Uma breve noção sobre o comportamento dos internautas em relação à segurança na rede

Leonardo Pinto Guilherme, Matheus Fernandes Ferreira, Gustavo Mello da Fonseca, Nilson M.Lazarin

[1]Bacharelado em Sistemas de Informação – Centro Federal de Educação Tecnológica Celso Suckow da Fonseca (Cefet/RJ) – Nova Friburgo, RJ – Brazil

lpinto39@yandex.com,{mattheusfferreira,gugamello40,nilsonmori}@gmail.com

Abstract. *Amid the hostile Internet scenario, the COVID-19 pandemic, unleashed in 2020, presents itself as a problematic factor for digital security. With more people connected to the Internet to carry out countless essential activities, the risks related to information security in this environment also grow. Meanwhile, many authors reinforce the role of digital education in building a safer online environment. Therefore, this article aims to analyze, from a sample obtained in a field research, how the instruction or not to responsible use of the network can influence a safer navigation for the user.*

Resumo. *Em meio ao cenário hostil da Internet, a pandemia da COVID-19, deflagrada em 2020, apresenta-se como um fator problemático para segurança digital. Com mais pessoas conectadas à Internet para realizar inúmeras atividades essenciais, crescem também os riscos relacionados à segurança da informação neste ambiente. Enquanto isso, muitos autores reforçam o papel da educação digital na construção de um ambiente online mais seguro. Para tanto, este artigo tem o objetivo de analisar, a partir de uma amostra obtida em uma pesquisa de campo, como a instrução ou não ao uso responsável da rede pode influenciar em uma navegação mais segura ao usuário.*

1. Introdução

Considerado um país altamente visado para ataques cibernéticos, o Brasil já ocupou a segunda colocação no mundo em prejuízos econômicos devido aos ciberataques. Pessoas, empresas e órgãos públicos são alvos simultâneos de inúmeros golpes diários que se inovam a cada ano para fazer novas vítimas. Apesar de ser um dos países mais conectados à rede mundial de computadores, tais fatos demonstram a fragilidade do ciberespaço brasileiro em relação a segurança [ITU 2019].

O cenário hostil da Internet se tornou mais evidente a partir de março de 2020, quando a Organização Mundial da Saúde decretou a pandemia do novo coronavírus (COVID-19). Como resposta para interromper as cadeias de transmissão do vírus respiratório e disseminado pelo ar, governos adotaram estratégias de distanciamento físico e forçaram uma mudança de comportamento social de pessoas, que gerou uma procura massiva e maior dependência dos recursos de TI para manter as atividades de trabalho, estudos e lazer. Por outro lado, tal mudança fez surgir uma escalada de ataques cibernéticos [Nagli 2020].

Esta fragilidade do ciberespaço em relação a segurança, potencializada pela pandemia da COVID-19 e que ameaça internautas possui como prevenção as medidas de educação digital ou cibereducação, isto é, o conhecimento, a cultura, as práticas e os hábitos das pessoas no ambiente digital. Assim, entende-se que a proporção de ataques cibernéticos em um país não está necessariamente relacionada ao tamanho da sua população conectada, mas ao preparo desta mesma população durante a navegação online. Isso significa que os ataques cibernéticos ocorrem de maneira oportunista, pois quanto maior é o despreparo de um indivíduo ao navegar na Internet, maior será a probabilidade de um ataque bem-sucedido e, consequentemente, maior o interesse de criminosos em buscar novas vítimas [Nagli 2020] [Carvalho and Marques 2017].

Este artigo apresenta uma pesquisa em que se buscou compreender como a pandemia da COVID-19 influenciou a rotina de internautas, com vistas na identificação de comportamentos de risco e a sua possível relação com o nível de conhecimento das pessoas. O objetivo é relacionar o conhecimento e o comportamento dos indivíduos com os riscos encontrados na rede, ou seja, como a cultura digital de uma pessoa influencia na navegação segura. Para isso, usuários da rede foram convidados a responder um questionário online sobre o perfil e hábitos online.

2. Trabalhos Relacionados

O trabalho de [Nagli 2020] evidencia como as medidas de distanciamento social, adotadas por influência da pandemia da COVID-19, inseriram novos adeptos ao ambiente de trabalho remoto. Esta súbita exposição à rede, sem os cuidados adequados, propiciou uma escalada de ataques cibernéticos, em que classifica como uma "pandemia na pandemia" e compara os cuidados necessários ao enfrentamento da COVID-19 com os cuidados para se evitar os golpes digitais. Em sua análise, defende que empresas devem se empenhar na capacitação de seus colaboradores a partir da educação digital.

Em [Pimenta and Quaresma 2016], é analisado de que maneira os comportamentos e as atitudes dos usuários podem constituir um risco ou uma defesa na segurança nos sistemas de informação nas organizações. A principal conclusão do estudo revela que os usuários, de uma forma geral, são uma parte bem importante para a proteção da segurança dos sistemas de informação nas organizações.

Já o trabalho de [Carvalho and Marques 2017] descreve os conceitos de Cibersegurança e de Segurança da Informação. Abordam de forma sucinta o conceito de cibercrime e são descritos os principais tipos de ataques informáticos existentes. Ao final apresenta um compêndio das principais ofertas formativas na área da cibersegurança existente nas principais instituições de ensino superior em Portugal. Chegam à consideração que a prevenção somente será alcançada com a aposta em dois pilares fundamentais: o desenvolvimento tecnológico e a formação dos utilizadores.

Este artigo utiliza a premissa que é comum aos três artigos mencionados acima: a segurança digital de um indivíduo diretamente relacionada ao seu comportamento online. Em vez de apresentar conceitos e fatos que reforçam essa relação de causa e efeito, este trabalho tem como objetivo de colocá-la à prova, isto é, se o preparo de um indivíduo para fazer uma navegação segura realmente atende a esta expectativa em uma pesquisa com internautas.

3. Metodologia

Para esta pesquisa, foi elaborado um questionário online para conhecer o perfil, avaliar o conhecimento e compreender o comportamento dos respondentes em relação a segurança na rede. A pesquisa foi compartilhada com o público geral, não foram escolhidos grupos específicos de usuários, através das redes sociais e grupos de aplicativos de mensagens de contatos dos autores. A participação foi anônima. Cada respondente precisou informar às seguintes questões:

- **Faixa etária**: até 25, de 26 a 44 anos, de 45 a 64 anos, de 65 a 80 anos ou acima de 80 anos. Estas faixas representam as gerações em relação à tecnologia, dadas as transformações do mundo ao longo das últimas décadas. As faixas etárias correspondem, respectivamente, às gerações Z, Y, X, Baby Boomers e Traditionalists;
- **Escolaridade**: se concluiu a escolaridade mais elevada entre ensino fundamental, médio, superior ou uma pós-graduação;
- **Uso da internet**: tempo em que está ativo na Internet por dia até 1 hora, até 2 horas, até 4 horas, até 8 horas, até 12 horas ou mais de 12 horas;
- **Uso de aplicativos**: a influência da pandemia no tempo de uso em aplicativos "internet banking", "aplicativos e sites para compras online", "aplicativos de mensagem instantânea", "aplicativos de trabalho remoto", "aplicativos de ensino remoto", portais e sites de notícia" e "redes sociais" eram a opções disponíveis aos respondentes. Para cada uma, deveria indicar se "passou a utilizar mais", "passou a utilizar menos" ou "indiferente";
- **Experiência em golpes**: se o respondente ou um conhecido já foi vítima de um golpe digital ou não dentre uma lista — em caso afirmativo, era possível selecionar a opção ele próprio e um conhecido. Os golpes da lista foram "alguém que tentou se passar por um conhecido para pedir dinheiro", "uma conta de aplicativo ou site invadida", "SMS falso que diz ser do banco", "uma compra em uma loja virtual falsa", "dados pessoais indevidamente usados por outra pessoa ou empresa", "dados de cartão de crédito roubados" e "chantagem com fotos íntimas";
- **Capacitação**: no uso da Internet, se recebeu treinamentos ou não de como navegar de maneira segura na Internet. Em caso afirmativo, o respondente deveria indicar se recebeu treinamentos na empresa em que trabalha, em uma instituição de ensino ou se buscou instruções por conta própria — era possível selecionar mais de uma opção, quando aplicável. Considera-se como treinamento o acesso a cartilhas, guias, cursos, palestras ou outras formas de conscientização sobre o uso seguro da Internet;
- **Comportamento**: se, alguma vez na vida, "baixou programas aplicativos, programas ou arquivos de origem duvidosa", "compartilhou celular ou computador com outras pessoas", "compartilhou conta pessoal de aplicativos ou sites com outras pessoas", "compartilhou dados de cartão de crédito em aplicativos de mensagem", "utilizou a mesma senha em vários aplicativos e sites", "clicou em links contidos em links estranhos" e "acessou conta bancária em wi-fi público". Para cada um destes itens, o respondente deveria selecionar "alguma vez sim", "sempre" ou "nunca".

Com os dados obtidos, foram analisados o perfil dos respondentes e as suas experiências com golpes digitais. As informações sobre a capacitação de usuários ao uso seguro da Internet foram utilizadas para identificar a possível relação com os comportamentos de risco listados.

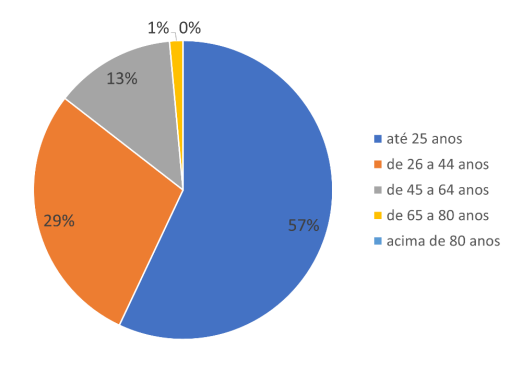

Figura 1. Faixa etária

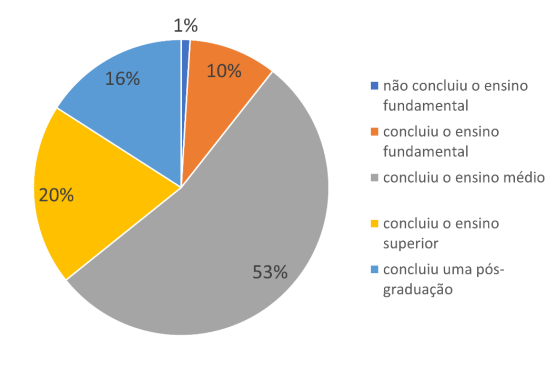

Figura 2. Escolaridade

4. Resultados

Um total de 207 pessoas participaram da pesquisa entre os meses de Abril e Maio de 2021. A maioria dos respondentes (118) tem idade de até 25 anos, completou o ensino médio (111) ou alguma formação superior (74). O perfil predominante dos respondentes é de pessoas de até 44 anos com, pelo menos, o nível secundário de escolaridade. Os resultados sobre a faixa etária são apresentados na Figura 1. Os resultados sobre a escolaridade são apresentados na Figura 2.

Quando questionados sobre o tempo em que passam conectados à Internet, o resultado foi um misto de respostas com a maior parcela (68) indicando estar mais da metade do dia conectados. Aqueles que estão conectados por menos tempo são a parcela mais ínfima dentre os respondentes. Os resultados sobre a conectividade são apresentados na Figura 3.

Sobre a capacitação, quase a metade dos respondentes buscou obter melhor conhecimento e preparo para a navegação segura. Empresas e instituições de ensino, porém, desempenham um papel pouco significativo nesta parcela. Aqueles que dizem nunca ter obtido qualquer tipo de instrução representam uma parcela significativa. Os resultados sobre o treinamento são apresentados na Figura 4.

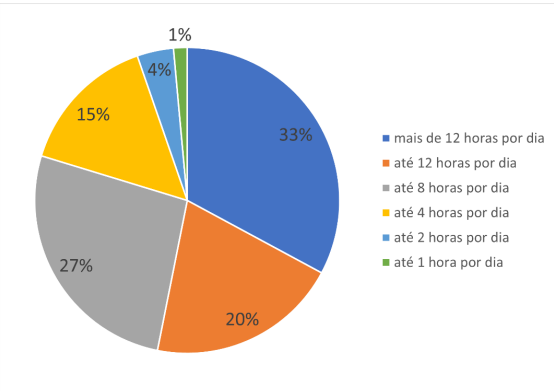

Figura 3. Conectividade.

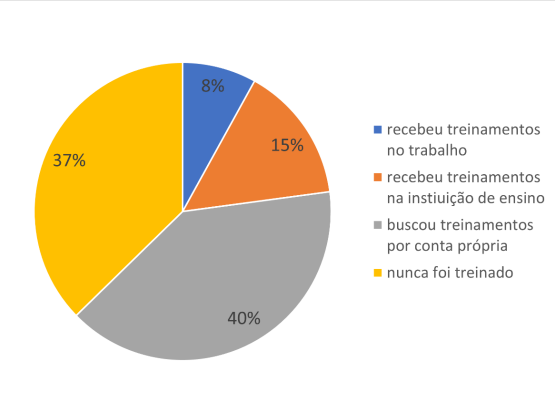

Figura 4. Treinamento.

Para a maioria, a pandemia da COVID-19 influenciou o maior tempo de uso em aplicativos de banco, compras online, mensagem instantânea, trabalho remoto, ensino

remoto, portais de notícias ou redes sociais. Uma parcela expressiva, mas em menor proporção, disse não ter se influenciado pela crise sanitária. Os resultados sobre o uso de aplicativos é apresentada na Figura 5.

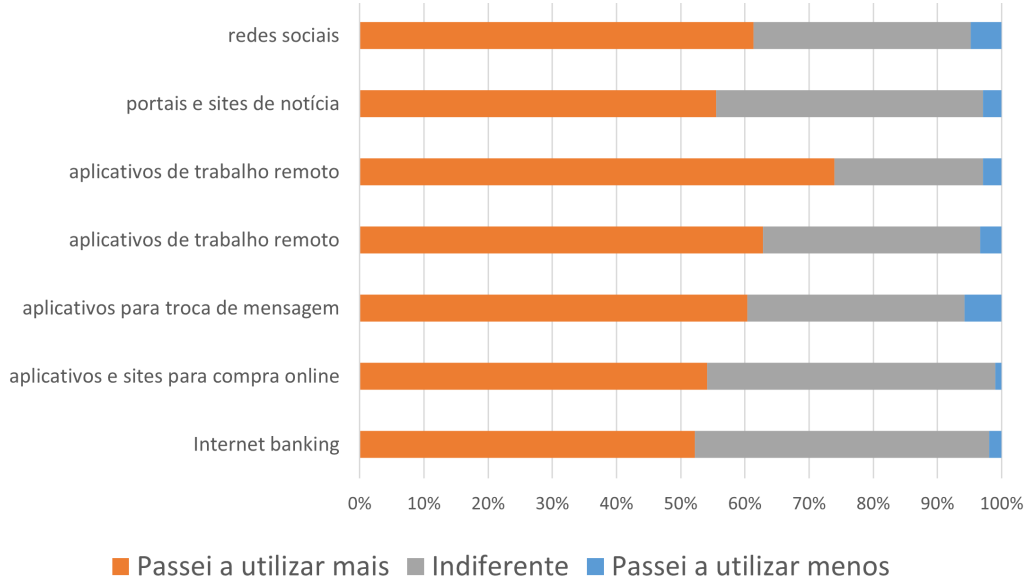

Figura 5. Uso de App.

Conforme apresentado na Figura 6, os internautas responderam se já foram ou conhecem uma vítima em cada um dos golpes listados. Enquanto uma parcela relevante diz não ser ou desconhecer vítimas, a experiência de internautas com golpes digitais é predominante.

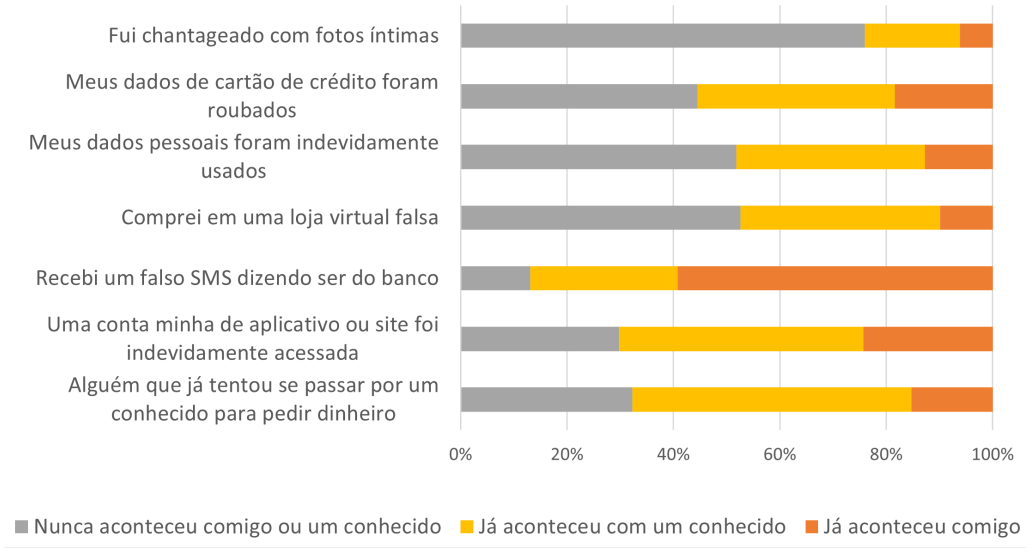

Figura 6. Golpes digitais.

Para analisarmos o comportamento dos usuários, dividimos os dados obtidos em dois grupos: aqueles que foram treinados sobre como fazer uma navegação segura (119) e aqueles que nunca foram treinados (88).

Conforme apresentado na Tabela 1, o grupo não treinado revela uma grande preferência em utilizar a mesma senha em diferentes serviços online e confiam em instalar aplicativos desconhecidos em seus dispositivos, além de admitir que outras pessoas podem utilizar o seu computador ou celular. Por outro lado, tende a rejeitar mensagens estranhas e utilizar o *internet banking* em redes compartilhadas.

Com Treinamento				Sem Treinamento		
Nunca	**Alguma Vez**	**Sempre**	**COMPORTAMENTO**	**Nunca**	**Alguma Vez**	**Sempre**
20,00%	69,17%	10,83%	**Baixar aplicativos, programas ou arquivos de origem duvidosa**	15,91%	71,59%	12,50%
26,67%	57,50%	15,83%	**Compartilhar celular ou computador com outras pessoas**	32,95%	53,41%	13,64%
53,33%	40,00%	6,67%	**Compartilhar conta pessoal de aplicativo ou site com outras pessoas**	52,27%	42,05%	5,68%
65,83%	29,17%	5,00%	**Compartilhar dados de cartão de crédito em aplicativo de mensagem**	64,77%	29,55%	5,68%
12,50%	50,83%	36,67%	**Utilizar a mesma senha em mais de um aplicativo ou site**	3,41%	52,27%	44,32%
80,00%	17,50%	2,50%	**Clicar em links contidos em e-mails estranhos**	69,32%	23,86%	6,82%
72,50%	23,33%	4,17%	**Acessar conta bancária online em wi-fi público**	79,55%	15,91%	4,55%

Tabela 1. Comportamento

Por fim, o grupo treinado não parece se distinguir significativamente do grupo não treinado. Em termos percentuais, a proporção daqueles que dizem sempre ou alguma vez cometer os hábitos listados é ainda maior comparado ao grupo não capacitado. De maneira geral, ambos os possuem os mesmos padrões de comportamento.

5. Conclusão

Os efeitos da pandemia da COVID-19 evidenciam a disposição das pessoas em se manterem mais tempo conectadas para os seus afazeres diários, uma informação que corrobora com a afirmação de mais da metade dos respondentes que dizem usar a Internet por pelo menos a metade do dia. Como mencionado neste artigo, tal fato abre uma janela de oportunidades para pessoas mal-intencionadas, especialmente por causa dos maus hábitos e da ingenuidade de uma parcela expressiva dos internautas.

Com os resultados obtidos nesta pesquisa, surge a necessidade de compreender o porquê de internautas, mesmo instruídos ao bom uso da Internet, insistirem em más práticas que colocam em risco a sua segurança digital. Quando a capacitação das pessoas não se faz suficiente para reverter os comportamentos de risco, encontrar os fatores que influenciam esta cultura é essencial para orientar estratégias e investimentos.

Considera-se relevante destacar o contraditório receio dos respondentes em acessar o internet banking em redes públicas enquanto, no mesmo dispositivo, instalam aplicativos de autoria duvidosa. Desconhecendo o fato de que mesmo em lojas oficiais diversos aplicativos falsos e maliciosos estão disponíveis para download e todos os anos, centenas de malwares são detectados [Malik and Khatter 2020].

Embora não se tenha encontrado uma forte relação entre comportamentos de risco e a educação digital nos resultados, conforme apresentado por [Nagli 2020] e [Carvalho and Marques 2017], os perigos da Internet continuam associados às condutas de cada indivíduo, uma vez que apresentam evidências suficientes. Neste contexto, trabalhos futuros podem avaliar a qualidade do treinamento recebido pelos usuários e/ou avaliar a grade curricular dos treinamentos oferecidos.

Referências

Carvalho, A. A. R. and Marques, M. R. M. (2017). CIBEREDUCAÇÃO COMO MEDIDA PREVENTIVA NO COMBATE AO CIBERCRIME. *Revista Científica Sobre*

Cyberlaw do Centro de Investigação Jurídica do Ciberespaço – CIJIC – Da Faculdade de Direito da Universidade de Lisboa, (nº IV):11–39.

ITU (2019). *Global Cybersecurity Index 2018*. International Telecommunication Union (ITU), Geneva - Switzerland.

Malik, S. and Khatter, K. (2020). Malicious application detection and classification system for android mobiles. In *Cognitive Analytics: Concepts, Methodologies, Tools, and Applications*, pages 122–142. IGI Global.

Nagli, L. S. D. (2020). PANDEMIA NA PANDEMIA: A ESCALADA DE ATAQUES CIBERNÉTICOS PÓS COVID-19. In *Anais do Congresso Transformação Digital 2020 (CTD 2020)*, São Paulo. Fundação Getulio Vargas.

Pimenta, A. M. S. and Quaresma, R. F. C. (2016). A SEGURANÇA DOS SISTEMAS DE INFORMAÇÃO E O COMPORTAMENTO DOS USUÁRIOS. *JISTEM - Journal of Information Systems and Technology Management [online]*, v. 13, n. 3:533–552.