamente, duas delas apresentaram médias acima do ponto central da escala, indicando que são situações que merecem especial atenção em relação ao comportamento dos alunos. Uma dessas afirmações representa uma situação comumente utilizada na internet por engenheiros sociais, em que pessoas tentam criar relação de confiança fazendo favores para obter retribuições. A segunda afirmação corresponde ao uso de palavras comuns na criação de senhas, o que facilita a ação de hackers na obtenção de acesso não autorizado.

Por fim, registra-se que os resultados desta pesquisa não podem ser generalizados, pois o estudo possui limitações em sua execução, como a obtenção de respondentes por conveniência e o acesso limitado de alunos à pesquisa em consequência do momento de pandemia de covid-19 vivenciado. Assim, sugere-se a reprodução desta pesquisa em outros *campi*, com o objetivo de se obter uma amostra maior e mais diversificada.

Agradecimentos

Esse projeto contou com o apoio da Pró-Reitoria de Pesquisa, Inovação e Pós-Graduação do IFPB, por meio do edital Chamada Interconecta 01/2020.

Declaração do Conselho de Ética

Parecer número 3.985.362.

Referências

ABNT – ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27002**: Tecnologia da informação: Técnicas de Segurança: Código de prática para a gestão da segurança da informação. Rio de Janeiro: ABNT, 2007.

CERT.br – CENTRO DE ESTUDOS, RESPOSTAS E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL. **Cartilha de segurança para internet**. 2017. Disponível em: https://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf. Acesso em: 10 fev. 2020.

CERVO, A. L.; BERVIAN, P. A.; SILVA, R. **Metodologia científica**. 6. ed. São Paulo: Pearson Prentice Hall, 2007.

CIALDINI, R. B. **As armas da persuasão**: como influenciar e não se deixar influenciar. Rio de Janeiro: Sextante, 2012.

CONHEADY, S. **Social engineering in IT security**: tools, tactics, and techniques. New York: McGraw-Hill Education, 2014.

CÔRTES, P. D. **Administração de sistemas de informação**. São Paulo: Saraiva, 2008.

COULDRY, N.; MEJIAS, U. A. Data colonialism: rethinking big data's relation to the contemporary subject. **Television & New Media**, v. 20, n. 4, p. 336-349, 2019. DOI: https://doi.org/10.1177%2F1527476418796632.

HADNAGY, C. **Social engineering**: the art of human hacking. Indianapolis: Wiley, 2011.

HADNAGY, C.; EKMAN, P. **Unmasking the social engineer**: the human element of security. Indianapolis: Wiley, 2014.

IBGE – INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA. **Cidades e estados**. 2020. Disponível em: https://www.ibge.gov.br/cidades-e-estados. Acesso em: 16 nov. 2020.

LUO, X.; BRODY, R.; SEAZZU, A.; BURD S. Social engineering: the neglected human factor for information security management. **Information Resources Management Journal**, v. 24, n. 3, p. 1-8, 2011. DOI: http://dx.doi.org/10.4018/irmj.2011070101.

MANN, I. **Engenharia Social**. São Paulo: Blucher, 2011.

MARTIN, N.; RICE, J. Spearing high net wealth individuals: the case of online fraud and mature age internet users. **International Journal of Information Security and Privacy**, v. 7, n. 1, p. 1-15, 2013. DOI: https://dx.doi.org/10.4018/jisp.2013010101.

MITNICK, K. D.; SIMON, W. L. **A arte de enganar**. Ataques de hackers: controlando o fator humano na segurança da informação. São Paulo: Pearson Makron Books, 2003.

MITNICK, K. D.; SIMON, W. L. **Fantasma no sistema**: minhas aventuras como o hacker mais procurado do mundo. Rio de Janeiro: Alta Books, 2013.

PELTIER, T. R. Social engineering: concepts and solutions. **Information Systems Security**, v. 15, n. 5, p. 13-21, 2006. DOI: https://doi.org/10.1201/1086.1065898X/46353.15.4.20060901/95427.3.

RHEES, R. Social engineering. **Mind**, v. LVI, n. 224, p. 317-331, 1947. DOI: https://doi.org/10.1093/mind/LVI.224.317.

SAMPIERI, R. H.; COLLADO, C. F.; LUCIO, P. B. **Metodologia de pesquisa**. 5. ed. Porto Alegre: Penso, 2013.

TETRI, P.; VUORINEN, J. Dissecting social engineering. **Behaviour & Information Technology**, v. 32, n. 10, p. 1014-1023, 2013. DOI: http://dx.doi.org/10.1080/0144929X.2013.763860.

VIANA, J. A. L. **O uso das tecnologias de informação e comunicação na terceira idade e a vulnerabilidade à engenharia social**. 2017. 107 f. Dissertação (Mestrado em Administração) – Centro de Ciências Sociais, Universidade Federal da Paraíba, João Pessoa, 2017. Disponível em: https://repositorio.ufpb.br/jspui/handle/tede/9378. Acesso em: 20 ago. 2022.

WORKMAN, M. Gaining access with social engineering: an empirical study of the threat. **Information Systems Security**, v. 16, n. 6, p. 315-331, 2007. DOI: https://doi.org/10.1080/10658980701788165.