ESTRATÉGIAS DE SEGURANÇA CIBERNÉTICA: COMO PROTEGER A SUA INTEGRIDADE VIRTUAL

CYBER SECURITY STRATEGIES: HOW TO PROTECT YOUR VIRTUAL INTEGRITY

Maria Luiza de Almeida Ruiz
Pedro Henrique Manxini Melo
Danilo José Camotti Oliveira

Resumo

No mundo digital atual, a segurança cibernética tornou-se uma grande preocupação, tendo em vista a crescente exposição a ameaças virtuais enfrentadas por indivíduos e organizações. Com o avanço da tecnologia e a sociedade cada vez mais imersa na vida digital, é fundamental fornecer orientações práticas para fortalecer a defesa contra possíveis ataques cibernéticos. Diante disso, o presente trabalho tem como objetivo analisar diferentes casos de ataques cibernéticos, investigar suas características e impactos gerados para os indivíduos e/ou organizações, propondo medidas preventivas eficazes para proteger dados e sistemas contra ameaças virtuais. A metodologia adotada consiste em uma abordagem qualitativa, incluindo uma revisão da literatura existente sobre segurança cibernética e uma análise de exemplos recentes e históricos de ataques virtuais. No decorrer da análise, são identificados padrões nos métodos utilizados pelos cibercriminosos, permitindo a proposição de estratégias para fortalecer a segurança cibernética. Os resultados destacam a importância da conscientização contínua sobre segurança digital e a divulgação adequada de informações sensíveis. Em conclusão, este estudo enfatiza a necessidade de uma abordagem proativa na gestão da segurança cibernética, reconhecendo-a como uma preocupação essencial no cenário atual. Assim, implementar as estratégias recomendadas são passos fundamentais para fortalecer a defesa contra ameaças virtuais e garantir a integridade dos dados e sistemas em um ambiente digital. Por fim, é essencial reconhecer que a segurança cibernética é uma responsabilidade compartilhada, envolvendo não apenas as empresas e os órgãos governamentais, mas também os indivíduos, que devem adotar práticas de segurança básicas.

Palavras-chave: Segurança Cibernética, Integridade Virtual, Engenharia Social, Prevenção de Ataques, Conscientização.

Alunos do curso de Tecnologia em Análise e Desenvolvimento de Sistemas, da Faculdade de Tecnologia de Presidente Prudente. E-mails: marialuiza01@fatec.sp.gov.br e pedro.melo9@fatec.sp.gov.br
Professor orientador Especialização em Redes de Computadores, da Faculdade de Tecnologia de Presidente Prudente. E-mail: danilo.oliveira103@fatec.sp.gov

Abstract

In today's digital world, cybersecurity has become a significant concern due to the growing exposure to virtual threats faced by individuals and organizations. As technology advances and society becomes increasingly immersed in digital life, providing practical guidance to strengthen defenses against potential cyberattacks is crucial. This study aims to analyze various cases of cyberattacks, investigating their characteristics and impacts on individuals and organizations, while proposing effective preventive measures to protect data and systems. The methodology includes a qualitative approach, reviewing existing cybersecurity literature and analyzing both recent and historical examples of virtual attacks. The analysis identifies patterns in cybercriminals' methods, enabling the proposal of strategies to enhance cybersecurity. The findings emphasize the importance of continuous awareness of digital security and the careful handling of sensitive information. Ultimately, this study highlights the need for a proactive approach to cybersecurity management, recognizing it as an essential concern in the current landscape. Implementing the recommended strategies is fundamental to strengthening defenses against virtual threats and ensuring data integrity in a digital environment. Furthermore, it is essential to acknowledge cybersecurity as a shared responsibility, involving not only companies and governmental entities but also individuals, who should adopt basic security practices.

Keywords: *Cybersecurity, Virtual Integrity, Social Engineering, Attack Prevention, Awareness.*

1. INTRODUÇÃO

A finalidade da segurança da informação é assegurar a integridade dos dados, a segurança dos sistemas de informação e das redes que conectam os computadores (Machado, 2014). Para tal fim, se faz necessárias diversas técnicas e medidas protetivas. Na atualidade, ambientes corporativos atestam a importância da segurança da informação, a qual é necessária para manter a confidencialidade de dados, a competitividade, eficiência e a qualidade das empresas. É importante ressaltar que, nenhum software e tecnologia, garante a segurança total de um indivíduo ou empresa (Mitnick, 2001).

Este artigo tem o objetivo de levantar e analisar os principais padrões de “medidas protetivas” que os indivíduos utilizam no ato de criação de novas contas e durante o uso do ambiente digital. A necessidade dessa pesquisa respalda no fato de que muitos usuários tendem a tomar decisões previsíveis e inseguras, como criação de senhas fracas, clique em links maliciosos, acesso a sites questionáveis, abertura de e-mails suspeitos, o que torna seu equipamento e suas contas vulneráveis a ataques cibernéticos.

Identificando esses padrões de senhas fracas e uso inseguro do ambiente digital, será possível conscientizar os usuários sobre a importância dos cuidados ao navegar na internet, visto que, a vida dos usuários, assim como suas intimidades, estão presentes no mundo virtual.

Assim, em mão de pessoas má intencionadas, essas informações sensíveis podem se tornar ferramenta para crimes ainda maiores.

É esperado que os resultados dessa pesquisa possam, de alguma forma, colaborar com a mitigação dos riscos associados a ataques cibernéticos e auxiliar os usuários a adotarem boas práticas no uso da internet, protegendo sua privacidade, informações e consequentemente sua integridade virtual.

2. METODOLOGIA

O presente estudo caracteriza-se como qualitativo, descritivo e exploratório. Inicialmente, realizou-se uma revisão da literatura sobre segurança cibernética, consultando artigos científicos indexados no *Google Scholar* e relatórios técnicos de instituições renomadas no setor, como Microsoft, Agência Brasileira de Inteligência (ABIN), IBM, Google, Kaspersky, entre outras. Com base nesta revisão, foi elaborado como instrumento de pesquisa um questionário no *Google Forms*, composto por 11 questões. Destas, duas visam coletar dados sociodemográficos dos participantes, enquanto as demais exploram, de forma qualitativa, suas percepções e práticas relacionadas à segurança cibernética, como consta no Apêndice 1.

Os participantes desta pesquisa foram os alunos do 1º e 6º módulos do curso de Análise e Desenvolvimento de Sistemas da FATEC de Presidente Prudente. O objetivo foi entender se há uma diferença de percepção e preocupação com a segurança cibernética entre alunos mais experientes, que estão concluindo o curso, e os que estão ingressando na faculdade. Diante dos dados coletados, foi realizada a discussão com exemplos recentes e históricos de ataques virtuais, analisando quais são os padrões nos métodos utilizados pelos cibercriminosos, permitindo a proposição de estratégias para fortalecer a segurança cibernética. Cabe pontuar também que, tanto para a discussão sobre os ataques quanto para as possíveis estratégias de segurança, foi utilizado, em sua maior parte, o site Cert.br como base.

3. SEGURANÇA CIBERNÉTICA

Conforme a sociedade se torna mais dependente de tecnologias digitais, pessoas e organizações sofrem com exposições devido à vulnerabilidade de seus dados. Portanto, a segurança cibernética, consequentemente, torna-se fundamental para garantir a integridade, confidencialidade e disponibilidade das informações. Sendo que essas existem e são

transmitidas de diversas formas, podendo ocorrer por meio da fala, armazenada em dispositivos eletrônicos, impressa, entre outros. Independentemente da forma de armazenamento ou transmissão da informação, é necessário que essa seja protegida de forma adequada. Diante disso, o papel da segurança da informação é assegurar a proteção contra diversos tipos de ameaças existentes (Coelho et al., 2014).

Outrora, a Segurança da Informação era muito mais simples: dados que hoje ficam armazenados em grandes *data centers* eram registrados em papel, guardados em gavetas e protegidos, sobretudo, por restrições físicas ao ambiente. Com os avanços tecnológicos, como o desenvolvimento de computadores pessoais e dispositivos móveis, esse cenário mudou significativamente (Santos & Silva, 2021).

Tendo em vista que, nesta nova realidade, existem diversos ataques que ocorrem no meio digital, ultrapassando as barreiras físicas. Considera-se ataque cibernético qualquer tentativa maliciosa com o objetivo de acessar dados sem autorização. Por meio desse acesso, podem modificar, expor, roubar e/ou destruir informações presentes em um sistema, rede ou qualquer dispositivo digital. Assim, esses ataques podem ser capazes de causar danos, interromper as atividades ou até destruir empresas, impactando diretamente ou indiretamente seus usuários (IBM, 2024).

Diante deste novo contexto digital, a segurança cibernética desempenha papel essencial na proteção das informações. Entende-se como Segurança Cibernética:

> Ações voltadas para a segurança de operações, de forma a garantir que os sistemas de informação sejam capazes de resistir a eventos no espaço cibernético capazes de comprometer a disponibilidade, a integridade, a confidencialidade e a autenticidade dos dados armazenados, processados ou transmitidos e dos serviços que esses sistemas ofereçam ou tornem acessíveis. (BRASIL, 2019).

Sendo assim, é de responsabilidade da segurança cibernética assegurar que as tecnologias aplicadas, medidas ou práticas de segurança adotadas para a proteção digital diminuam e previnam as possíveis ameaças e seus impactos. Assim como, cooperar para o desenvolvimento de estratégias que visem a educação e conscientização dos usuários sobre o uso mais seguro dos recursos digitais.

3.1 Princípios Básicos de Segurança

Coelho et al. (2014) afirmam que, de acordo com o padrão ISO 7498-2, o qual aborda os aspectos de segurança no modelo *Open Systems Interconnection* (OSI), os serviços de segurança funcionam como medidas preventivas contra ameaças identificadas. Esses serviços, portanto, ajudam a aumentar a proteção em reposta a possíveis ataques, utilizando mecanismos de segurança que reforçam a integridade do sistema.

É importante entender que os ataques podem ser passivos e/ou ativos. O primeiro representa um ataque com objetivo de obter dados por meio de monitoramento de transmissões e/ou escutas e pode ser realizado em uma chamada telefônica, por exemplo. Já o segundo consiste em negar serviços, modificar dados e criar informações falsas. Esses ataques possuem características diferentes de ataques passivos, exigem um conhecimento técnico avançado e são mais complexos de tratar pelo fato de ser necessário uma defesa da comunicação e processamento constantemente (Coelho et al., 2014).

Contudo, como nenhum sistema é inviolável, caso o ataque seja detectado é necessário tomar medidas para tratá-lo de imediato. Destarte, os princípios básicos de segurança são indispensáveis tanto para a redução de danos quanto para a prevenção de ataques. Ademais, conforme os autores Coelho et al. (2014) os serviços de segurança também podem ser denominados como princípios básicos de segurança, que incluem:

- Confidencialidade**:** busca garantir que a informação seja acessível apenas para indivíduos autorizados, prevenindo o acesso indevido. Para proteger os dados contra os ataques passivos, são implementadas estratégias de segurança, como controle de acesso rigoroso e criptografia, assegurando que informações sensíveis permaneçam protegidas.
- Integridade: assegura que a informação não foi alterada ou removida indevidamente por pessoas não autorizadas. Assim, atuando na garantia contra os ataques ativos. A violação da integridade ocorre quando uma informação é acessada por um indivíduo não autorizado, que pode alterar seu conteúdo sem a devida aprovação ou controle do responsável pela informação, seja no âmbito corporativo ou privado.
- Disponibilidade: assegura que usuários autorizados tenham acesso a informações e a recursos quando necessários, protegendo-as de perdas ou degradações. Além disso, a perda da disponibilidade ocorre quando não é possível acessar informações necessárias quando solicitadas. Isso pode acontecer devido intervenções internas e/ou externas a

equipamentos, bem como por ações de indivíduos sem autorização, sejam suas ações má intencionadas ou não.

- Autenticidade: busca garantir a autenticidade de uma comunicação, assegurando que as partes envolvidas sejam quem elas alegam ser, possibilitando que tanto o remetente quanto o destinatário confirmem a identidade dos envolvidos no processo. Nesse cenário, entende-se remetente e destinatário como usuários, dispositivos e processos.
- Irretratabilidade (Não Repúdio): é o processo que assegura que nenhum dos envolvidos em dada comunicação possa negar que enviou ou recebeu determinada mensagem. Assim, serve como uma maneira de comprovar a origem de uma mensagem enviada e a do seu destinatário.
- Controle de Acesso: restringe o controle de acesso físico/lógico aos patrimônios de um indivíduo ou organização, por intermédio de processos de identificação, autorização e autenticação, protegendo os meios de acessos indevidos.
- Conformidade: busca aderir e promover o cumprimento de regulamentos e leis internas e/ou externas existentes em determinada organização, garantindo que as práticas e processos estejam respeitando as diretrizes presentes.

Diante disso, é necessário compreender os princípios fundamentais de segurança para construir um ambiente digital mais seguro, e desenvolver estratégias que promovam a conscientização dos usuários e criação de ferramentas que visam a proteção de dados. Dessa forma, contribuindo para a mitigação de ataques e ameaças.

3.2 Ameaças cibernéticas no cenário atual

De acordo com o ABIN (2023), ameaça são condições ou conjunto de influências externas que podem causar um evento indesejado, apresentando um potencial risco de danificar um sistema e/ou organizações. No contexto digital, a IBM (2024) aborda a ameaça cibernética como uma indicação de que uma pessoa ou grupo mal-intencionado está elaborando estratégias para obter acesso indevido a um sistema com o objetivo de executar um ataque cibernético.

Há diferentes formas de ameaças cibernéticas, podendo ser mais simples ou complexas. As ameaças simples podem ser por meio de e-mails enganosos oferecendo prêmios ou ofertas imperdíveis, normalmente utilizando-se da engenharia social, estratégia realizada para persuadir pessoas a realizarem ações por meio de manipulação e falsas informações, visando

obter dados sigilosos, como: senhas, contas bancárias, acessos restritos, entre outros. Já as ameaças mais complexas requerem conhecimento para elaborar códigos maliciosos capazes de burlar proteções presentes nos sistemas. Cabe ressaltar que o conhecimento dos colaboradores funciona como ferramenta essencial na prevenção de ataques cibercriminosos (IBM, 2024).

Quando uma ameaça é concretizada ou explorada, pode resultar em um incidente de segurança que envolve violação de dados. Esse tipo de ocorrência, caracterizado como um ataque cibernético, pode levar à danificação ou exclusão de informações. Neste contexto, o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br), representa um grupo de resposta a incidentes de segurança de responsabilidade nacional.

No portal oficial do site CERT.br, é possível analisar estatísticas de incidentes relatados por profissionais de tecnologia e usuários da internet, que, de forma voluntária, notificam o grupo. Os dados estatísticos presentes neste centro de estudo estão em produção desde 1999. Em um detalhamento de 2024, englobando os meses de janeiro a setembro, apontaram que os principais incidentes reportados foram: DoS, Fraude, Invasão, *Scan*, *Web*, e uma categoria denominada “Outros” que, segundo o portal, são incidentes que não se encaixam nas categorias descritas.

Figura 1 – Detalhamento das notificações recebidas

Totais mensais e anual classificados por categoria de incidente -- Janeiro a Outubro de 2024

Mês	Total	DoS (%)		Fraude (%)		Invasão (%)		Scan (%)		Web (%)		Outros (%)	
jan	40.540	74	0,18	2.455	6,06	154	0,38	37.357	92,15	391	0,96	109	0,27
fev	33.893	1.156	3,41	1.600	4,72	150	0,44	30.498	89,98	392	1,16	97	0,29
mar	39.950	943	2,36	1.763	4,41	370	0,93	36.306	90,88	470	1,18	98	0,25
abr	32.003	94	0,29	2.223	6,95	1.102	3,44	27.791	86,84	393	1,23	400	1,25
mai	29.843	91	0,30	2.404	8,06	114	0,38	26.385	88,41	588	1,97	261	0,87
jun	32.011	98	0,31	2.238	6,99	123	0,38	28.534	89,14	615	1,92	403	1,26
jul	40.808	4.563	11,18	2.327	5,70	165	0,40	32.995	80,85	551	1,35	207	0,51
ago	55.186	19.042	34,51	1.664	3,02	233	0,42	33.636	60,95	469	0,85	142	0,26
set	51.970	13.999	26,94	1.954	3,76	188	0,36	35.277	67,88	409	0,79	143	0,28
out	73.956	10.238	13,84	1.909	2,58	193	0,26	58.910	79,66	2.145	2,90	561	0,76
Total	430.160	50.298	11,69	20.537	4,77	2.792	0,65	347.689	80,83	6.423	1,49	2.421	0,56

Fonte: https://stats.cert.br/incidentes/

Analisando a figura, é possível observar que os incidentes mais relatados estão nas seguintes categorias, *Scan*, *DoS* e Fraude respectivamente. Segundo o CERT.br entende-se as categorias como:

- ***Scan***: envolve notificações relativas a varreduras em redes de computadores e de força bruta de senhas, tentativas falhas de encontrar e aproveitar vulnerabilidades em serviços de rede que estão presentes no meio digital e são acessíveis ao público.
- **DoS** (DoS -- *Denial of Service*): representam as notificações relacionadas a negação de serviço, nas quais os ataques são realizados por meio de um ou vários computadores com o objetivo de desabilitar um serviço, rede ou dispositivo.
- **Fraude**: indicam as notificações relacionadas a tentativa de fraude, ação realizada com má intenção, cujo objetivo é tirar proveito de terceiros, seja por questões financeiras ou não. No contexto dos dados apresentados Fraude representa duas sub-categorias de incidentes, sendo elas:
    - *Phishing*: notificações de sites fraudulentos, visando ganho financeiro ou outros serviços, como serviços de e-mail, acessos indevidos a ambientes corporativos e serviço de nuvem.
    - *Malware*: notificações de códigos nocivos, com o objetivo de prejudicar o usuário de alguma forma, como roubar dados sensíveis e informações de acesso.
- **Web**: Ataques que buscam comprometer páginas da *web* e atacar servidores que o hospedam.
- **Invasão**: Quando há sucesso em um ataque, o que resulta em interações não autorizadas com redes e computadores. O *ransomware*, por exemplo, é um *malware* que, quando executado em um dispositivo, criptografa os arquivos, sequestrando os dados do dispositivo infectado e solicita um valor, normalmente em criptomoedas para o resgate (IBM, 2024).

A partir do que foi apresentado, é possível notar que há muitos incidentes notificados, mesmo com as notificações sendo realizadas de forma voluntária. Além disso, podem acontecer de diferentes maneiras. Desse modo, além de compreender os princípios básicos de segurança, é essencial conhecer os possíveis incidentes e seus funcionamentos, buscando sempre se adaptar às mudanças no meio tecnológico.

3.3 Autenticação e controle de acesso

Os ataques cibernéticos estão em constante evolução, e a partir desse crescente, a autenticação segura torna-se imprescindível. Sua principal função é verificar a identidade do

usuário e possuir esse controle de acesso assegura que apenas indivíduos autorizados tenham acesso às informações, evitando acessos indevidos e possíveis ameaças.

3.3.1 Criptografia para autenticação segura

A criptografia é um pilar fundamental para a cibersegurança, visto que protege os dados e informações sensíveis contra alterações ou comprometimentos. Ela converte o texto simples em um formato codificado, utilizando algoritmos matemáticos criptográficos, tornando-os ilegíveis para partes não autorizadas. Quando as credenciais de autenticação são informadas durante o login, os dados relacionados são regularmente transmitidos por redes e, sem a criptografia, esses dados ficam vulneráveis e podem ser capturados por pessoas mal-intencionadas. Desse modo, a criptografia assegura que, mesmo com os dados expostos, eles não podem ser decifrados sem a chave de decodificação (Google, 2024).

A criptografia simétrica e assimétrica são os tipos mais comuns de algoritmos. Na criptografia simétrica, usa-se a mesma chave compartilhada para criptografar e descriptografar os dados. O lado negativo é que, em casos de invasão, pessoas não autorizadas podem descriptografar os dados e informações confidenciais. A criptografia assimétrica possui uma chave pública e uma chave privada, com duas chaves separadas para criptografar e descriptografar. Assim, o usuário é autenticado com segurança, eliminando a necessidade de compartilhar a chave privada (Google, 2024).

O *hashing* é um processo unidirecional que recebe mensagens de tamanhos variados como entrada e gera uma cadeia de bits de tamanho fixo como saída, chamada de *hash*. Essa forma de criptografia é essencial para proteger informações sensíveis, como senhas, evitando que sejam alvo de acessos não autorizados ou mal-intencionados. Os algoritmos de hash seguro (SHA - *Secure Hash Algorithms*) são um conjunto de funções de hash criptográficas padronizadas pelo NIST (*National Institute of Standards and Technology*) para garantir a segurança, ajustado conforme surgem novas vulnerabilidades e mudanças na segurança digital. Atualmente, o conjunto SHA conta com quatro principais versões: SHA-0, SHA-1, SHA-2 e SHA-3, sendo a SHA-3 a mais segura (Gonçalves, 2022).

3.3.2 Gerenciadores de Senhas

De acordo com Zelster (2015), o número de cadastros em contas cresce a cada dia, dada a quantidade de contas que cada pessoa possui, torna-se inviável criar senhas fortes e únicas e

memorizá-las para cada acesso. Assim, os gerenciadores de senhas surgem como uma solução eficiente, funcionando como um cofre digital para o armazenamento seguro das credenciais. Esses gerenciadores possuem a funcionalidade de criptografar os dados armazenados no cofre, que são protegidos por uma senha principal conhecida apenas pelo usuário. Essa senha deve ser forte, exclusiva e se possível, utilizar a verificação em duas etapas, pois basta digitá-la para desbloquear o cofre.

Bitwarden é um gerenciador de senhas de código aberto que se destaca como um excelente protetor digital. Ugli Kodirov (2023) afirma que, assim como outros gerenciadores, o *Bitwarden* prioriza a segurança, oferecendo criptografia de ponta a ponta, ou seja, somente o próprio usuário pode descriptografar suas informações. A chave mestra não é armazenada em seus servidores, e nem mesmo a equipe da empresa tem acesso às senhas ou dados confidenciais dos usuários. Além disso, o *Bitwarden* já passou por auditorias de segurança e testes de penetração.

Para adicionar uma camada extra de segurança, o *Bitwarden* também oferece suporte à autenticação em duas etapas (2FA). Assim, mesmo que alguém consiga descobrir a chave mestra, ainda precisará passar pela segunda etapa de verificação para obter acesso à conta, o que reduz a chance de acessos não autorizados.

3.3.3 Verificação de dois fatores (2FA)

A verificação de dois fatores (2FA) serve para gerenciar a identidade do usuário, sendo uma camada extra de segurança, garantindo que em caso de tentativa de invasão, o acesso seja dificultado, uma vez que requer duas formas de identificação para realizar o login. O método mais popular de autenticação de dois fatores (2FA) é através do SMS, no qual um código é enviado aos usuários (Microsoft, 2024).

De acordo com os padrões de segurança da Microsoft (2024), o uso da autenticação multifator pode bloquear mais de 99,9% dos ataques automatizados. Recentemente, em 2024, a FATEC adicionou uma camada extra de segurança, exigindo que os alunos ao fazer login no e-mail institucional, além de informar a senha, também realizem a verificação de identidade por meio de um código enviado para seus dispositivos móveis. Consequentemente, reduzindo as chances de ataques e adicionando uma barreira extra para proteção das contas dos alunos e funcionários.

Aplicativos como *Microsoft Authenticator, Google Authenticator e Authy* possuem

funcionalidades semelhantes, gerando códigos de autenticação temporários que podem ser inseridos em sites compatíveis, ou seja, que suportam a autenticação de dois fatores. Além disso, a biometria é outro método mais avançado, utilizando características únicas como impressão digital, reconhecimento facial ou íris dos olhos.

O *phishing* é um ataque cibernético usado para enganar as pessoas e roubar informações, como senhas. Em razão da crescente evolução de técnicas de *phishing*, as senhas são consideradas fatores de segurança fracos, principalmente para aqueles que usam as mesmas senhas para várias contas, tornando crucial adotar medidas adicionais, como autenticação 2FA para maximizar a segurança, dificultando a invasão de um segundo fator (IBM, 2024).

4. ESTUDO DOS RESULTADOS

Com o constante avanço tecnológico, indivíduos que não possuem o conhecimento necessário das práticas básicas da segurança digital, estão mais propensos a ataques. Segundo o Relatório de Ameaças da *Kaspersky* (2019), a falta de conhecimento em segurança digital é um dos principais motivos pelos quais os usuários comuns se tornam vítimas frequentes de ataques, exacerbando os riscos em um ambiente tecnológico em constante evolução.

> Por que as pessoas não checam um link enviado por e-mail, SMS ou WhatsApp antes de abri-lo? As mensagens fraudulentas são um dos golpes online mais populares na América Latina e esse devia ser um comportamento básico, assim como olhar para os dois lados da rua antes de atravessá-la. Se os internautas tivessem mais conhecimento acerca da segurança digital, muitos golpes que exploram a desatenção das pessoas não existiriam, pois não seriam rentáveis", afirma Tricarico (2021).

A presente pesquisa realizada pelo *Google Forms* objetiva analisar e comparar os cuidados que os alunos do 1º e 6º módulos, matriculados no curso de Análise e Desenvolvimento de Sistemas da FATEC de Presidente Prudente, têm diante de seu uso do ambiente digital. A amostragem resultou em 40 respostas, sendo elas, 19 do primeiro módulo e 21 do sexto módulo.

A primeira pergunta do formulário diz respeito ao uso de senhas iguais em diferentes sites. De acordo com os dados coletados, há uma pequena distinção entre as porcentagens dos dois grupos, sendo que 71,4% das respostas do 6° módulo indicaram que utilizam a mesma senha em vários sites, já no 1° a porcentagem foi de 78,9%.

Figura 1 – 1º Módulo

Figura 2 – 6º Módulo

Fonte: Elaboração própria a partir de dados coletados com o *Google Forms*.

Ambas as amostras demonstraram baixa preocupação neste quesito, apresentando um fator negativo. Tendo em vista que, segundo a Cartilha de autenticação do CERT.br, utilizar a mesma senha em diversos lugares é um grande risco, já que, um invasor, descobrindo a senha de uma conta, pode acessar outros lugares onde ela é utilizada.

Para amenizar esta problemática, existem ferramentas que podem ser utilizadas com o objetivo de consultar vazamentos de dados, exibindo quais informações foram vazadas dos usuários, como senhas, endereço de e-mail, localização entre outros. Como exemplo de ferramenta com esta função temos o *Have I Been Pwned*, site disponível no Brasil e gratuito, no qual pode ser conferido se algum dado já foi vazado (Biczók et al., 2020).

Outra questão do formulário que abordou sobre senha foi em relação a criação de senhas fortes. De acordo com os resultados, as porcentagens foram variadas entre os dois módulos, sendo que no 6° módulo 90,5% das pessoas responderam que se preocupam com a criação de senhas fortes, mas as vezes reutilizam suas senhas em algumas contas e 9,5% se preocupam, mas nem sempre se dedicam a criação de senhas fortes. Já o primeiro módulo, apresentou as porcentagens de 47,4% e 26,3%, respectivamente. O restante da porcentagem concentrou-se em respostas que o 6° módulo não aderiu, 21% dos alunos responderam que sempre criam senhas fortes e únicas para cada conta, no entanto, 5,3% responderam que raramente se preocupam com a complexidade de suas senhas.

Figura 3 – 1º Módulo

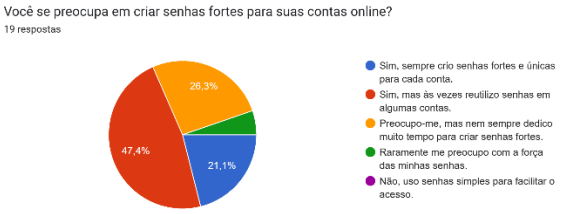


Figura 4 – 6º Módulo

Fonte: Elaboração própria a partir de dados coletados com o *Google Forms*.

Tanto a ausência de respostas do 6° módulo indicando a utilização de senhas únicas para cada conta, quanto a falta de preocupação do 1° módulo, que relataram raramente se preocupar com a criação de senhas fortes, demonstram que as contas desses usuários podem estar em risco, visto que as senhas são a primeira barreira de proteção ao acesso de suas contas e dispositivos. Consonante a cartilha (CERT.br), senhas fortes são caracterizadas por senhas longas, com caracteres de diferentes tipos, numéricos, alfabéticos maiúsculos, minúsculos, caracteres especiais, além de ser recomendado a não utilização de sequências do teclado ou informações relacionadas a vida pessoal do usuário e informações que podem ser encontradas em redes sociais ou em outros meios.

Ademais, conforme citado anteriormente, Zelster (2015) aborda sobre a dificuldade na criação e memorização de senhas fortes e únicas, neste caso é recomendado que ocorra a utilização de uma ferramenta auxiliar, como aplicativos gerenciadores de senhas que poderiam ajudar tanto no armazenamento de senhas quanto na criação, dessa forma aumentando a proteção das contas e segurança do usuário.

O uso da autenticação em duas etapas (2FA), como mencionado anteriormente, adiciona uma camada adicional de segurança (Microsoft, 2024). Além disso, a cartilha de autenticação da CERT.br, indica que essa medida ajuda a proteger as contas contra acessos não autorizados, tornando mais difícil para invasores obterem acesso mesmo que saibam a senha.

De acordo com os dados coletados na presente pesquisa, observamos que de maneira geral, os participantes estão atentos a essa questão. Cerca de 80% dos respondentes afirmaram utilizar a autenticação 2FA em todas as suas contas ou apenas nas que acessam com maior frequência. Os participantes do 1° módulo apresentaram uma porcentagem de 79% e o 6° módulo 80,9% no quesito de adoção dessa medida de segurança. Entretanto, 21,1% e 19%,

respectivamente do 1° e 6°, não fazem uso dessa tecnologia.

Figura 5 – 1º Módulo

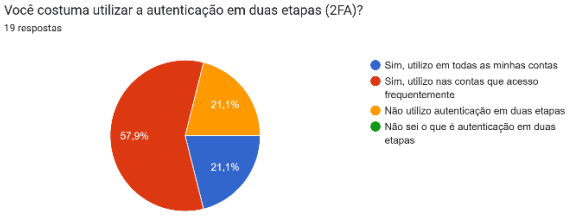
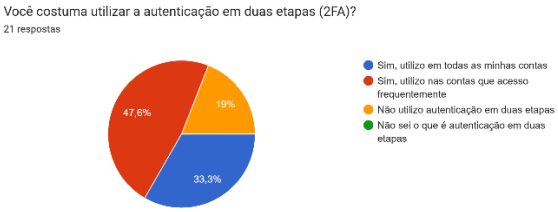


Figura 6 – 6º Módulo



Fonte: Elaboração própria a partir de dados coletados com o *Google Forms*.

Apesar do bom resultado, os participantes que não se preocupam estão vulneráveis a ataques, principalmente se não possuírem uma senha forte o suficiente. Como destaca a cartilha (CERT.br), a utilização de autenticação em duas etapas deve ser acompanhada de boas práticas de segurança, como a criação de senhas robustas e a preferência por métodos mais seguros, como chaves de segurança físicas ou geradores de códigos por aplicativos, em vez de SMS, o qual é recomendado como última opção.

A análise dos dados coletados revelou também a baixa preocupação com a realização de *backups* de dados pessoais no 1º módulo, no qual apenas 52,6% dos participantes realizam *backups* regularmente ou com pouca frequência, enquanto no 6º módulo essa preocupação aumenta significativamente para 80,9% dos respondentes.

Figura 7 – 1º Módulo

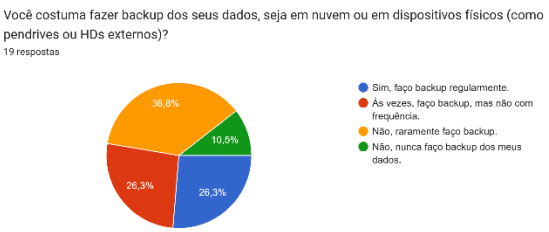


Figura 8 – 6º Módulo

Fonte: Elaboração própria a partir de dados coletados com o *Google Forms*.

Essa diferença discrepante demonstra uma possível crescente conscientização sobre a importância dos *backups*, refletindo a maturidade adquirida ao longo do curso. Um caso que exemplifica a importância dessa prática ocorreu em 18 de outubro de 2024, quando a SABESP sofreu um ataque cibernético envolvendo *ransomware*. Apesar dos criminosos terem

derrubado mais de dois mil servidores, a empresa conseguiu restaurar seus sistemas sem pagar o resgate, graças à existência de *backups* não violados pelos cibercriminosos (Lauterjung, 2024). Esse incidente reforça a necessidade de manter cópias de segurança atualizadas, destacando como essa medida pode ser determinante na proteção e recuperação eficaz de informações diante de ameaças digitais.

Outra questão que chamou a atenção foi em relação às infecções por *malware*. Embora 84,2% dos respondentes do 1º módulo afirmam nunca ter sido infectados, isso provavelmente se deve à falta de conhecimento sobre os riscos, já que infecções desse tipo são mais comuns do que muitos imaginam.

A educação digital é essencial para casos como esse, uma vez que muitos usuários não estão cientes das vulnerabilidades às quais podem estar expostos. Os 15,8% que afirmaram ter sido infectados não souberam identificar qual *malware* foi responsável, o que novamente pode ser atribuído à falta de conhecimento sobre os riscos e as ameaças digitais.

No 6º módulo, o número de infectados quase dobra, atingindo 33,3%, e alguns participantes foram capazes de identificar o tipo de *malware* responsável, com menções a *adware*, *spyware* e *ransomware*, *e*nquanto 66,7% responderam que nunca foram infectados. Isso se dá, possivelmente, ao aumento de conscientização sobre as ameaças, incluindo o conhecimento para diferenciar os tipos de *malware*. No entanto, é claro que a maioria dos respondentes precisam trabalhar essa questão da segurança cibernética, adotando medidas como o uso de antivírus, *backup* e boas práticas.

Figura 9 – 1º Módulo

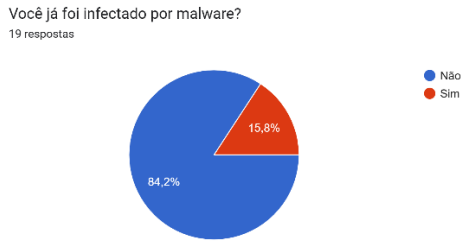
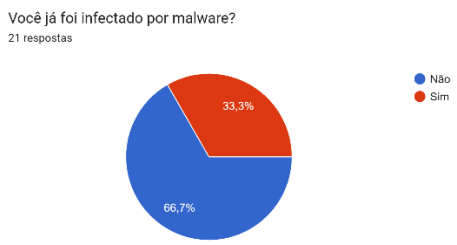


Figura 10 – 6º Módulo



Fonte: Elaboração própria a partir de dados coletados com o *Google Forms*.

Como citado anteriormente, a adoção de boas práticas é essencial para fortalecer a segurança virtual (CERT.br). Com base nos resultados obtidos na pergunta sobre manter programas atualizados, observou-se que somente 5,3% dos usuários do 1º módulo realizam

apenas as atualizações obrigatórias, enquanto no 6º módulo, esse número sobe para 19%.

Figura 11 – 1º Módulo

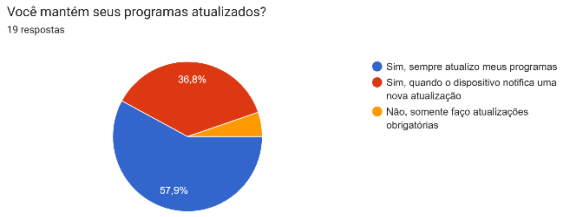
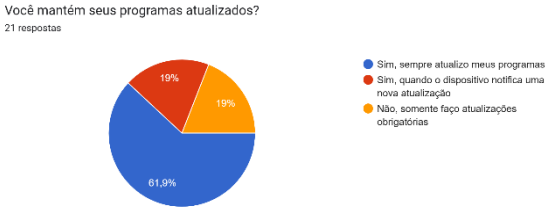


Figura 12 – 6º Módulo



Fonte: Elaboração própria a partir de dados coletados com o *Google Forms*.

Este resultado não era esperado, já que se antecipa que com o avanço do curso e o maior grau de maturidade, os participantes do 6º módulo adotem um maior interesse em relação a manter os programas atualizados.

Entretanto, é importante considerar que existem poucas matérias no curso que objetivam abordar sobre a segurança cibernética e boas práticas. Na presente grade curricular do curso de Análise e Desenvolvimento de Sistemas da FATEC de Presidente Prudente, no ano de 2024, existe somente a matéria “Segurança da Informação”, além disso possui apenas 2 aulas semanais, enquanto algumas das outras principais matérias do curso possuem 4 aulas semanais. Dessa forma, é possível notar que a quantidade de aulas não é suficiente para abarcar essa temática de forma mais eficaz, o que pode estar relacionado ao resultado obtido na pesquisa.

Além disso, a pesquisa também investigou o comportamento dos participantes em relação à verificação da procedência dos e-mails recebidos. Apenas 15,8% dos participantes do 1º módulo e 14,3% do 6º módulo afirmaram não se preocupar em verificar se os e-mails são legítimos, o que é um dado positivo, mas que ainda pode ser melhorado.

Figura 13 – 1º Módulo

Figura 14 – 6º Módulo

Fonte: Elaboração própria a partir de dados coletados com o *Google Forms*.

Segundo a *Kaspersky* (2018), um dos golpes mais comuns envolve notificações falsas de serviços de e-mail, em que cibercriminosos induzem os usuários a restaurar suas senhas ou a aumentar o espaço das caixas de e-mail supostamente lotadas, tornando a fraude mais convincente ao oferecer algo que parece legítimo e atrativo. Dessa maneira, esse contexto reforça a importância de educar os usuários sobre a importância de verificar a procedência dos e-mails recebidos, assim como orientar de que maneira esse procedimento pode ser realizado.

Diante disso, mesmo com um certo conhecimento sobre tecnologia, considerando que os respondentes estão em formação na área e enfrentam tentativas diárias de golpes, os resultados mostram que há a necessidade de promover uma educação digital mais efetiva e focada em práticas preventivas.

5. CONSIDERAÇÕES FINAIS

O presente artigo objetivou compreender a segurança digital, analisar as ameaças mais relevantes no cenário digital atual e investigar as práticas de proteção adotadas pelos alunos do módulo inicial e final do curso de Análise e Desenvolvimento de Sistemas. Diante da análise dos dados coletados foi observado um pequeno avanço nos cuidados relacionados à segurança digital no 6° módulo em relação a preocupação com a realização de *backups* e sobre o conhecimento relativo a *malwares*. Entretanto, no que diz respeito a proteção de senhas, atualizações de programas, autenticação em duas etapas e verificação da procedência de e-mails não foi notado grande discrepância entre os resultados dos dois módulos. O que sugere uma possível falta de ênfase nos temas de segurança dentro da grade curricular do curso e a necessidade de abordar de forma mais eficaz essa temática.

Vale ressaltar que qualquer violação dos princípios de segurança impacta tanto o usuário final quanto as empresas, tornando evidente que a conscientização sobre o uso seguro da internet é fundamental para a proteção contra atacantes. Empresas que não se atualizam ou não se adéquam aos avanços tecnológicos perdem competitividade e credibilidade no mercado. Da mesma forma, usuários que negligenciam práticas básicas de segurança se tornam alvos vulneráveis para cibercriminosos. Portanto, a conscientização e educação sobre segurança digital são essenciais para proteger indivíduos e organizações em um mundo cada vez mais digital.

REFERÊNCIAS

AFSHAR, V. *Cybersecurity: strategies to protect business data*. ZDNet, 2024. Disponível em: https://www.zdnet.com/article/cybercrime-can-be-the-biggest-threat-to-business-growth/. Acesso em: 10 nov. 2024.

BRASIL. Agência Brasileira de Inteligência. Ameaças, 2023. Disponível em: https://www.gov.br/abin/pt-br/institucional/acoes-e-programas/PNPC/ameacas. Acesso em: 5 out. 2024.

BRASIL. Portaria PR-GSI nº 93, de 5 de dezembro de 2019. Glossário de segurança da informação. Brasília: Tribunal Regional do Trabalho da 8ª Região, 2019. Disponível em: https://govti.trt8.jus.br/conformidade/media/base_juridica/PORTARIA%20PR-GSI%20N%C2%BA%2093-2019%20Gloss%C3%A1rio%20de%20Seguran%C3%A7a%20da%20Informa%C3%A7%C3%A3o.pdf. Acesso em: 16 nov. 2024.

BICZÓK, G.; HORVÁTH, M.; SZEBENI, S.; LÁM, I.; BUTTYÁN, L. The Cost of Having Been Pwned: A Security Service Provider's Perspective. Lecture notes in computer science, [*s. l.*], p. 154–167, 2020. Disponível em: https://www.researchgate.net/publication/347323566_The_Cost_of_Having_Been_Pwned_A_Security_Service_Provider's_Perspective. Acesso em: 18 nov. 2024.

CERT.br. Cert.br: estatísticas de incidentes. CERT.br, 2024. Disponível em: https://stats.cert.br/incidentes/. Acesso em: 15 nov. 2024.

COELHO, F. E. S. et al. Gestão da segurança da informação NBR 27001 e NBR 27002. 2016. Disponível em: https://www.kufunda.net/publicdocs/Gest%C3%A3o%20da%20seguran%C3%A7a%20da%20informa%C3%A7%C3%A3o%20NBR%2027001%20e%20NBR%2027002%20(Flavia%20Est%C3%A9lia%20Silva%20Coelho%20etc.).pdf. Acesso em: 21 out. 2024.

COUTINHO, MATEUS MICAEL et al. Estudo de caso: Principais pilares da segurança da informação nas organizações. Revista Gestão em Foco, 2017. Disponível em: https://portal.unisepe.com.br/unifia/wp-content/uploads/sites/10001/2018/06/052_estudo5.pdf. Acesso em: 20 out. 2024.

GOOGLE. O que é criptografia? Google Cloud, 2024. Disponível em: https://cloud.google.com/learn/what-is-encryption?hl=pt-BR. Acesso em: 9 nov. 2024.

GONÇALVES, L. Propostas de soluções para proteção de dados em ambientes corporativos. Trabalho de Conclusão de Curso (Bacharelado em Engenharia da Computação) – Universidade Federal de Pernambuco, Recife, 2022. Disponível em:

https://www.cin.ufpe.br/~tg/2022-1/tg_EC/TG_lgoq.pdf. Acesso em: 13 nov. 2024.

KASPERSKY. Desconhecimento é o maior desafio para a segurança no celular, alerta Kaspersky. 2021. Disponível em: https://www.kaspersky.com.br/about/press-releases/desconhecimento-e-o-maior-desafio-para-a-seguranca-no-celular-alerta-kaspersky. Acesso em: 18 nov. 2024.

KOSINKI, M. O que é phishing? IBM, 2024. Disponível em: https://www.ibm.com/br-pt/topics/phishing. Acesso em: 8 nov. 2024.

KOSINKI, M. O que é ransomware? IBM, 2024. Disponível em: https://www.ibm.com/br-pt/topics/ransomware. Acesso em: 29 out. 2024.

KOSINKI, M.; LINDEMULDER G. O que é segurança cibernética? IBM, 2024. Disponível em: https://www.ibm.com/br-pt/topics/cybersecurity. Acesso em: 3 nov. 2024.

LAUTERJUNG, B. Grupo hacker assume ataque ransomware contra a SABESP. [S. l.: s. n.], 2024. Disponível em: https://tiinside.com.br/01/11/2024/grupo-hacker-assume-ataque-ransomware-contra-a-sabesp/. Acesso em: 18 nov. 2024.

MICROSOFT. O que é autenticação de dois fatores (2FA)? Microsoft, 2024. Disponível em: https://www.microsoft.com/pt-br/security/business/security-101/what-is-two-factor-authentication-2fa. Acesso em: 27 out. 2024.

MICROSOFT. O que é segurança cibernética? Microsoft, 2024. Disponível em: https://www.microsoft.com/pt-br/security/business/security-101/what-is-cybersecurity. Acesso em: 5 nov. 2024.

ROCHA, Ronan. O uso da tecnologia no combate ao cibercrime. 2019. Disponível em: https://ri.unipac.br/repositorio/wp-content/uploads/2019/08/Ronan.pdf. Acesso em: 26 out. 2024.

STOKOE, E. A importância da segurança da informação na era digital. Revista Brasileira de Tecnologia e Inovação, 2018. Disponível em: https://www.fateccampinas.com.br/rbti/index.php/fatec/article/view/75/34. Acesso em: 7 nov. 2024.

ZELTSER, L. Ouch! Boletim de segurança. UFPel, 2015. Disponível em: https://wp.ufpel.edu.br/seginfo/files/2016/06/OUCH-201510_pt.pdf. Acesso em: 2 nov. 2024.

APÊNDICES

Apêndice 1

Qual termo você está cursando?
A) 1º
B) 6º

Qual a sua faixa etária?
A) Entre 17 e 25 anos
B) Entre 26 a 30 anos
C) Entre 31 a 40 anos
D) Acima de 40 anos

Você costuma utilizar a mesma senha em vários sites?
A) Sim
B) Não

Você se preocupa em criar senhas fortes para suas contas online?
A) Sim, sempre crio senhas fortes e únicas para cada conta.
B) Sim, mas às vezes reutilizo senhas em algumas contas.
C) Preocupo-me, mas nem sempre dedico muito tempo para criar senhas fortes.
D) Raramente me preocupo com a força das minhas senhas.
E) Não, uso senhas simples para facilitar o acesso.

Você costuma utilizar a autenticação em duas etapas (2FA)?
A) Sim, utilizo em todas as minhas contas
B) Sim, utilizo nas contas que acesso frequentemente
C) Não utilizo autenticação em duas etapas
E) Não sei o que é autenticação em duas etapas

Você costuma fazer backup dos seus dados, seja em nuvem ou em dispositivos físicos (como pendrives ou HDs externos)?
A) Sim, faço backup regularmente.
B) Às vezes, faço backup, mas não com frequência.
C) Não, raramente faço backup.
D) Não, nunca faço backup dos meus dados.

Você já foi infectado por malware?
A) Sim
B) Não

Se sim, qual foi o malware?

Você mantém seus programas atualizados?
A) Sim, sempre atualizo meus programas
B) Sim, quando o dispositivo notifica uma nova atualização

C) Não, somente faço atualizações obrigatórias

Você verifica a procedência (remetente) dos e-mails que recebe?
A) Sim
B) Não