PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS
ESCOLA POLITÉCNICA
GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

ESTUDO DE CASO SOBRE SEGURANÇA EM *E-COMMERCE*

MATHEUS DE OLIVEIRA MOTA

GOIÂNIA

2021

MATHEUS DE OLIVEIRA MOTA

ESTUDO DE CASO SOBRE SEGURANÇA EM *E-COMMERCE*

Trabalho de Conclusão de Curso apresentado à Escola Politécnica, da Pontifícia Universidade Católica de Goiás, como parte dos requisitos para a obtenção do título de Bacharel em Ciência da Computação.

Orientador:
Prof. Dr. José Luiz de Freitas Júnior
Banca examinadora:
Profª. Ma. Ludmilla Reis Pinheiro dos Santos
Prof. Me. Eugênio Júlio M. Cândido Carvalho

GOIÂNIA

2021

MATHEUS DE OLIVEIRA MOTA

ESTUDO DE CASO SOBRE SEGURANÇA EM *E-COMMERCE*

Trabalho de Conclusão de Curso aprovado em sua forma final pela Escola Politécnica, da Pontifícia Universidade Católica de Goiás, para obtenção do título de Bacharel em Ciência da Computação, em____/____/_____.

_____
Orientador: Prof. Dr. José Luiz de Freitas Júnior

_____
Profª. Ma. Ludmilla Reis Pinheiro dos Santos
Coordenadora de Trabalho de Conclusão de Curso

GOIÂNIA

2021

AGRADECIMENTOS

Primeiramente a Deus, pela minha vida, e por me ajudar a chegar aonde estou, ultrapassando todos os obstáculos encontrados ao longo do curso.

A minha namorada Letícia Félix, por toda a compreensão, paciência e apoio incondicional.

Aos meus familiares e amigos, que sempre me incentivaram e ajudaram durante a graduação.

Ao professor José Luiz de Freitas Júnior, orientador acadêmico, pelo seu incentivo, paciência, dedicação e orientações nas quais contribuíram para a realização deste trabalho.

Aos professores e à coordenação da Escola Politécnica, pela contribuição com o enriquecimento do meu conhecimento.

"Eu aprendi muito mais com os meus erros do que com meus acertos."

Thomas Edison

RESUMO

Com a crescente evolução da internet, houve um aumento no número de transações. Estas transações, necessitam de elementos que garantam a integridade e segurança dos dados envolvidos, a fim de que os usuários não tenham receio de realizá-las. O presente trabalho teve como objetivos: (a) estudos de boas práticas na área de segurança digital em que foram abordados diversos cuidados necessários para utilizar os serviços de internet, assim evitando ter informações expostas a terceiros; (b) estudo das ferramentas para o desenvolvimento de um site onde foi realizado o estudo de caso; (c) desenvolvimento de um site para captura de dados para o estudo de caso; e (d) o estudo de caso relacionado a compras *online* afim de demonstrar que o usuário pode ter suas informações coletadas sem seu conhecimento. Ressalta-se a importância de cuidados necessários para realização de compras *online* com maior segurança devido a existência do *Keylogger,* que é um tipo de malware, classificado na categoria de *spyware*.

Palavras-Chave: Compras *online*, segurança digital, *keyloggers*, *spyware*.

ABSTRACT

With the growing evolution of the internet, there was an increase in the number of transactions. These transactions need elements that guarantee the integrity and security of the data involved, so that users are not afraid to carry them out. The present work had as objectives: (a) studies of good practices in the area of digital security, in which several necessary precautions to use internet services were addressed, thus avoiding having information exposed to third parties; (b) study of tools for the development of a website where the case study was carried out; (c) development of a website to capture data for the case study; and (d) the case study related to online shopping in order to demonstrate that the user can have their information collected without their knowledge. It emphasizes the importance of care necessary to make online purchases with greater security due to the existence of the Keylogger, which is a type of malware, classified in the spyware category.

Keywords: *Online shopping, digital security, keyloggers, spyware*.

LISTA DE FIGURAS

Figura 1 - Vendas no comércio eletrônico brasileiro 14
Figura 2 - *Phishing* via *e-mail* exemplo 1 18
Figura 3 - *Phishing* via *e-mail* exemplo 2 parte 1 19
Figura 4 - *Phishing* via *e-mail* exemplo 2 parte 2 20
Figura 5 - Gráfico de vulnerabilidade de senhas 21
Figura 6 - Relatório das 30 senhas mais utilizadas no mundo 22
Figura 7 - Gerenciador de senhas LastPass 24
Figura 8 - Gerenciador de senhas Dashlane 24
Figura 9 - Ícone do cadeado verde 27
Figura 10 - *Software* Revealer Keylogger Free 34
Figura 11 - Dados registrados 35
Figura 12 - Tela de *login* 39
Figura 13 - Tela do produto 40
Figura 14 - Tela de compra 41
Figura 15 - Captura de dados 41

LISTA DE SIGLAS

API	*Application Programming Interface*
B2B	*Business-to-Business*
B2C	*Business-to-Consumer*
CEP	Código de Endereçamento Postal
COVID-19	*Corona Vírus Disease 2019*
CSS	*Cascading Style Sheets*
DNS	*Domain Name System*
HTML	*Hypertext Markup Language*
HTTPS	*Hyper Text Transfer Protocol Secure*
HYTIME	*Hypermedia/Time-based Document Structuring Language*
IDE	*Integrated Development Environment*
IP	*Internet Protocol*
PHP	*Hypertext Preprocessor*
SGML	*Standard Generalized Markup language*
SMS	*Short Message Service*
SQL	*Structured Query Language*
SSL	*Secure Socket Layer*
URL	*Uniform Resource Locator*
VoIP	*Voice Over Internet Protocol*
W3C	*World Wide Web Consortium*
WEB	*World Wide Web*
XHTML	*Extensible HyperText Markup Language*
XML	*Extensible Markup Language*

SUMÁRIO

1 INTRODUÇÃO 12
1.1 Objetivos 12
1.2 Justificativa 12
1.3 Metodologia 13
1.4 Estrutura do trabalho 13
2 REFERENCIAL TEÓRICO 14
2.1 Crescimento do *e-commerce* 14
2.2 *Phishing* 15
2.2.1 De onde vem o phishing? 16
2.2.2 Tipos de phishing 16
2.2.3 Como reconhecer phishing? 18
2.3 Importância das senhas 20
2.3.1 Vulnerabilidade das senhas 21
2.3.2 Gerenciadores de senhas 23
2.3.3 Métodos que ajudam manter as senhas mais seguras 25
2.4 Seguraça *web* 26
2.4.1 Segurança em lojas virtuais 28
2.5 Vulnerabilidades em *wi-fi* públicos 30
2.6 *Keyloggers* 32
3 IMPLEMENTAÇÃO E RESULTADOS 34
3.1 Captura de dados utilizando *keylogger* 34
3.2 Desenvolvimento do site para realizar estudo de caso 36
3.2.1 HTML 36
3.2.2 CSS 37
3.2.3 JavaScript 37
3.2.4 Visual Studio Code 38
3.2.5 Implementação 38
3.3 Captura de dados utilizando o site desenvolvido 41
4 CONSIDERAÇÕES FINAIS 43
4.1 Considerações finais 43
4.2 Dificuldades encontradas 43
4.3 Trabalhos futuros 44
REFERÊNCIAS BIBLIOGRÁFICAS 45

APÊNDICE A – CÓDIGO HTML DA PÁGINA INICIAL.....50
APÊNDICE B – CÓDIGO CSS DA PÁGINA INICIAL.....51
APÊNDICE C – CÓDIGO JAVASCRIPT DA PÁGINA INICIAL.....52
APÊNDICE D – CÓDIGO HTML DA PÁGINA DO CARRINHO.....54
APÊNDICE E – CÓDIGO CSS DA PÁGINA DO CARRINHO.....57
APÊNDICE F – CÓDIGO JAVASCRIPT DA PÁGINA DO CARRINHO.....59
APÊNDICE G – CÓDIGO HTML DA PÁGINA DE PAGAMENTO.....62
APÊNDICE H – CÓDIGO CSS DA PÁGINA DE PAGAMENTO.....66
APÊNDICE I – CÓDIGO JAVASCRIPT DA PÁGINA DE PAGAMENTO.....67
APÊNDICE J – TERMO DE AUTORIZAÇÃO DE PUBLICAÇÃO DE PRODUÇÃO ACADÊMICA.....69

1 INTRODUÇÃO

Com o crescimento e a popularização de computadores e celulares ficou cada vez mais fácil efetuar compras em lojas de *e-commerce*, porém, também houve um aumento nos crimes cibernéticos relacionados a este tipo de comércio, onde pessoas mal-intencionadas aproveitam oportunidades para tirar proveito de outras pessoas na internet.

Sendo assim, percebeu-se a importância de mostrar como isto ocorre, além de práticas para evitar que criminosos obtenham vantagem sobre a vítima.

1.1 Objetivos

Este trabalho teve os seguintes objetivos:

- Estudos de boas práticas na área de segurança digital em que foram abordados diversos cuidados necessários para utilizar os serviços de internet, assim evitando ter suas informações expostas a terceiros;
- Estudo das ferramentas para o desenvolvimento de um site onde foi realizado o estudo de caso;
- Desenvolvimento do site para captura de dados do estudo de caso;
- Estudo de caso relacionado a compras *online* afim de demonstrar que o usuário pode ter suas informações coletadas sem seu conhecimento.

1.2 Justificativa

Este tema foi escolhido devido ao aumento das compras *online*, principalmente após a restrição de circulação de pessoas nas cidades brasileiras devido a contenção pelo *Corona Vírus Disease 2019 (*COVID-19). Observou-se no ano de 2020 um aumento significativo de 70% em faturamento em relação a pedidos e compras *online* realizados no Brasil (E-COMMERCE BRASIL, 2020).

Devido ao aumento de compras *online*, consequentemente aumentou o número de golpes virtuais, invasão por hackers, vazamento de dados pessoais, clonagem de cartões, vírus etc. Sendo assim, achou-se importante realizar o trabalho abordando diversas recomendações e orientações a fim de ajudar aos usuários a navegarem na internet de maneira mais segura para a realização de compras *online*.

1.3 Metodologia

No decorrer do trabalho, utilizou-se como materiais para a realização do estudo, um computador, navegadores e sites relacionados a compras *online*, utilizou-se como base de dados para revisão de literatura, revistas, artigos e páginas da *web* nos quais foram fundamentais para o estudo.

Na primeira etapa do estudo de caso foi utilizado o *software* Revealer Keylogger Free (LOGIXOFT, 2021). Este *software* tem como objetivo realizar a captura de textos sem deixar que o usuário perceba este tipo de ação.

Na segunda etapa, para que fosse possível realizar a implementação do site foram utilizadas as linguagens *Hypertext Markup Language* (HTML), *Cascading Style Sheets* (CSS) e JavaScript. A *Integrated Development Environment* (IDE) utilizada durante todo o desenvolvimento foi o Visual Studio Code. Para a hospedagem do site foram utilizados os serviços da Netlify. Para visualizar as páginas do site será utilizado um navegador *web*.

A escolha da linguagem provém da facilidade que ela disponibiliza no desenvolvimento de uma página *web*.

1.4 Estrutura do trabalho

Este trabalho está dividido em 4 capítulos. Neste primeiro capítulo foram apresentadas as motivações pelas quais levaram ao estudo sobre a segurança digital em compras *online*.

No segundo capítulo é apresentado toda pesquisa bibliográfica deste trabalho onde é abordado o crescimento do *e-commerce*, *phishing*, importância das senhas, segurança *web*, vulnerabilidade em *wi-fi* públicos e *keyloggers*.

No terceiro capítulo é descrito os resultados obtidos dos experimentos realizados com captura de dados.

Por fim, no quarto capítulo é apresentado as considerações finais, incluindo as dificuldades encontradas e sugestões de trabalhos futuros.

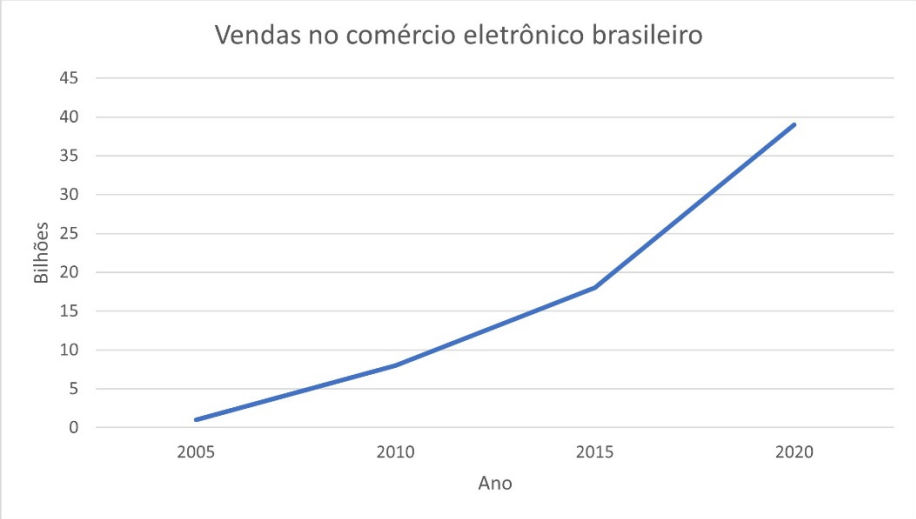
2 REFERENCIAL TEÓRICO

Este capítulo aborda o crescimento do *e-commerce* brasileiro, maneiras de detecção e bloqueio de golpes de *phishing*, sugestões para manter os dados protegidos contra invasores, além de mostrar a importância das senhas, segurança *web* e suas vulnerabilidades.

2.1 Crescimento do *e-commerce*

Por volta de 2000, com o advento da Internet, o *e-commerce* no Brasil deu seus primeiros passos silenciosos e hesitantes. Pesquisas da Ebit|Nielsen mostram, Figura 1 que as vendas por meio desse canal no primeiro semestre de 2005 foram de R$ 1 bilhão. Esse número subiu para R$ 8 bilhões em 2010, R$ 18 bilhões em 2015 e só atingiu R$ 39 bilhões no primeiro semestre de 2020, um aumento de 47% em relação a 2019 (GARGIONI, 2020).

Figura 1 – Vendas no comércio eletrônico brasileiro



Fonte: Elaborado pelo autor, com base em GARGIONI, 2020

O mais surpreendente é que no período abril a junho de 2020, quando a maioria das cidades brasileiras adotou medidas restritivas para conter a pandemia de COVID-19, as incertezas dominaram o mundo. E, com a atividade econômica em forte declínio, o *e-commerce* cresceu 70% em número de pedidos em relação ao mesmo período de 2019 (GARGIONI, 2020).

> De acordo com o Ebit|Nielsen, mais de 7 milhões de brasileiros realizaram agora sua primeira compra *online*, fazendo o Brasil ultrapassar a marca de 40 milhões de clientes ativos. A escalada de crescimento geométrico catapultado pela pandemia deixa clara e transparente a consolidação das mudanças extraordinariamente profundas no comércio de bens e serviços. Como resultado, no dia dos pais as vendas no *e-commerce* cresceram 127% com mais de 6 milhões de pedidos. Outros estudos realizados por entidades e consultorias especializadas apontam que fecharemos o ano de 2020 com vendas de R$ 120 bilhões — ou seja, 50% acima de 2019 —, enquanto as projeções indicam uma cifra anual de R$ 200 bilhões em 2024 (GARGIONI, 2020).

É importante mencionar e compreender que este não é um movimento novo, mas a pandemia apenas acelerou essa tendência e firmou a grande virada nas relações de negócios para sempre. Mesmo os consumidores que não desejam mudar e que foram forçados a aderir ao modelo devido à pandemia reconheceram sua praticidade e conveniência e o usaram com mais frequência. A comodidade de receber um produto com as características selecionadas, dentro do prazo em casa, sem o incômodo de custos, riscos e tempo de deslocamento, são elementos fundamentais para continuar utilizando cada vez mais o comércio eletrônico (GARGIONI, 2020).

2.2 *Phishing*

Phishing é uma técnica de crime cibernético que utiliza de fraudes, truques ou engano para manipular as pessoas e obter informações confidenciais (BELCIC, 2021).

Em 2004 houve o primeiro caso de *phishing* conhecido e registrado judicialmente. O mesmo ocorreu através da criação de um site falso o qual passou a obter informações confidenciais dos usuários que o acessavam. O site foi criado por um adolescente da Califórnia (GONÇALVES, 2021). Em 2013, a empresa Target sofreu um ataque de hackers, em que eles conseguiram acessar os leitores de cartões de ponto de venda da empresa e coletaram 11 GB de informações sobre cartões de crédito e débito.

Já em 2018, durante a preparação para a Copa do Mundo (FIFA 2018) em Moscou, surgiram vários *phishing* de ingressos gratuitos, ofertas de hotéis de última hora e produtos das equipes (BELCIC, 2021).

2.2.1 De onde vem o phishing?

Os crimes de *phishing* podem chegar até ao usuário por *e-mails*, *Short Message Service* (SMS), ligações, sites falsos e *pop-ups* falsos colocados em sites inseguros, todos com uma abordagem atraente (GONÇALVES, 2021).

Os conteúdos podem ser muito variados, desde bancos, governo, instituições financeiras, como o *PayPal* ou mesmo os correios, exigindo sempre uma ação ou informação. Por exemplo, pode ser solicitado que abra um determinado *link* ou arquivo, faça ligação ou instale/atualize um *software* específico (GONÇALVES, 2021).

Os criminosos usam todos os meios para atacar os usuários e obter acesso a informações confidenciais das quais eles possam tirar proveito (GONÇALVES, 2021).

2.2.2 Tipos de phishing

Existem diferentes formas de ataques de *phishing*, sendo os principais apresentados a seguir:

- *Scam*: Os golpes de *phishing scam* são tentativas de criminosos para induzi-lo a revelar informações pessoais, como números de contas bancárias, senhas e números de cartão de crédito, ao abrir *links* ou arquivos contaminados. Essas informações podem ser usadas para acessar sua conta indevidamente, roubar dinheiro e realizar transações. O contato pode ser feito através de telefone, *e-mail*, SMS ou redes sociais (GONÇALVES, 2021);
- *Blind Phishing*: O mais comum de todos, desencadeado por *e-mails* em massa e sem muitas estratégias, que se baseiam unicamente na “sorte” de que alguns usuários caírem na armadilha (GONÇALVES, 2021);
- *Spear phishing*: Quando o ataque é contra um grupo específico. Pode ser dirigido contra funcionários do governo, clientes de uma empresa específica ou até mesmo uma pessoa específica. O *spear phishing* visa acessar este banco de dados específico para obter informações confidenciais ou arquivos sigilosos (GONÇALVES, 2021);

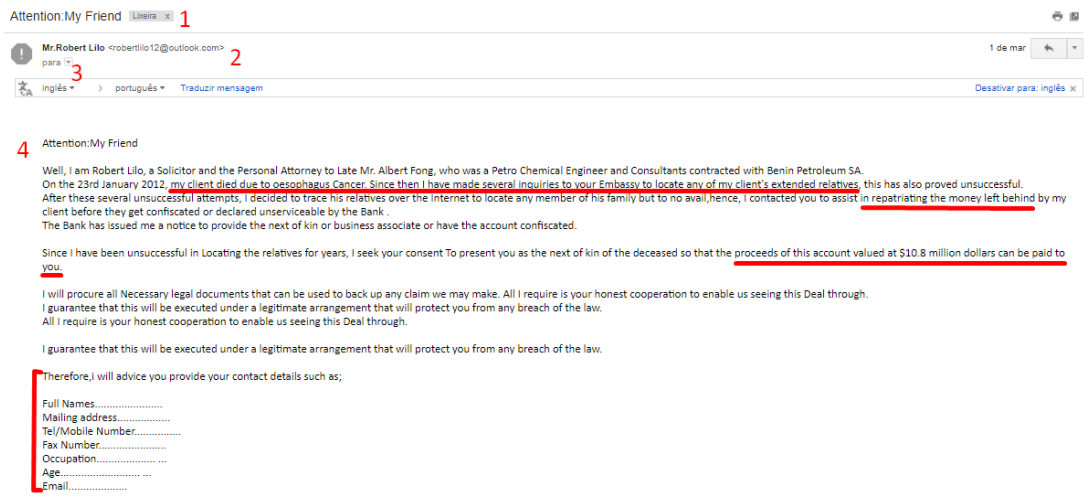
- *Clone phishing*: Este golpe clona um site original para atrair os usuários. Geralmente, ao acessar o site falso, a pessoa precisa inserir as informações cadastrais em um formulário malicioso que transmitirá as informações do usuário para os criminosos. O usuário então é direcionado para a página original sem perceber que foi uma vítima (GONÇALVES, 2021);
- *Whaling*: O termo vem da palavra *whale* (baleia, em inglês) e que significa caça à baleia. Isso significa que este crime está relacionado ao "tamanho do peixe a ser capturado". *Whaling* é dirigido a executivos de alto nível ou personalidades de relevância, como o presidente de uma empresa, e faz isso em nome da empresa para qual trabalha. Estes ataques vêm mascarados como intimações judiciais ou notificações empresariais internas (GONÇALVES, 2021);
- *Vishing*: a letra "p" foi substituída pela "v" porque o *vishing* usa mecanismos de voz para aplicar golpes. Podem vir acompanhados por mensagens de texto indicando que seu cartão foi bloqueado e você precisa ligar para um número específico para solicitar o desbloqueio, mas também pode ser uma ligação direta para sua casa ou seu celular. Os criminosos usam o *Voice Over Internet Protocol* (VoIP) porque é fácil ocultar a identidade de quem está ligando (GONÇALVES, 2021);
- *Pharming*: Ocorre quando o *Domain Name System* (DNS) é comprometido e atinge os usuários em uma larga escala. Sempre que o usuário procura por um site na internet, o DNS resolve o nome do domínio para o número de *Internet Protocol* (IP) do servidor quando a *Uniform Resource Locator* (URL) é inserida, por exemplo, www.google.com.br. Mas se o DNS estiver comprometido, a URL digitada poderá levar o usuário para uma página falsa criada para o ataque (GONÇALVES, 2021);
- *Smishing*: Termo para *phishing* realizado através de SMS. São mensagens que tendem a constranger o usuário como dívidas ou que levam a tomar decisões imediatas por meio de emoções, como sorteio, prêmios ou uma grande quantia a ser recebida (GONÇALVES, 2021).

2.2.3 Como reconhecer phishing?

Para a segurança dos usuários é importante verificar se o contato que o usuário está recebendo é, na verdade, *phishing*. Há algumas questões que podem ser avaliadas antes de simplesmente fornecer suas informações a criminosos que se passarão por heróis, sem cair em uma armadilha (GONÇALVES, 2021). Os *phishing* podem estar presentes em:

- Ofertas Lucrativas; que atraem os usuários a clicarem em *links* maliciosos objetivando roubas as informações do usuário (GONÇALVES, 2021);
- Loteria Premiada; com oferta de viagens, *smartphones* e carros de forma gratuita e com muita facilidade de acesso (GONÇALVES, 2021);
- Senso de Urgência; solicitando aos usuários uma ação rápida, com ofertas de oportunidades exclusivas ao usuário (GONÇALVES, 2021);
- Recebimento de Ameaças virtuais, tais como: “Sua conta foi bloqueada, clique para verificar”. Recebimento de *e-mail* ou mensagens com *links* externos, além disso também atual com o envio de arquivos maliciosos e remetente desconhecido (GONÇALVES, 2021). A Figura 2 apresenta um exemplo de *phishing*.

Figura 2 – *Phishing* via *e-mail* exemplo 1



Fonte: GONÇALVES, 2021

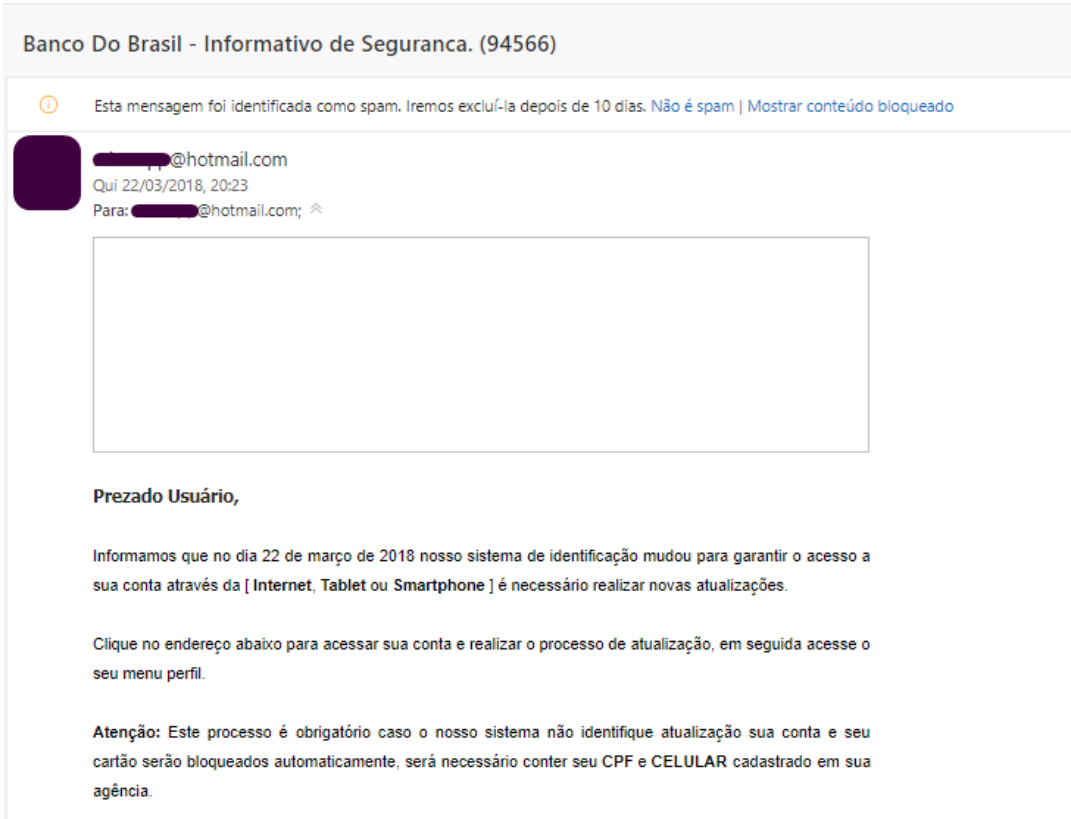
Este *e-mail* foi enviado para a caixa de entrada de um usuário brasileiro. Se analisarmos os pontos discutidos acima, podemos identificar características como:

- Título atraente;

- *E-mail* de remetente suspeito, estrangeiro e desconhecido;
- Não identifica o destinatário, sugerindo que foi enviado para uma lista;
- Ao longo do texto, várias passagens envolvem o leitor. Em suma, a história contada é sobre um suposto advogado que morreu em nome de um engenheiro químico, deixando um legado de US$ 10,8 milhões. E solicita informações pessoais para que o dono da conta de *e-mail* seja contatado para que receba a herança.

O próximo exemplo apresentado na Figura 3, os criminosos estão se passando por um banco e já no cabeçalho do *e-mail* é possível identificar indícios de fraude. O remetente e o destinatário foram mascarados e indicam que o proprietário da conta enviou e recebeu o *e-mail* ao mesmo tempo. O discurso adotado diz respeito às alterações no *software* e à urgência da necessidade de atualização, indicando um *link* para o internauta clicar e "atualizar". (GONÇALVES, 2021).

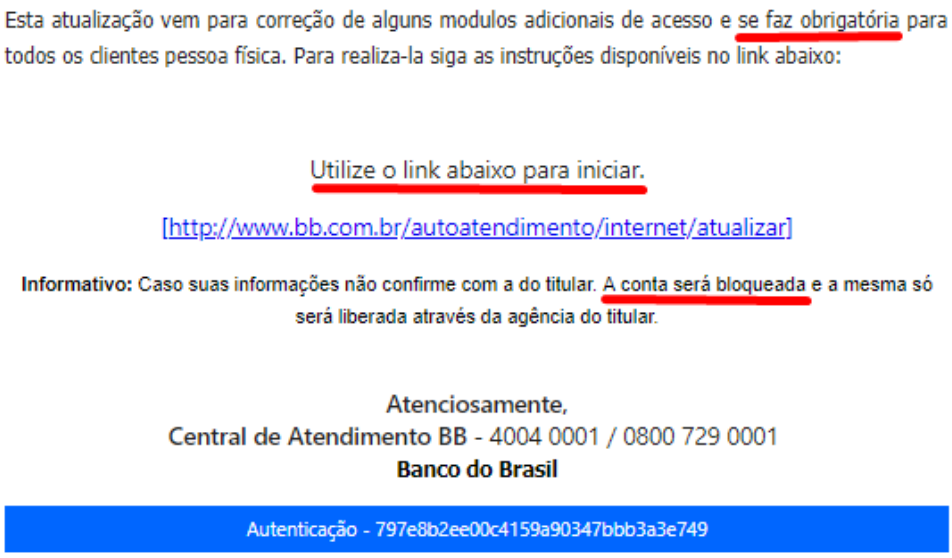
Figura 3 – *Phishing* via *e-mail* exemplo 2 parte 1



Fonte: GONÇALVES, 2021

No restante do mesmo *e-mail*, Figura 4, podemos identificar os argumentos obrigatórios, *links* e ameaças caso o cliente não "atualize o *software*" o mesmo terá a conta bloqueada (GONÇALVES, 2021).

Figura 4 – *Phishing* via *e-mail* exemplo 2 parte 2



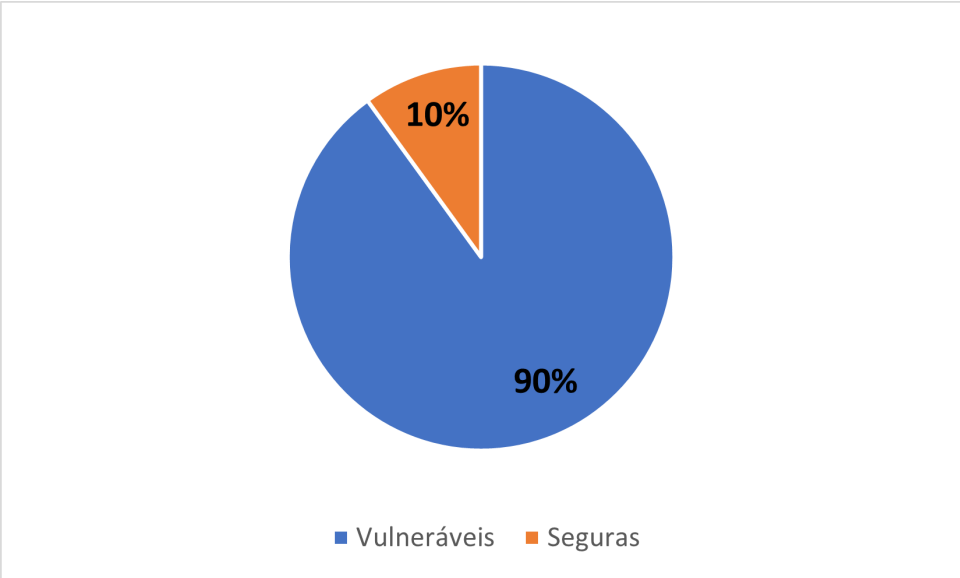
Fonte: GONÇALVES, 2021

2.3 Importância das senhas

As senhas são um conjunto de caracteres (letras, números ou símbolos) nas quais são utilizadas para fornecer um acesso a algo restrito (CONCEITO, 2020). A senha é o principal recurso para comprovar a autenticidade de um usuário e protegê-lo do acesso indevido em sistemas de bancos e outros sistemas (redes sociais, *e-mail*). É viável não utilizar a mesma senha em diversas contas ou verificar se cada senha que está sendo utilizada seja diferente de suas senhas anteriores ou diferente de outras senhas comuns existentes, assim irá aumentar sua segurança contra ataques de hackers (FRITZEN, 2020).

Aproximadamente 90% das senhas são consideradas vulneráveis e podem ser descobertas com facilidade, conforme mostra a Figura 5. Caso ocorra uma violação de informações através de um ataque *hacker*, ele terá acesso a todos os perfis e contas da vítima. Devido a isso, é importante que o usuário utilize senhas fortes e seguras, as quais não serão descobertas com facilidade (FRITZEN, 2020).

Figura 5 – Gráfico de vulnerabilidade de senhas



Fonte: Elaborado pelo autor, com base em FRITZEN, 2020

2.3.1 Vulnerabilidade das senhas

A Figura 6 resume as descobertas da equipe de pesquisa do SafetyDetectives, na qual reuniu um conjunto com mais de 18 milhões de senhas para descobrir as 30 mais utilizadas, mais previsíveis e, por fim, as senhas mais hackeadas do mundo (MARINO, 2020).

Figura 6 – Relatório das 30 senhas mais utilizadas no mundo

Fonte: MARINO, 2020

Para a criação de senhas fortes é viável a utilização de algumas estratégias como: não utilizar informações pessoais (nome, data de nascimento), sequência de letras ou números (exemplo; 12345 ou abc123 ou *password*), ou informações óbvias como a palavra “senha” (EMPEY, 2018). Evite uso de nome de familiares, abreviações ou erros ortográficos comuns, palavras escritas ao contrário, não use caminhos de teclado memorizáveis (exempolo: qwerty) (EMPEY, 2018; FRITZEN, 2020).

Uma senha forte é composta por no mínimo 8 caracteres, a qual é composta por caracteres alfanuméricos, letras maiúsculas e minúsculas, números e símbolos. (FRITZEN, 2020). Para a criação de uma senha segura é ideal utilizar palavras incomuns, adicionar caracteres aleatórios no meio das palavras ou entre elas, usar as primeiras duas letras iniciais de cada palavra (exemplo: “Old Duke é meu pub favorito no sul de Londres”, senha: “OlDuemepufanosudeLo”) (EMPEY, 2018). Quanto maior for a variedade de caracteres mais forte a senha se tornará (FRITZEN, 2020).

As senhas podem ser consideradas portas de entrada para o mundo digital, pois com elas é possível acessar contas de bancos, *e-mails*, aplicativos nos *smartphones*, redes corporativas e sistemas de gestão. Senhas *podem* ser usadas para requerem acesso a dados e informações (UNIMAKE SOFTWARE, 2018).

Atualmente o acesso biométrico vem ganhando espaço no meio digital, porém o uso de senhas ainda é o principal passaporte de segurança dos usuários digitais (UNIMAKE SOFTWARE, 2018).

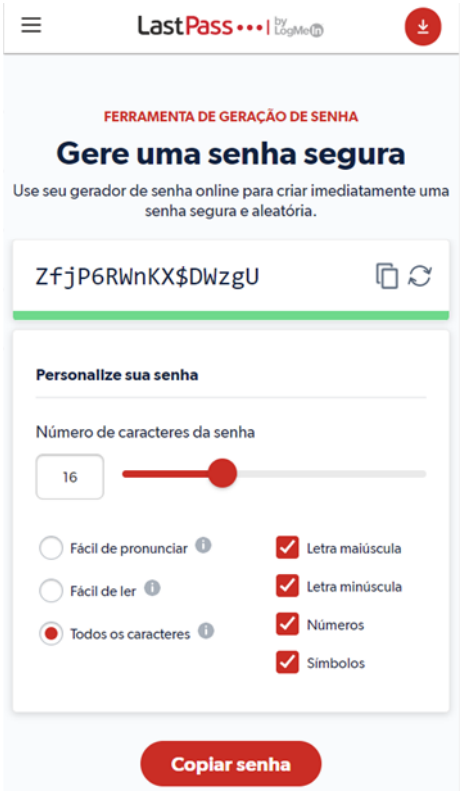
Os usuários virtuais deveriam atentar-se ao uso de senhas devido a sua grande importância para o acesso no mundo virtual. Além disso, é importante destacar que, senhas consideradas fracas e/ou muito antigas podem abrir as portas das informações dos usuários e de suas empresas para os criminosos virtuais (UNIMAKE SOFTWARE, 2018).

2.3.2 Gerenciadores de senhas

O gerenciador de senha é um site ou aplicativo que permite a criação de uma senha aleatória, que poderá ser usada em diversos sites e serviços (GOGONI, 2019). Os gerenciadores de senha podem gerar senhas longas e complexas, isso irá dificultar um ataque *hacker* (EMPEY, 2018).

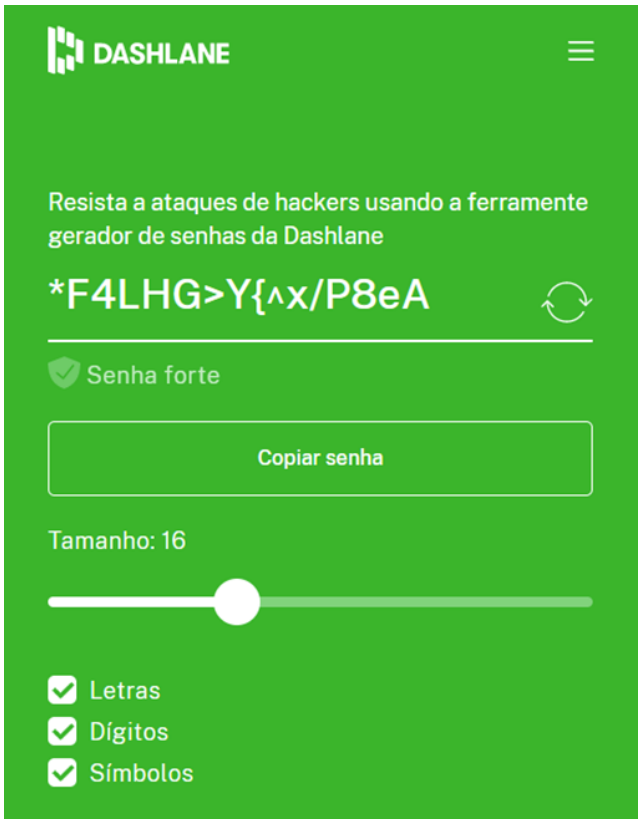
Há disponível em sites e aplicativos gerenciadores de senha como: Google Chrome (possui um gerenciador de senhas embutido), Gerador de senha (geradordesenha.com.br), LastPass (lastpass.com) mostrado na Figura 7, Gerador de senhas seguras (passwordgenerator.net), 4Devs (4devs.com.br), Avast - gerador de senhas aleatórias (avast.com), Dashlane (dashlane.com) mostrado na Figura 8 entre outros (GOGONI, 2019).

Figura 7 – Gerenciador de senhas LastPass



Fonte: LOGMEIN, 2021

Figura 8 – Gerenciador de senhas Dashlane



Fonte: DASHLANE INC, 2021

2.3.3 Métodos que ajudam manter as senhas mais seguras

Para que as senhas estejam seguras é importante utilizar bases seguras para armazená-las como os serviços de gerenciamento de senhas em nuvem. Esses serviços funcionam em sistema de nuvens ou em computadores físicos. Para ter acesso a este serviço será necessário utilizar apenas uma senha única que será a senha mestra, a qual lhe dará acesso a todas as outras senhas que estejam guardadas (MELO, 2019).

Além disso, para uma maior segurança da senha mestra de acesso, grande parte destes serviços de senhas oferecem a autenticação dupla através de um *software token*, mensagem de texto, notificação *push* ou grupos de *tokens* pré-definidos (cartão de números *token*) (MELO, 2019).

Em relação a alteração de senha, havia uma recomendação comum nas plataformas digitais especialmente no ambiente corporativo que era o recurso de expiração de senhas, ou seja, as senhas possuem validade máxima de aproximadamente três meses, após este período os usuários recebiam uma sugestão de alteração de senha, objetivando dificultar o acesso indevido de *hackers* (ALECRIM, 2019).

No entanto, a expiração de senha pode causar danos aos usuários, pois eles podem criar senhas previsíveis, compostas por palavras e números sequenciais relacionados entre si devido ao recebimento da informação de expiração sugerindo-se a troca. Assim, estes podem gerar uma senha prevista com base na senha anterior, a qual poderá ser fraca e de fácil acessibilidade (MICROSOFT, 2021).

A atual recomendação para troca de senhas é que ela seja alterada imediatamente sempre que desconfiar que ela possa ter sido descoberta ou após a utilização em computadores compartilhados, invadidos ou infectados (CERT, 2017). Além do mais, recomenda-se também a não reutilização de senhas anteriores ou criação de senhas semelhantes a senhas já utilizadas, manter as informações de recuperação de senhas atualizadas para auxiliar na identificação do usuário, além da autenticação multifator (MICROSOFT, 2021).

2.4 Seguraça *web*

Ferreira (2017) afirma que usuários leigos não sabem como avaliar se uma determinada aplicação ou acesso é realmente segura e/ou confiável. No geral, apenas acessam aplicações e/ou sites desenvolvidas por empresas conhecidas, nas quais acreditam ser seguras e de confiança. Assim, visando benefícios e segurança aos usuários *web* é importante que as empresas realizem investimentos para obterem segurança da informação, para não perderem a confiança de seus clientes e para evitarem possíveis danos a estes usuários.

Atualmente, construir uma aplicação *Web* segura é difícil devido aos ataques que os usuários podem sofrer. Em sua maioria, os ataques virtuais estão relacionados com as vulnerabilidades presentes na infraestrutura de aplicações, podendo ocorrer devido há *softwares* desatualizados, como por exemplo, o sistema operacional e os servidores de aplicações (FERREIRA, 2017).

Existe um ataque *web* simples e de fácil realização no qual consiste em apenas digitar comandos *Structured Query Language* (SQL) nos inputs de formulários da aplicação. Este ataque é chamado de SQL *Injection*. O ataque funciona da seguinte forma: valores digitados pelos usuários nos campos concatenados, ou seja, ligados diretamente há comandos SQL, sem ser realizada uma validação estará vulnerável ao ataque. O ataque é considerado simples pois não exige conhecimentos técnicos avançados para sua realização. Para realizá-lo, basta acessar na aplicação a tela que possua campo de texto e digitar trechos de comandos SQL nele. Por exemplo: '; *delete from usuarios*; (FERREIRA, 2017).

Caso uma aplicação possua vulnerabilidade que permita um ataque de SQL *Injection*, e se o usuário ou *hacker* executar o comando, ninguém conseguirá ter acesso a ela. Além disso, durante o ataque é possível digitar comandos SQL para apagar informações da aplicação e digitar comandos para a obtenção de informações dos usuários. Além disso, o ataque também pode recuperar informações sigilosas de seus usuários, como por exemplo, os dados de seus cartões de crédito como senhas; códigos de acesso. Isso pode gerar prejuízos grandes as empresas e aos seus clientes devido a exposição de informações sigilosas (FERREIRA, 2017).

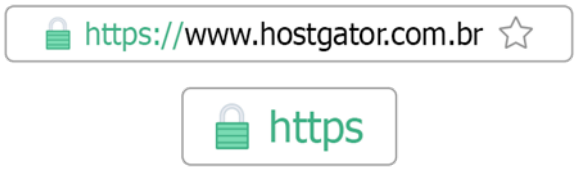
Devido aos ataques nas plataformas digitais é importante que os usuários fiquem atentos durante seu uso. É necessário ao ver a identificação da plataforma acessada, realizar a autenticação observando se a entidade é realmente quem ela diz

ser, gerenciar a autorização determinando que ações a entidade pode executar, verificar a integridade e a confidencialidade ou sigilo os quais são necessários para a segurança do usuário (CERT, 2012). É importante atentar-se para os certificados *Secure Socket Layer* (SSL) nas plataformas digitais.

Segundo um estudo do Serasa Experian, em parceria com a BigData Corp, no Brasil a cada seis lojas de *e-commerce*, uma delas não tem o certificado SSL. Apesar disto, houve um crescimento no número de lojas que decidiram buscar a proteção que o SSL proporciona. 83,3% das lojas tinham o certificado em abril de 2019, enquanto que, no ano anterior, esse índice era de apenas 79,9% (DEVALY, 2019).

O SSL é um mecanismo de criptografia criado para aumentar a segurança de dados que foram compartilhados pela *web*. Com a instalação do Certificado SSL, a URL do site passa para o formato *Hyper Text Transfer Protocol Secure* (HTTPS), com isso, é possível visualizar o ícone de um cadeado verde, mostrado na Figura 9, sinalizando que o site é seguro (DEVALY, 2019).

Figura 9 – Ícone do cadeado verde



Fonte: DEVALY, 2019

O Certificado SSL tem como objetivo adicionar uma proteção extra ao site de compras e entre outros, serve para proteger dados e informações financeiras. Essa forma de proteção é recomendada principalmente para sites de *e-commerce*. Quando o usuário digitar o número de um cartão de crédito em um site com o certificado SSL, os números serão codificados. Caso haja alguma invasão de hacker na conexão em busca de dados, ele não conseguirá traduzi-los (DEVALY, 2019).

Os certificados SSL possui algumas categorias: validação de domínio que é a proteção mais básica, a qual serve para identificar se um domínio é confiável e seguro para navegação; a validação da organização é um nível intermediário de segurança, em que ela certifica as informações de domínio e valida as informações da organização; e a validação estendida que é a mais completa, esta realiza uma análise profunda da empresa e do site (DEVALY, 2019).

Há disponível na *web* algumas ferramentas de verificação de vulnerabilidade do SSL como: SSL Labs, SSL Checker, Geekflare, Wormly, DigiCert, SSL Server Security Test, HowsMySSL, SSL Checker, Observatory, CryptCheck. Essas ferramentas *online* gratuitas servem para validar o parâmetro do certificado SSL e comunicação, visando manter o aplicativo *Web* seguro e menos vulnerável (FRARE, 2020).

2.4.1 Segurança em lojas virtuais

É crescente o número de usuários em sites de comércio eletrônico ou *e-commerce*. O *e-commerce* é definido como operações comerciais feitas no ambiente virtual, com ajuda de meios eletrônicos, de forma prática é comprar itens a quilômetros de distância, sem a necessidade de sair de casa ou do escritório (PERES, 2017).

As operações comerciais incluem a compra ou venda de produtos e/ou serviços por meio eletrônico, incluindo as atividades de negociação com as redes de computadores, no qual é feito a comunicação e negociação, o fechamento de pedidos, o pagamento e o atendimento ao cliente, dentre outras atividades pertinentes tudo de forma virtual (ECKERT et al, 2017). Seu acesso é facilitado através da utilização de *smartphone*, computador ou outros dispositivos (PERES, 2017).

Em 2013 no Brasil, empresas de varejo *online* faturaram R$ 28 bilhões, superando em mais de 20% as receitas do ano anterior (2012). No ano de 2014, as compras *online* movimentaram cerca de R$ 35 bilhões, evidenciando um crescimento de 24% em relação ao ano anterior. Já em 2015, o faturamento do setor de *e-commerce* foi de R$ 48,2 bilhões (ECKERT, 2017).

É possível observar que o crescimento das compras *on-line* reflete vantagens, para todos os usuários sejam ele compradores e/ou vendedores. Além disso, oferece vantagens também sobre lojas físicas ou tradicionais, gerando maior flexibilidade, maior alcance de mercado, estruturas de custos mais baixos, transações mais rápidas, linhas de produtos mais amplas, maior comodidade aos clientes e possibilidades de personalização (ECKERT, 2017).

As operações no ambiente virtual englobam todas as transações comerciais com base no processamento eletrônico, as quais incluem: transmissão de dados, textos, sons e/ou imagens, os quais são compartilhadas entre uma empresa e um consumidor, por exemplo, mercado do tipo *Business-to-Consumer (*B2C*)*, ou entre

diferentes empresas como no mercado corporativo do tipo *Business-to-Business (*B2B*)*. Em ambos os tipos de mercado, são levantadas questões de segurança técnica (ECKERT, 2017).

No mercado do tipo B2C são levantas maiores questões de privacidade, visto que há uma interação e compartilhamento de informações sigilosas entre uma empresa e um consumidor. Já no mercado corporativo B2B a atenção e os investimentos acerca de questões de segurança e privacidade já vem sendo intensificados, tendo em vista o volume de recursos transacionados e a magnitude de eventuais perdas ou penalizações (ECKERT, 2017).

Além do mais, durante as compras *on-line* a privacidade está direcionada à preocupação com a informação que é gerada como resultado das ações dos consumidores. Essas atividades *on-line* lidam-se basicamente com a coleta de dados e informações dos consumidores, do seu compartilhamento, da sua utilização e armazenamento adequado. Além disso, registros referentes às transações efetivadas, dados pessoais, informações demográficas e econômico-financeiras. Sendo assim, a privacidade virtual refere-se ao grau em que o site de compras *on-line* é seguro, sendo capaz de proteger os dados e as informações dos clientes (ECKERT, 2017).

Nos sites de *e-commerce* há disponível diversas formas de pagamento como: transferência ou boleto bancário, cartão de débito e crédito e cartão virtual (ABCOMM, 2013). Atualmente o boleto bancário é a forma de pagamento mais escolhida em *websites* de *e-commerce* de pequeno porte, em que o cliente reconhece a dívida e dá o aceite no arquivo eletrônico que é o boleto (DANTAS, 2021).

Na utilização da forma de cobrança *online* com o cartão de débito, é necessário o envio do arquivo de cobrança da empresa prestadora para o cliente. Em seguida, o banco solicita autorização do cliente para debitar diretamente da conta corrente (DANTAS, 2021).

Nas compras com cartão de crédito, o cliente paga no exato momento da confirmação da compra, ou seja, o banco emissor do cartão de crédito do cliente, recebe a informação em tempo real, realiza a solicitação de aprovação, após a aprovação é cobrado o valor da compra no limite do cartão de crédito do cliente (DANTAS, 2021).

Atualmente vem sendo utilizado o cartão virtual, que é classificado como uma versão digital do cartão físico, podendo ser utilizado para compras na internet entre outras plataformas. Ele proporciona aos seus usuários maior segurança, oferecendo

uma proteção a mais contra golpes virtuais. Ele também possui a vantagem de efetuar compras mesmo sem ter o cartão físico em mãos, os usuários só precisam tê-lo em um aplicativo instalado no smartphone (BEZERRA, 2020).

Além disso, há também ferramentas de pagamento *online* seguras, estas ferramentas não enviarão os dados para a loja destino, mas para uma conta virtual do serviço de pagamento, realizando então uma intermediação do processo. Caso deseje utilizar essas ferramentas de pagamento, utilize serviços mais comuns como o PagSeguro, PayPal, Bcash, Mercado Pago e Moip (ABCOMM, 2013).

É importante que os usuários fiquem atentos durante a realização de compras *online*. Sendo assim, é viável que não seja efetuado download de aplicativos suspeitos; não abrir *links* desconhecidos; não fornecer dados pessoais e sigilosos sem antes verificar a segurança do site; é importante desconfiar sempre e checar a procedência do site; não cadastrar a mesma senha e *login* em todos os sites utilizados; não deixar os dados do cartão de crédito salvos no site (POLÍCIA CIVIL DO CEARÁ, 2020).

2.5 Vulnerabilidades em *wi-fi* públicos

Em 1985, foi criada a rede *Wi-Fi*, que é uma tecnologia utilizada em redes de computadores, que possui a capacidade de transmitir dados sem a necessidade de cabos. Ela pode ser usada através de dispositivos como *smartphones*, TVs, *notebooks*, entre outros (TASINAFFO, 2019).

Segundo Martins et al (2017), há um crescimento considerável de usuários conectados através das redes públicas. Porém, com este aumento de usuários se conectando através de redes públicas sem fio, também crescem as ameaças; os ataques cibernéticos, invasões e roubo de informações, que podem ocasionar problemas para os usuários. Além disso, Martins et al (2017) também ressalta que as redes *Wi-Fi* públicas oferecem riscos quando ocorre conexão à internet sem as devidas medidas de proteção.

Sabe-se que quando se utiliza a conexão por rede sem fio de forma doméstica, existe um protocolo de segurança, o qual permite apenas as máquinas autenticadas (aquelas em que utilizaram a senha de acesso) a utilizá-la, bem como um *firewall*, que, em geral, garante a não conexão de usuários desconhecidos na respectiva rede. Porém, nas redes públicas não existe esta garantia de autenticidade, uma vez que,

mesmo solicitando a realização de um *login* e senha para acesso, este processo é somente para a liberação da utilização do sinal, não é uma garantia de segurança do tráfego de dados como uma forma de segurança (TASINAFFO, 2021).

A utilização de redes *Wi-Fi* públicas e computadores de terceiros, não oferecem conexões seguras (ABCOMM, 2013). Aproximadamente, 58% dos usuários brasileiros acreditam que suas informações pessoais estão seguras mesmo durante o uso do *Wi-Fi* público. Porém, nas redes públicas, não há nenhuma garantia de autenticidade ou que os roteadores possuem protocolo de segurança, ou que estejam utilizando um *firewall* (OLHAR DIGITAL, 2019).

Ao conectar-se em uma rede pública, todos os usuários conectados ficaram visíveis uns para os outros, e um criminoso virtual pode com facilidade descobrir um computador vulnerável para interceptar as informações enviadas. Dessa forma, o criminoso consegue acesso ao que está sendo verificado pelo usuário, conseguindo capturar todas as informações pessoais disponíveis, como senhas, dados bancários, entre outras informações (TASINAFFO, 2019).

Durante a utilização de *wi-fi* público é importante atentar-se a alguns prontos: ficar atento aos sites acessados e verificar se ele apresenta o ícone de segurança, que é comumente conhecido pelo cadeado na barra de endereço, este confirma que o site visitado conta com o chamado HTTPS, isso assegura que a transferência de dados entre usuário e site é seguro e criptografado (TASINAFFO, 2021).

Além disso, não é recomendável realizar compras que necessitem a digitação de numeração completa de cartão de crédito e/ou acesso a informações corporativas mesmo que os sites visitados, como os de instituições bancárias, contenham mecanismos fortes de segurança, ainda existe a possibilidade das informações pessoais dos usuários serem interceptados. Isso é o ataque "*man-in-the-middle*", onde o criminoso acessa todos os dados enquanto o usuário navega (TASINAFFO, 2021).

Um outro risco que o uso do *Wi-fi* público pode trazer é o recebimento de mensagens falsas, via WhatsApp ou *e-mail*, isso ocorre devido as práticas de *phishing* que é uma armadilha para pegar informações e dados importantes. Em sua maioria, as mensagens chegam com o oferecimento de algum brinde ou promoção, objetivando levá-lo a clicar no *link* malicioso (OLHAR DIGITAL, 2019).

Além disso, após acessar *e-mail*, conta em lojas virtuais, Facebook, internet banking ou qualquer outro serviço que exige nome de usuário e senha, é muito importante realizar o “*Logout*” (sair), *Logoff*, desconectar das contas acessadas após

o término para manter as informações pessoais seguras (ABCOMM, 2013; DEV SOLUTIONS, 2016).

Caso não forem realizados tais procedimentos para encerramento do acesso, o site não receberá a instrução de encerramento, desta forma outra pessoa poderá reabrir a página usada logo em seguida e acessar as informações, ou seja, poderá *hackear* os dados disponíveis ali devido ao não encerramento de acesso (DEV SOLUTIONS, 2016).

2.6 *Keyloggers*

Keylogger em inglês significa "gravador de teclado" e como o nome sugere ele registra todas as teclas digitadas por um usuário infectado para obter senhas números de cartão de crédito etc. Esse tipo de *malware* é classificado na categoria de *spyware* (HSC Brasil, 2019).

Embora seja usado por criminosos para capturar informações pessoais, o uso de *keyloggers* não é exclusivo dos criminosos, ele pode ser usado de forma não fraudulenta para registrar *logs* de dados ou para salvar informações inseridas por um *software* de terceiros (HSC Brasil, 2019).

Keyloggers geralmente passam despercebidos pelos usuários, mas dependendo do *software*, pode causar oscilações do *mouse* ao usar o teclado. Isso pode significar que a digitação está sendo capturada por um programa *spyware*, que pode enviar as informações a um invasor (HSC Brasil, 2019).

Uma maneira eficaz de identificar uma infecção de *keylogger* é usar um bom sistema antivírus (HSC Brasil, 2019).

A melhor maneira de se proteger contra ameaças cibernéticas é por meio da prevenção. E para prevenção, temos duas formas principais: boas práticas e sistemas de proteção (HSC Brasil, 2019).

Como boa prática, comportamentos de risco devem ser evitados ao navegar na Internet, como baixar *software* pirata, principalmente via *torrents*, visitar sites desconhecidos e que utilizam de anúncios de marcas de reputação duvidosa e clicar em *links* em *e-mails* recebidos por pessoas que não são conhecidas (HSC Brasil, 2019).

Em um ambiente empresarial, o ideal é capacitar os usuários, explicando os perigos de uma navegação imprudente. Afinal, isso coloca em risco os dados dos funcionários e a própria empresa (HSC Brasil, 2019).

Um dos métodos usados pelos bancos para proteger seus clientes é inserir senhas e outros dados confidenciais por meio de teclados virtuais. Isso evita que um *malware* capture informações inseridas com o teclado. Embora não seja eficaz contra todas as ameaças, é eficaz contra *keyloggers* (HSC Brasil, 2019).

Uma maneira eficaz de os usuários se protegerem é usar a tecnologia de proteção contra ameaças. Um bom antivírus é definitivamente uma boa ideia. Mas é necessário ir mais longe, é preciso agir antes da infecção acontecer (HSC Brasil, 2019).

3 IMPLEMENTAÇÃO E RESULTADOS

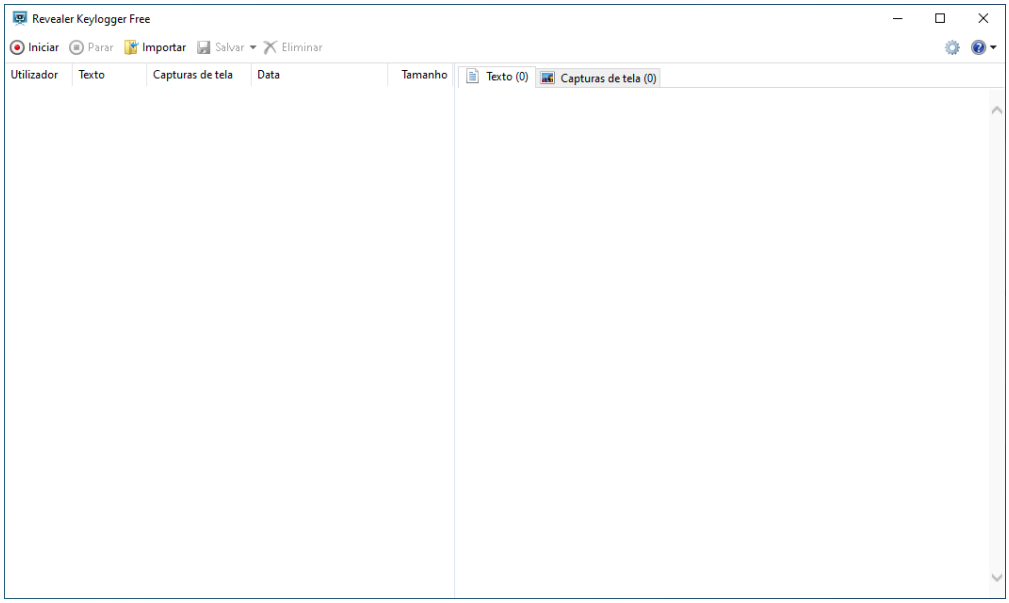
Nesta seção serão apresentados a implementação de um site, as discussões e resultados que foram apresentados no decorrer deste trabalho. Em todos os testes foram realizadas ilustrações de capturas de dados dos usuários sem o conhecimento ou consentimento deles. Na primeira etapa do estudo de caso foi utilizado uma ferramenta para realizar a captura de dados. Na segunda etapa, para o estudo de caso foi desenvolvido um site para realizar este tipo de captura.

Em 2007, houve episódios de captura de senhas através de site falso. O ataque recebeu o nome de “Zeus”, o qual era muito utilizados em casos de roubos de credenciais e senhas (INSTITUTO INFORMATION MANAGEMENT, 2019).

3.1 Captura de dados utilizando *keylogger*

Os experimentos foram realizados utilizando o *software* Revealer Keylogger Free. Uma vez instalado na máquina e executando o mesmo, é possível iniciar a captura de dados ao clicar no botão “Iniciar”, conforme apresentado na Figura 10.

Figura 10 – *Software* Revealer Keylogger Free



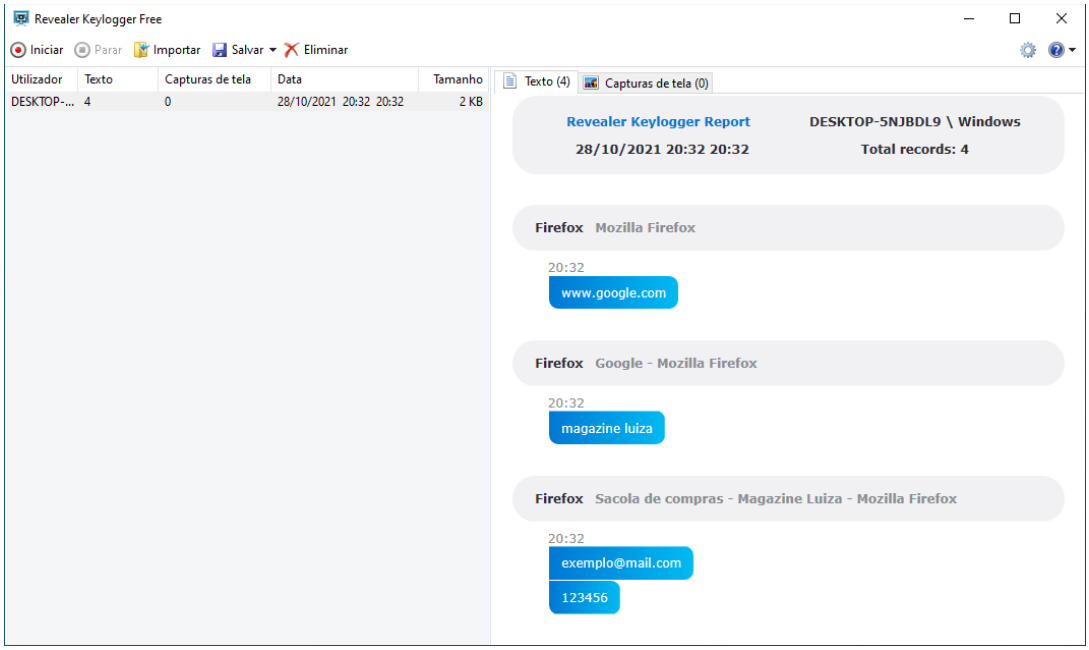
Fonte: Elaborado pelo autor

Após iniciar, o *software* é executado em segundo plano de forma oculta e não exibe nenhuma mensagem na tela que possa identificar a execução dele. O programa

não aparece no gerenciador de tarefas, na barra de tarefas ou na lista de programas instalados.

No decorrer do experimento, foi realizado o acesso ao site do Google para efetuar uma busca por Magazine Luiza, após acessar o site foi realizada uma tentativa de *login*. Todos os dados digitados foram registrados pelo programa, desde o acesso ao Google, até os dados de *login* no site da Magazine Luiza. Além do registro de digitação, o *software* também realiza uma contagem de registros que foram capturados e salva a data e a hora de cada captura, conforme mostrado na Figura 11. Tudo isto realizado sem que o usuário perceba.

Figura 11 – Dados registrados



Fonte: Elaborado pelo autor

Conforme exposto na seção 2.6 o *software* utilizado faz parte da categoria de *spyware* onde ele realizou a captura de *login* e senha do usuário, nos quais são considerados dados sigilosos, além de outras informações de navegação, a captura ocorreu de forma silenciosa e oculta, de maneira que o usuário não desconfie de nada.

3.2 Desenvolvimento do site para realizar estudo de caso

Serão apresentadas a seguir as tecnologias para o desenvolvimento do site utilizado no estudo de caso.

3.2.1 HTML

O *Hypertext Markup Language (*HTML) significa Linguagem de Hipertexto por Anotações, foi criado por um físico, Tim Berners-Lee, do centro de pesquisas CERN, na Suíça. O HTML surgiu com a ideia de um sistema de hipertexto na internet. Um hipertexto é um texto que possui referências, ou seja, *links* para outros textos que podem ser acessados imediatamente. O HTML é uma implementação simultânea da norma ISO 8879:1986 *Standard Generalized Markup language* (SGML) e da norma ISO 10744:1992 *Hypermedia/Time-based Document Structuring Language (*HYTIME*)* (LONGEN, 2021).

O HTML permite que os usuários criem e estruturem seções, parágrafos, cabeçalhos e *links* para páginas da internet ou até mesmo aplicações. Ele não é uma linguagem de programação, ou seja, não pode ser usado para criar funcionalidades dinâmicas. Porém, o HTML possibilita a organização e formatação de documentos, semelhante ao Microsoft Word (LONGEN, 2021).

As diretivas HTML (que não são sensíveis ao tipo de caixa, isto é, maiúsculas e minúsculas são idênticas) são delimitados pelos caracteres menor < e maior > e, por exemplo; exemplos de diretivas são: <TITLE>, <HEAD>, <P>, etc. Elas são interpretadas pelo navegador com objetivo de produzir algum efeito visual ou de estrutura lógica do documento hipertexto (LONGEN, 2021).

O programador de HTML não tem controle sobre o efeito final do documento. Assim, este *link* pode variar, de acordo com as configurações do navegador, tais como: dimensões da área de visualização, escolha das fontes tipográficas, nível de HTML suportado, versão e marca do programa navegador, limitações de dispositivos (*hardware* e *software*) (LONGEN, 2021).

3.2.2 CSS

O CSS, foi desenvolvido pelo *World Wide Web Consortium (*W3C*)* em 1996. O CSS dá estilo ao código criado por linguagens como por exemplo: HTML, *Extensible Markup Language* (XML) ou *Extensible HyperText Markup Language* (XHTML). Assim, ela funciona como uma camada de personalização ao conteúdo visível (GONÇALVES, 2021; OKUBO, 2021).

O CSS é um código em que há possibilidade de realizar alterações rápidas de layout, como definição de cores e fontes. Essa camada proporciona não apenas a facilidade de personalização, mas também ajuda a diminuir a repetição de conteúdo na estrutura do código. Esse tipo de configuração pode ser feito na folha de estilo, não precisaria se repetir diversas vezes na própria linguagem (OKUBO, 2021).

Algumas das propriedades que ele permite são: manter um padrão de formatação em diferentes navegadores, controle de *layout* em apenas uma folha, criação de formatações com *designs* mais responsivos, pensando em usabilidade e experiência do usuário (OKUBO, 2021).

O CSS possui alguns estilos que podem ser utilizados como o Interno, Externo e o *Inline*. O estilo Interno, é carregado cada vez que um site é atualizado, o que pode aumentar o tempo de carregamento. No estilo Externo tudo é feito externamente em um arquivo .css., podendo fazer todo o estilo em um arquivo separado e aplicar o CSS a qualquer página desejada. No estilo *Inline*, este trabalha com elementos específicos que possuem a tag <*style*>. Cada componente deve ser estilizado (GONÇALVES, 2021).

3.2.3 JavaScript

O JavaScript, foi criado em 1996 pelo programador Brendan Eich. O JavaScript é uma linguagem de programação de alto-nível. Essa linguagem de programação Javascript permite ao desenvolvedor implementar diversos itens de alto nível de complexidade em páginas *web*, como por exemplo; animações, mapas, gráficos ou informações que se atualizam em intervalos de tempo padrão. Além disso, o Javascript é a terceira camada do bolo de desenvolvimento *web* e *front-end*, juntamente com HTML, CSS e *Hypertext Preprocessor* (PHP) (ESTRELLA, 2021).

Com a utilização do JavaScript o programador irá encontrar alguns benefícios do uso dessa linguagem, como; não necessita de um compilador porque os navegadores de internet o interpretam com HTML, em relação a aprendizagem ele é mais fácil de ser aprendido em relação a outras linguagens de programação, caso haja erros este são mais fáceis de serem localizados, ele pode ser designado a certos elementos de páginas de internet ou eventos específicos, como cliques e rolagens de mouse personalizados, é compatível com várias plataformas e navegadores, além disso, ele é mais rápido e mais leve que outras linguagens de programação (ESTRELLA, 2021).

3.2.4 Visual Studio Code

Em 2015 foi lançado pela Microsoft um editor de código destinado ao desenvolvimento de aplicações *web* chamado Visual Studio Code. É uma ferramenta leve e multiplataforma que está disponível para Windows, Mac OS e Linux, sendo executada nativamente em cada plataforma (MACORATTI, 2016).

Além disso, o Visual Studio Code atende a uma quantidade grande de projetos (ASP .NET, Node.js) e oferece suporte para mais de 30 linguagens de programação, como JavaScript, C#, C++, PHP, Java, HTML, R, CSS, SQL, Markdown, TypeScript, LESS, SASS, JSON, XML e Python, assim como muitos outros formatos de arquivos comuns (MACORATTI, 2016).

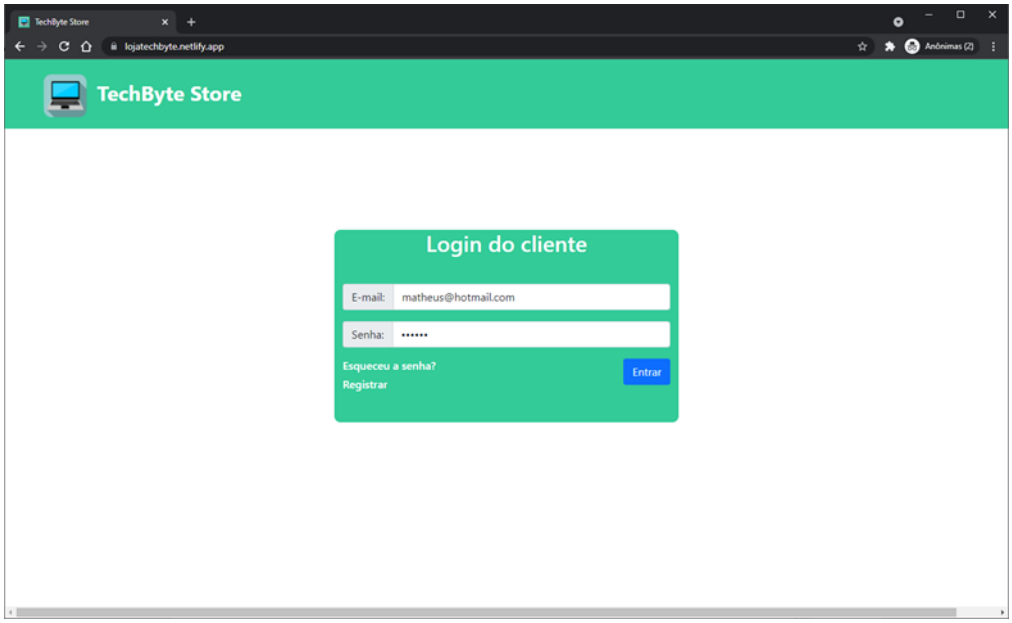
O VSCode é um editor leve de primeira classe, com gestos centralizados no teclado. Com ele é possível permanecer no contexto enquanto ocorre a movimentação através de grandes arquivos de código e através da sua base de código. O Visual Studio Code suporta o fluxo de trabalho de desenvolvimento de ponta a ponta para aplicativos em ASP.NET 5 e Node.js, IntelliSense completo, suporte para depuração e muito mais (MACORATTI, 2016).

3.2.5 Implementação

Foi desenvolvido um site *web* com a intenção de simular páginas falsas de uma loja virtual. Esta página pode ser encontrada através do anúncio do produto no qual possui um *link* de acesso a este site. Foi desenvolvido a página de *login*, apresentada na Figura 12, onde o usuário deve informar um *e-mail* e senha, porém não é realizado

qualquer tipo de validação para as credenciais informadas deixando o usuário acessar o sistema, o código fonte HTML encontra-se no Apêndice A, CSS no Apêndice B e JavaScript no Apêndice C.

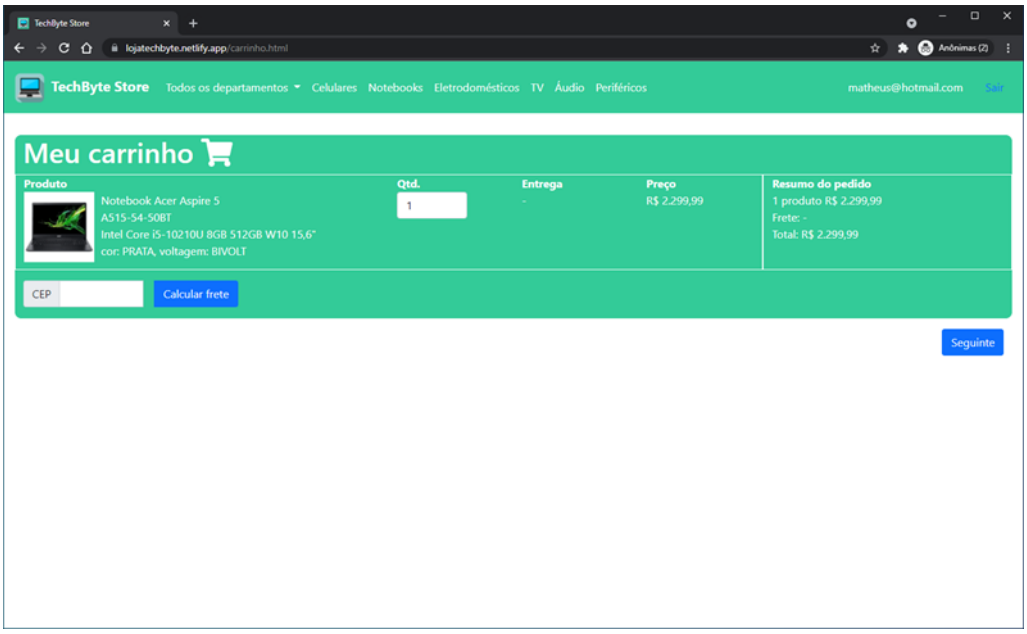
Figura 12 – Tela de *login*



Fonte: Elaborado pelo autor

Foi desenvolvida a página do produto, mostrada na Figura 13, onde é possível encontrar mais detalhes do produto, além de um campo para preenchimento do Código de Endereçamento Postal (CEP) onde é realizada uma requisição a uma *Application Programming Interface* (API) de CEP para buscar os dados de endereço conforme o CEP informado. Também é simulado o cálculo do frete do produto com entrega para 5 dias após a data no qual está sendo realizada a compra. O código fonte HTML encontra-se no Apêndice D, CSS no Apêndice E e JavaScript no Apêndice F.

Figura 13 – Tela do produto



Fonte: Elaborado pelo autor

Na etapa da compra, mostrado na Figura 14, são solicitadas as informações do usuário, onde o sistema pode trazer informações do endereço com base no CEP informado na etapa anterior. O site não possui nenhuma validação dos dados informados, mas ao finalizar a compra é simulado um envio de *e-mail* referente a compra realizada. O código fonte HTML encontra-se no Apêndice G, CSS no Apêndice H e JavaScript no Apêndice I.

Figura 14 – Tela de compra

Fonte: Elaborado pelo autor

3.3 Captura de dados utilizando o site desenvolvido

O experimento foi realizado no site desenvolvido para realizar este estudo de caso. Foi realizado o acesso no site utilizando o *login* com o *e-mail* matheus.oliveira@hotmail.com e senha 123456. A página do site avançou normalmente para as próximas telas sem problema algum.

Durante a utilização do site o usuário pode ter suas informações coletadas sem seu conhecimento ou consentimento, como apresentado na Figura 15, podendo assim serem utilizadas para efetuar *login* nos sites oficiais ou outros serviços, caso exista cadastro com as mesmas informações.

Figura 15 – Captura de dados

Key	Value
dados_login	[{"usuario":"matheus@hotmail.com","senha":"123456"}]

Fonte: Elaborado pelo autor

Conforme abordado na seção 2.2.2, o site falso pode coletar as informações cadastrais do usuário e transmiti-las para os criminosos. Uma vez que o usuário tenha seus dados capturados, o prejuízo pode ser ainda maior, caso ele utilize os mesmos

dados para diversos sites ou serviços diferentes, por isso a importância de se ter senhas diferentes em cada conta, conforme exposto na seção 2.3.

4 CONSIDERAÇÕES FINAIS

Neste capítulo serão abordadas as conclusões referentes as pesquisas e experimentos realizados, além de obstáculos encontrados durante todo o desenvolvimento deste trabalho.

4.1 Considerações finais

Apresentou-se neste trabalho um estudo de boas práticas na segurança *web* nos quais são possíveis identificar como funcionam os ataques de *phishing.* Realizou-se o desenvolvimento de uma página *web*. Também foi demonstrado como os dados podem ser capturados em sites de *e-commerce* sem que o usuário perceba, em um site verdadeiro ou falso.

Conclui-se com este trabalho que existem usuários que por falta de atenção ou conhecimento muitas vezes caem em golpes e crimes virtuais de maneira muito fácil e quando eles percebem já é tarde demais, ou seja, tiveram seus dados capturados podendo serem utilizados de forma indevida e por conta disto podem ser prejudicados de alguma forma.

Também podemos notar a importância de seguir as boas práticas de segurança que foram abordadas neste trabalho para evitar cair nestes golpes virtuais.

4.2 Dificuldades encontradas

Durante o desenvolvimento do trabalho, encontrou-se dificuldade quanto ao material de pesquisa, pois não foi encontrado livros referentes ao assunto abordado, forçando a limitar-se apenas com pesquisas *web*, revistas e artigos.

Houve dificuldade para realizar um estudo de caso utilizando um site falso que seja real. Devido a estes sites não se manterem por um longo período no ar foi realizado o desenvolvimento de um site para suprir esta necessidade.

4.3 Trabalhos futuros

Algumas sugestões de trabalho futuro são:

- Realizar estudo de caso relacionado as demais técnicas de *phishing* apresentadas neste trabalho;
- Realizar estudo de caso sobre a rede de *wi-fi* pública, de forma a demonstrar na prática como ocorre a captura de dados nestas redes através de ferramentas apropriadas;
- Realizar estudo a fim de mostrar a facilidade de quebrar senhas que não seguem as recomendações de segurança abordadas na seção 2.3.1.

REFERÊNCIAS BIBLIOGRÁFICAS

ABCOMM. ASSOCIAÇÃO BRASILEIRA DE COMÉRCIO ELETRÔNICO. **Aprenda a comprar com segurança na internet.** Cartilha do e-consumidor brasileiro. 2013. Disponível em: <https://www2.camara.leg.br/atividadelegislativa/comissoes/comissoes-permanentes/cdc/publicacoes/cartilhaeconsumidorabcomm.pdf>. Acesso em: 2021.

ALECRIM, Emerson. **Microsoft deixa de recomendar mudança periódica de senha no Windows.** Tecno blog. 2019. Disponível em: <https://tecnoblog.net/287341/microsoft-windows-10-expiracao-senha/>. Acesso em: 2021.

BELCIC, Ivan. **O guia essencial sobre phishing: Como funciona e como se proteger.** AVAST. 2021. Disponível em: <https://www.avast.com/pt-br/c-phishing#topic-1> Acesso em: 2021.

BEZERRA, Leonardo. **O que é cartão virtual: novas formas de aceitar crédito ou débito.** Boavista Tecnologia. 2020. Disponível em: <https://boavistatecnologia.com.br/blog/o-que-e-cartao-virtual/>. Acesso em: 2021.

CERT. 8. **Contas e Senhas**. Cartilha de Segurança para Internet. Centro de Estudos, Respostas e Tratamentos de Incidentes de Segurnaça no Brasil. 2017. Disponível em: <https://cartilha.cert.br/senhas/>. Acesso em: 2021.

CERT. **Cartilha de segurança para a internet.** versao 4.0 / CERT.br – S ˜ ao Paulo: Comitê Gestor da Internet no Brasil, 2012. Disponivel em: <https://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf> Acesso em: 2021.

CONCEITO.DE. **Conceito de senha.** 2020. Disponivel em: <https://conceito.de/senha>. Acesso em: 2021.

DANTAS, Rodrigo. **Pagamento online: como receber por boleto, cartão de crédito e débito.** Vindi Blog. 2021. Disponível em: <https://blog.vindi.com.br/pagamento-online/>. Acesso em: 2021.

DEVALY, Eduarda. **O que é certificado SSL e porque você deve utilizar no seu site.** HostGator Blog. 2019. Disponível em: <https://www.hostgator.com.br/blog/o-que-e-certificado-ssl-e-porque-voce-deve-utilizar-no-seu-site/>. Acesso em: 2021.

DEV SOLUTIONS. **SAIA CLICANDO EM "LOGOUT", "SAIR" OU EQUIVALENTE.** DevSolutions Blog. 2016. Disponível em: <https://www.devsolutions.com.br/blog/artigos/saia-clicando-em-logout-sair-ou-equiva lente>. Acesso em: 2021.

E-COMMERCE BRASIL. **E-commerce brasileiro tem a maior alta dos últimos 20 anos, aponta Ebit|Nielsen.** 2020. Disponível em: <https://www.ecommercebrasil.com.br/noticias/e-commerce-brasileiro-tem-a-maior-alta-dos-ultimos-20-anos-aponta-ebit nielsen/>. Acesso em: maio, 2021.

ECKERT, Alex**. E-COMMERCE: PRIVACIDADE, SEGURANÇA E QUALIDADE DAS INFORMAÇÕES COMO PREDITORES DA CONFIANÇA.** Revista Pensamento Contemporâneo em Administração, vol. 11, núm. 5, pp. 49-69. Universidade Federal Fluminense Rio de Janeiro. 2017.

EMPEY, Charlotte**. Como criar uma senha segura.** 2018. Blog Avast. Disponível em: <https://blog.avast.com/pt-br/como-criar-uma-senha-segura>. Acesso em: 2021.

ESTRELLA, Carlos Felipe Penedo de Paiva. **O que é JavaScript.** Hostinger. 2021. Disponível em: <https://www.hostinger.com.br/tutoriais/o-que-e-javascript?ppc_campaign=google_performance_max&gclid=Cj0KCQjwnoqLBhD4ARIsAL5JedLtgct3n09_jWBXM18ZFeG8Sn8KOgi8xEe2HCPlFb1Z1QYnojKREWUaAhteEALw_wcB>. Acesso em: 2021.

FERREIRA, Rodrigo. **Segurança em aplicações Web.** Série Caelum. Casa do Código. 2017. Disponível em: <https://www.google.com.br/books/edition/Seguran%C3%A7a_em_aplica%C3%A7%C3%B5es_Web/IyUaDgAAQBAJ?hl=pt-BR&gbpv=1&printsec=frontcover>. Acesso em: 2021.

FRARE, Adriano. **CERTIFICADO DIGITAL CIBERSEGURANÇA DESTAQUES NOTÍCIAS TLS E SSL - 10 ferramentas online para testar SSL, TLS e vulnerabilidades.** CRYPTO ID. 2020. Disponível em: <https://cryptoid.com.br/banco-de-noticias/10-ferramentas-online-para-testar-ssl-tls-e-vulnerabilidades/>. Acesso em: 2021.

FRITZEN, Cledison Eduardo. **Recomendações e dicas para criar senhas fortes e seguras.** 2020. Disponível em: <https://www.lumiun.com/blog/recomendacoes-e-dicas-para-criar-senhas-fortes-e-seguras/>. Acesso em: 2021.

GARGIONI, Tarcísio. **E-commerce no Brasil: a evolução e as tendências do setor.** E-commerce Brasil. 2011. Disponível em: <https://www.ecommercebrasil.com.br/artigos/e-commerce-no-brasil-a-evolucao-e-as-tendencias-do-setor/>. Acesso em: 27 de outubro de 2021.

GOGONI, Ronaldo. **10 apps e sites com gerador de senha para você usar.** 2019. Tecno blog. Disponível em: <https://tecnoblog.net/310406/10-apps-e-sites-com-gerador-de-senha-para-voce-usar/>. Acesso em: 2021.

GOLÇALVES, Ariane. **O que é phishing e como se proteger de golpes na internet.** Hostinger. 2021. Disponível em: <https://www.hostinger.com.br/tutoriais/o-que-e-phishing-e-como-se-proteger-de-golpes-na-internet>. Acesso em: 2021.

GONÇALVES, Ariane. **O que é CSS? Guia Básico para Iniciantes.** Hostinger. 2021. Disponível em: <https://www.hostinger.com.br/tutoriais/o-que-e-css-guia-basico-de-css?ppc_campaign=google_performance_max&gclid=Cj0KCQjwnoqLBhD4ARIsAL5JedJ6Yz8zIkhCyJxOwauGnN4oKPi5eA00MoxFmwUAIZCvUqVCD4aYkzAaAkJ9EALw_wcB>. Acesso em: 2021

HSC Brasil. **Keylogger, o que é e como se proteger desta ameaça!.** 2019. Disponível em: <https://www.hscbrasil.com.br/keylogger/>. Acesso em: 2021

INFORMATION Instituto, Ariane. **8 casos reais e famosos de ataques de malware.** 2019. Disponível em: <https://docmanagement.com.br/06/27/2019/8-casos-reais-e-famosos-de-ataques-de-malware>. Acesso em: 2021

JACKSON, Scott. **10 melhores gerenciadores de senhas [promoções + cupons].** Safety Detectives. 2021. Disponível em: <https://pt.safetydetectives.com/best-password-managers/>. Acesso em: 10 maio. 2021.

LOGIXOFT. **Baixar o Revealer Keylogger Grátis 2021 para Windows 10.** Logixoft. 2011. Disponível em: <https://www.logixoft.com/pt-br/index>. Acesso em: 27 de outubro de 2021.

LONGEN, Andrei Silveira. **O Que é HTML? Guia Básico Para Iniciantes.** Hostinger. 2021. Disponível em: <https://www.hostinger.com.br/tutoriais/o-que-e-html-conceitos-basicos/amp> Acesso em: 2021.

MACORATTI, José Carlos. **Visual Studio Code – Apresentando o editor multiplataforma da Microsoft.** iMasters. 2016. Disponível em: <https://imasters.com.br/desenvolvimento/visual-studio-code-apresentando-o-editor-multiplataforma-da-microsoft> Acesso em: 2021.

MARINO, M. **A 20 senhas mais hackeadas do mundo: A sua está aqui?** Disponível em: <https://pt.safetydetectives.com/blog/the-most-hacked-passwords-in-the-world-pt/>. Acesso em: Acesso em: 10 maio. 2021.

MARTINS, Jâmison de Mendonça. **WI-FI PÚBLICO RISCOS E SOLUÇÕES*.** XIII Congresso Internacional de Linguagem e Tecnologia Online. UEMG Carangola. 2017.

MELO, Kleber. **Onde armazenar minhas senhas? É seguro usar serviços em nuvem?** .2019. Minuto da segurança o blog da segurança da informação. Disponível em: <https://minutodaseguranca.blog.br/onde-armazenar-minhas-senhas-e-seguro-usar-servicos-em-nuvem/>. Acesso em: 2021.

MICROSOFT. **Recomendações de política de senha.** 2021. Disponível em: <https://docs.microsoft.com/pt-br/microsoft-365/admin/misc/password-policy-recommendations?view=o365-worldwide>. Acesso em: 2021.

OKUBO, Beatriz. **Você Sabe o que é CSS? Entenda Como Funciona e Para que Serve.** GoDaddy. 2021. Disponível em: <https://br.godaddy.com/blog/voce-sabe-o-que-e-css-entenda-como-funciona-e-para-que-serve/amp/> .Aceso em: 2021.

OLHAR DIGITAL. **Wi-Fi público: entenda os riscos de usar o Wi-Fi fora de casa.** 2019. Disponível em: <https://olhardigital.com.br/2019/07/19/seguranca/wi-fi-publico-entenda-os-riscos-de-usar-o-wi-fi-fora-de-casa/> .Acesso em: 2021.

PERES, Paulo Júnior de Jesus; et.al. **Construindo Aplicações Web Habilitadas à Segurança.** Revista Científica Multidisciplinar Núcleo do Conhecimento. Edição 07. Ano 02, Vol. 03. pp 44-51, Outubro de 2017. ISSN:2448-0959.

POLÍCIA CIVIL DO CEARÁ. **Polícia Civil orienta sobre como evitar golpes em compras virtuais durante quarentena.** Secretaria da Segurança Pública e Defesa Social. Governo do Estado do Ceará. 2020. Disponível em: <https://www.policiacivil.ce .gov.br/2020/04/16/policia-civil-orienta-sobre-como-evitar-golpes-em-compras-virtuais-durante-quarentena/> .Acesso em: 2021.

TASINAFFO, Fernanda**. Os riscos da utilização do WiFi público.** Jusbrasil. 2019. Disponível em: <https://canalc ienciascriminais.jusbrasil.com.br/artigos/561307814/os-riscos-da-utilizacao-do-wifi-publico> Acesso em: 2021.

TASINAFFO, Fernanda. **Riscos da utilização do wi-fi público.** Migalhas. 2021. Disponível em: <https://www.migalhas.com.br/depeso/340063/riscos-da-utilizacao-do-wi-fi-publico> Acesso em: 2021.

TAGIAROLI, G. **Especialistas dão dicas para memorizar e criar senhas na web.** UOL Notícias. 2011. Disponível em: <https://www.uol.com.br/tilt/noticias/redacao/2011/02/22/especialistas-dao-dicas-para-memorizar-e-criar-senhas-na-web.htm>. Acesso em: 10 maio. 2021.

APÊNDICE A – CÓDIGO HTML DA PÁGINA INICIAL

```
<!DOCTYPE html>
<html lang="pt-br">
  <head>
    <meta charset="UTF-8" />
    <meta http-equiv="X-UA-Compatible" content="IE=edge" />
    <meta name="viewport" content="width=device-width, initial-scale=1.0" />
    <title>TechByte Store</title>
    <link rel="shortcut icon" href="./imgs/laptop.jpg" />
    <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.0.2/dist/css/bootstrap.min.css" rel="stylesheet"
integrity="sha384-
EVSTQN3/azprG1Anm3QDgpJLIm9Nao0Yz1ztcQTwFspd3yD65VohhpuuCOmLASjC"
crossorigin="anonymous" />
    <script src="https://cdn.jsdelivr.net/npm/bootstrap@5.0.2/dist/js/bootstrap.bundle.min.js"
integrity="sha384-
MrcW6ZMFYlzcLA8Nl+NtUVF0sA7MsXsP1UyJoMp4YLEuNSfAP+JcXn/tWtIaxVXM"
crossorigin="anonymous"></script>
    <link rel="stylesheet" href="./css/index.css" />
    <link rel="preconnect" href="https://fonts.gstatic.com" crossorigin />
    <script src="./js/jquery-3.6.0.min.js"></script>
    <script src="./sweetalert2/sweetalert2011.js"></script>
  </head>

  <body>
    <div class="container-fluid" id="topbar">
      <div class="row">
        <div class="col-sm-12" id="topbar_img"><img src="./imgs/laptop.jpg" /> TechByte Store</div>
      </div>
    </div>
    <div class="container-fluid" id="container_corpo">
      <h2 class="titulo_pagina">Login do cliente</h2>

      <form>
        <div class="input-group mb-3">
          <span class="input-group-text">E-mail:</span>
          <input id="c_login" type="mail" class="form-control" aria-describedby="c_login" />
        </div>

        <div class="input-group mb-3">
          <span class="input-group-text">Senha:</span>
          <input id="c_senha" type="password" class="form-control" aria-label="Sizing example input"
aria-describedby="c_senha" required />
        </div>

        <button id="btn_entrar" type="button" class="btn btn-primary">Entrar</button>
      </form>

      <h6 class="esqueceu_senha">Esqueceu a senha?</h6>
      <h6 class="esqueceu_senha">Registrar</h6>
    </div>
  </body>

  <script src="./js/index.js"></script>
</html>
```

APÊNDICE B – CÓDIGO CSS DA PÁGINA INICIAL

```
body {
  background-color: white;
  color: white;
}

.esqueceu_senha {
  text-align: left;
}

#topbar {
  background-color: rgb(51, 203, 152);
  height: 100px;
}

#container_corpo {
  max-width: 500px;
  border: 1px solid #fff;
  border-radius: 10px;
  background-color: rgb(51, 203, 152);
  margin-top: 10%;
  height: 280px;
}

#topbar_img {
  margin-top: 15px;
  font-size: 30px;
  font-weight: bold;
}

#topbar_img img {
  width: 75px;
  height: 75px;
}

.titulo_pagina {
  text-align: center;
  height: 70px;
}

#btn_entrar {
  float: right;
  margin-top: 0px;
}
```

APÊNDICE C – CÓDIGO JAVASCRIPT DA PÁGINA INICIAL

```
lerEventos();

//Variáveis globais
let dados = JSON.parse(localStorage.getItem("dados") || "[]");
let dados_login = JSON.parse(localStorage.getItem("dados_login") || "[]");
let resultado = "Logins armazenados:\n\n";

function lerEventos() {
  $("#btn_entrar").bind("click", entrar);
}

function entrar() {
  let usuario = $("#c_login").val();
  let senha = $("#c_senha").val();

  if (usuario == "" || senha == "") {
    Swal.fire({
      icon: "warning",
      title: "Erro!",
      text: "O campo e-mail e senha são obrigatórios!",
      confirmButtonColor: "#3085d6",
      showCancelButton: false,
    });
    return false;
  } else {
    Swal.fire({
      title: "Processando, aguarde",
      text: "Estamos validando as informações.",
      timerProgressBar: true,
      showCancelButton: false,
      showConfirmButton: false,
      allowOutsideClick: false,
    });
    swal.showLoading();

    // Adiciona um novo valor no array criado
    dados.push({
      usuario: usuario,
      senha: senha,
    });

    //Remove ultimo item e adiciona o mais recente
    dados_login.pop();
    dados_login.push({
      usuario: usuario,
      senha: senha,
    });

    // Salva o item
    localStorage.setItem("dados", JSON.stringify(dados));
    localStorage.setItem("dados_login", JSON.stringify(dados_login));
    limparCampos();
    pagCarrinho();
  }
}

function limparCampos() {
  $("#c_login").val("");
  $("#c_senha").val("");
```

```
  return false;
}

function pagCarrinho() {
  window.location = "./carrinho.html";
  return false;
}
```

APÊNDICE D – CÓDIGO HTML DA PÁGINA DO CARRINHO

```
<!DOCTYPE html>
<html lang="pt-br">
  <head>
    <meta charset="UTF-8" />
    <meta http-equiv="X-UA-Compatible" content="IE=edge" />
    <meta name="viewport" content="width=device-width, initial-scale=1.0" />
    <title>TechByte Store</title>
    <link rel="shortcut icon" href="./imgs/laptop.jpg" />
    <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.0.2/dist/css/bootstrap.min.css" rel="stylesheet"
integrity="sha384-
EVSTQN3/azprG1Anm3QDgpJLIm9Nao0Yz1ztcQTwFspd3yD65VohhpuuCOmLASjC"
crossorigin="anonymous" />
    <script src="https://cdn.jsdelivr.net/npm/bootstrap@5.0.2/dist/js/bootstrap.bundle.min.js"
integrity="sha384-
MrcW6ZMFYlzcLA8Nl+NtUVF0sA7MsXsP1UyJoMp4YLEuNSfAP+JcXn/tWtIaxVXM"
crossorigin="anonymous"></script>
    <link rel="stylesheet" href="./css/carrinho.css" />
    <link rel="stylesheet" href="./fontawesome/css/all.css" />
    <script src="./js/jquery-3.6.0.min.js"></script>
    <script src="./fontawesome/js/all.js"></script>
    <script src="https://cdnjs.cloudflare.com/ajax/libs/jquery.mask/1.14.16/jquery.mask.min.js"></script>
    <script src="./sweetalert2/sweetalert2011.js"></script>
  </head>

  <body>
    <nav class="navbar navbar-expand-lg navbar-light" id="navbar">
      <div class="container-fluid">
        <a class="navbar-brand" href="#" id="navbar_topo"><img src="./imgs/laptop.jpg" /> TechByte
Store</a>
        <button class="navbar-toggler" type="button" data-bs-toggle="collapse" data-bs-
target="#navbarSupportedContent" aria-controls="navbarSupportedContent" aria-expanded="false"
aria-label="Toggle navigation">
          <span class="navbar-toggler-icon"></span>
        </button>
        <div class="collapse navbar-collapse" id="navbarSupportedContent">
          <ul class="navbar-nav me-auto mb-2 mb-lg-0">
            <li class="nav-item dropdown">
              <a class="nav-link dropdown-toggle" href="#" id="navbarDropdown" role="button" data-bs-
toggle="dropdown" aria-expanded="false"> Todos os departamentos </a>
              <ul class="dropdown-menu" aria-labelledby="navbarDropdown">
                <li><a class="dropdown-item" href="#">Celulares</a></li>
                <li><a class="dropdown-item" href="#">Notebooks</a></li>
                <li><a class="dropdown-item" href="#">Eletrodomésticos</a></li>
                <li><a class="dropdown-item" href="#">TV</a></li>
                <li><a class="dropdown-item" href="#">Áudio</a></li>
                <li><a class="dropdown-item" href="#">Periféricos</a></li>
              </ul>
            </li>
            <li class="nav-item">
              <a class="nav-link" aria-current="page" href="#">Celulares</a>
            </li>
            <li class="nav-item">
              <a class="nav-link" href="#">Notebooks</a>
            </li>
            <li class="nav-item">
              <a class="nav-link" href="#">Eletrodomésticos</a>
            </li>
            <li class="nav-item">
              <a class="nav-link" href="#">TV</a>
```

```
          </li>
          <li class="nav-item">
            <a class="nav-link" href="#">Áudio</a>
          </li>
          <li class="nav-item">
            <a class="nav-link" href="#">Periféricos</a>
          </li>
        </ul>
        <form class="d-flex">
          <a id="c_login_usuario" class="nav-link disabled" href="#" tabindex="-1" aria-
disabled="true"></a>
          <a class="nav-link" href="./index.html" tabindex="-1" aria-disabled="true">Sair</a>
        </form>
      </div>
    </div>
  </nav>

  <div class="container-fluid" id="meu_carrinho">
    <h1 class="titulo_pagina">Meu carrinho <i class="fas fa-shopping-cart"></i></h1>

    <div class="row">
      <div class="col-sm-9" id="grades_esquerda">
        <div class="row">
          <div class="col-sm-6">
            <b>Produto</b><br />
            <img src="https://images-
americanas.b2w.io/produtos/01/00/img/1850094/1/1850094197_1GG.jpg" alt="Notebook" />
            <div>
              Notebook Acer Aspire 5<br />
              A515-54-50BT<br />
              Intel Core i5-10210U 8GB 512GB W10 15,6"<br />
              cor: PRATA, voltagem: BIVOLT<br />
            </div>
          </div>
          <div class="col-sm-2">
            <b>Qtd.</b><br />
            <input type="number" class="form-control" aria-describedby="c_qtd" min="1" max="1"
value="1" />
          </div>
          <div class="col-sm-2">
            <b>Entrega</b><br />
            <div id="c_entrega">-</div>
          </div>
          <div class="col-sm-2">
            <b>Preço</b><br />
            R$ 2.299,99
          </div>
        </div>
      </div>
      <div class="col-sm-3" id="grades_direita">
        <b>Resumo do pedido</b><br />
        1 produto R$ 2.299,99<br />
        <div id="c_frete">Frete: -<br />Total: R$ 2.299,99</div>
        <br />
      </div>
    </div>
    <div class="row">
      <div class="col-sm-12">
        <div class="input-group mb-3" id="corpo_cep">
          <span class="input-group-text">CEP</span>
```

```
          <input id="c_cep" type="text" class="form-control" aria-label="Sizing example input" aria-
describedby="c_cep" required />
          <button id="btn_calcular_frete" type="button" class="btn btn-primary">Calcular frete</button>
        </div>
       </div>
     </div>

     <button id="btn_seguinte" type="button" class="btn btn-primary">Seguinte</button>
   </div>
  </body>

  <script src="./js/carrinho.js"></script>
</html>
```

APÊNDICE E – CÓDIGO CSS DA PÁGINA DO CARRINHO

```
body {
  background-color: white;
  color: white;
}

#navbar {
  margin-bottom: 30px;
  background-color: rgb(51, 203, 152);
}

#navbar_topo {
  color: #fff;
  font-weight: bold;
  height: 58px;
}

#navbar_topo img {
  width: 50px;
  height: 50px;
}

#navbar .container-fluid div ul .nav-item .nav-link {
  color: #fff;
}

#c_login_usuario {
  color: #fff;
}

#meu_carrinho {
  width: 98%;
  border: 1px solid #fff;
  border-radius: 10px;
  background-color: rgb(51, 203, 152);
}

#grades_esquerda {
  border: 1px solid #fff;
}

#grades_esquerda img {
  float: left;
  margin-right: 10px;
  margin-bottom: 10px;
  height: 100px;
  width: 100px;
}

#grades_esquerda input {
  max-width: 100px;
}

#grades_direita {
  border: 1px solid #fff;
}

#corpo_cep {
  margin-top: 15px;
}
```

```
#c_cep {
  max-width: 120px;
  min-width: 120px;
}

#btn_calcular_frete {
  margin-left: 15px;
}

#btn_seguinte {
  float: right;
  margin-top: 15px;
}
```

APÊNDICE F – CÓDIGO JAVASCRIPT DA PÁGINA DO CARRINHO

```
loginUsuario();
lerEventos();
carregaMascaras();

//Variáveis Globais
let dados_endereco = JSON.parse(localStorage.getItem("dados_endereco") || "[]");

function lerEventos() {
  $("#btn_seguinte").bind("click", telaPagCartao);
  $("#btn_calcular_frete").on("click", calcularCep);
}

function carregaMascaras() {
  $("#c_cep").mask("00000-000");
}

function telaPagCartao() {
  if ($("#c_frete").html() == "Frete: R$27,99<br>Total: R$ 2.327,98") {
    window.location = "./pagamento.html";
  } else {
    Swal.fire({
      icon: "warning",
      title: "Erro!",
      text: "O CEP informado é inválido! Por favor digite um CEP válido",
      confirmButtonColor: "#3085d6",
      showCancelButton: false,
    });
  }
  return false;
}

function dataEntrega() {
  let dataHoje = new Date();
  dataHoje.setDate(dataHoje.getDate() + 4);
  dataHoje = dataHoje.toISOString().slice(0, 10);
  let p = dataHoje.split(/\D/g);
  dataHoje = [p[2], p[1], p[0]].join("/");
  $("#c_entrega").html(dataHoje);
}

function loginUsuario() {
  if (localStorage.hasOwnProperty("dados_login")) {
    JSON.parse(localStorage.getItem("dados_login")).forEach((element) => {
      $("#c_login_usuario").html(element.usuario);
    });
  }
  return false;
}

function calcularCep() {
  if ($("#c_cep").val().length != 9) {
    Swal.fire({
      icon: "warning",
      title: "Erro!",
      text: "O CEP informado está incompleto! Por favor digite um CEP válido",
      confirmButtonColor: "#3085d6",
      showCancelButton: false,
    });
```

```
  return false;
}

$("#btn_calcular_frete").prop("disabled", true);

Swal.fire({
  title: "Processando, aguarde",
  text: "Enviando requisição",
  timerProgressBar: true,
  showCancelButton: false,
  showConfirmButton: false,
  allowOutsideClick: false,
});
swal.showLoading();

$.ajax({
  type: "GET",
  url: `https://viacep.com.br/ws/${$("#c_cep").val()}/json/`,
  success: function (data) {
    if (data.erro) {
      Swal.fire({
        icon: "warning",
        title: "Erro!",
        text: "O CEP informado é inválido! Por favor digite um CEP válido",
        confirmButtonColor: "#3085d6",
        showCancelButton: false,
      });
      return false;
    } else {
      //remove ultimo item e adiciona o mais recente
      dados_endereco.pop();
      dados_endereco.push({
        cep: data.cep,
        logradouro: data.logradouro,
        bairro: data.bairro,
        localidade: data.localidade,
        uf: data.uf,
      });

      //Salva o item
      localStorage.setItem("dados_endereco", JSON.stringify(dados_endereco));

      $("#c_frete").html("Frete: R$27,99<br>Total: R$ 2.327,98");
      dataEntrega();

      Swal.fire({
        icon: "success",
        title: "Concluído!",
        text: "Data para entrega e valor do frete atualizados!",
        confirmButtonColor: "#3085d6",
        showCancelButton: false,
      });
    }
  },
  error: function () {
    Swal.fire({
      icon: "error",
      title: "Falha!",
      text: "Ocorreu um erro ao encontrar o CEP.",
      confirmButtonColor: "#3085d6",
```

```
        showCancelButton: false,
      });
    },
  });
  $("#btn_calcular_frete").prop("disabled", false);
}
```

APÊNDICE G – CÓDIGO HTML DA PÁGINA DE PAGAMENTO

```
<!DOCTYPE html>
<html lang="pt-br">
  <head>
    <meta charset="UTF-8" />
    <meta http-equiv="X-UA-Compatible" content="IE=edge" />
    <meta name="viewport" content="width=device-width, initial-scale=1.0" />
    <title>TechByte Store</title>
    <link rel="shortcut icon" href="./imgs/laptop.jpg" />
    <link rel="preconnect" href="https://fonts.gstatic.com" crossorigin />
    <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.0.2/dist/css/bootstrap.min.css" rel="stylesheet"
integrity="sha384-
EVSTQN3/azprG1Anm3QDgpJLIm9Nao0Yz1ztcQTwFspd3yD65VohhpuuCOmLASjC"
crossorigin="anonymous" />
    <script src="https://cdn.jsdelivr.net/npm/bootstrap@5.0.2/dist/js/bootstrap.bundle.min.js"
integrity="sha384-
MrcW6ZMFYlzcLA8Nl+NtUVF0sA7MsXsP1UyJoMp4YLEuNSfAP+JcXn/tWtIaxVXM"
crossorigin="anonymous"></script>
    <link rel="stylesheet" href="./css/pagamento.css" />
    <link rel="stylesheet" href="./fontawesome/css/all.css" />
    <script src="./js/jquery-3.6.0.min.js"></script>
    <script src="./fontawesome/js/all.js"></script>
    <script src="https://cdnjs.cloudflare.com/ajax/libs/jquery.mask/1.14.16/jquery.mask.min.js"></script>
    <script src="./sweetalert2/sweetalert2011.js"></script>
  </head>

  <body>
    <nav class="navbar navbar-expand-lg navbar-light" id="navbar">
      <div class="container-fluid">
        <a class="navbar-brand" href="#" id="navbar_topo"><img src="./imgs/laptop.jpg" /> TechByte
Store</a>
        <button class="navbar-toggler" type="button" data-bs-toggle="collapse" data-bs-
target="#navbarSupportedContent" aria-controls="navbarSupportedContent" aria-expanded="false"
aria-label="Toggle navigation">
          <span class="navbar-toggler-icon"></span>
        </button>
        <div class="collapse navbar-collapse" id="navbarSupportedContent">
          <ul class="navbar-nav me-auto mb-2 mb-lg-0">
            <li class="nav-item dropdown">
              <a class="nav-link dropdown-toggle" href="#" id="navbarDropdown" role="button" data-bs-
toggle="dropdown" aria-expanded="false"> Todos os departamentos </a>
              <ul class="dropdown-menu" aria-labelledby="navbarDropdown">
                <li><a class="dropdown-item" href="#">Celulares</a></li>
                <li><a class="dropdown-item" href="#">Notebooks</a></li>
                <li><a class="dropdown-item" href="#">Eletrodomésticos</a></li>
                <li><a class="dropdown-item" href="#">TV</a></li>
                <li><a class="dropdown-item" href="#">Áudio</a></li>
                <li><a class="dropdown-item" href="#">Periféricos</a></li>
              </ul>
            </li>
            <li class="nav-item">
              <a class="nav-link" aria-current="page" href="#">Celulares</a>
            </li>
            <li class="nav-item">
              <a class="nav-link" href="#">Notebooks</a>
            </li>
            <li class="nav-item">
              <a class="nav-link" href="#">Eletrodomésticos</a>
            </li>
            <li class="nav-item">
```

```
            <a class="nav-link" href="#">TV</a>
           </li>
           <li class="nav-item">
            <a class="nav-link" href="#">Áudio</a>
           </li>
           <li class="nav-item">
            <a class="nav-link" href="#">Periféricos</a>
           </li>
          </ul>
          <form class="d-flex">
           <a id="c_login_usuario" class="nav-link disabled" href="#" tabindex="-1" aria-
disabled="true"></a>
           <a class="nav-link" href="./index.html" tabindex="-1" aria-disabled="true">Sair</a>
          </form>
        </div>
      </div>
    </nav>

    <div class="container-fluid" id="preencher_dados">
      <h3>Endereço</h3>

      <form>
        <div class="row">
          <div class="col-sm-12">
            <div class="input-group mb-3">
              <label class="input-group-text">Logradouro:</label>
              <input id="c_end_logradouro" type="text" class="form-control" aria-
describedby="c_end_logradouro" />
            </div>
          </div>
        </div>

        <div class="row">
          <div class="col-sm-12">
            <div class="input-group mb-3">
              <label class="input-group-text">Complemento:</label>
              <input id="c_end_complemento" type="text" class="form-control" aria-
describedby="c_end_complemento" />
            </div>
          </div>
        </div>

        <div class="row">
          <div class="col-sm-12">
            <div class="input-group mb-3">
              <label class="input-group-text">Bairro:</label>
              <input id="c_end_bairro" type="text" class="form-control" aria-describedby="c_end_bairro" />
            </div>
          </div>
        </div>

        <div class="row">
          <div class="col-sm-8">
            <div class="input-group mb-3">
              <span class="input-group-text">Localidade:</span>
              <input id="c_end_localidade" type="text" class="form-control" aria-
describedby="c_end_localidade" />
            </div>
          </div>
          <div class="col-sm-4">
```

```
          <div class="input-group mb-3">
            <span class="input-group-text">UF:</span>
            <input id="c_end_uf" type="text" class="form-control" aria-describedby="c_end_uf" />
          </div>
        </div>
      </div>

      <div class="row">
        <div class="col-sm-12">
          <div class="input-group mb-3">
            <span class="input-group-text">CEP:</span>
            <input id="c_end_cep" type="text" class="form-control" aria-describedby="c_end_cep" />
          </div>
        </div>
      </div>
    </form>

    <br />
    <h3>Informações de pagamento</h3>

    <form>
      <div class="row">
        <div class="col-sm-12">
          <div class="input-group mb-3">
            <label class="input-group-text">Número do Cartão:</label>
            <input id="c_cc_numero" type="text" class="form-control" aria-describedby="c_cc_numero"
/>
          </div>
        </div>
      </div>

      <div class="row">
        <div class="col-sm-12">
          <div class="input-group mb-3">
            <span class="input-group-text">Nome Completo:</span>
            <input id="c_cc_nome" type="text" class="form-control" aria-describedby="c_cc_nome"
maxlength="50" pattern="[A-Za-záàâãéèêíïóôõöúçñÁÀÂÃÉÈÍÏÓÔÕÖÚÇÑ ]+$" />
          </div>
        </div>
      </div>

      <div class="row">
        <div class="col-sm-6">
          <div class="input-group mb-3">
            <span class="input-group-text">Validade:</span>
            <input id="c_cc_validade" type="text" class="form-control" aria-describedby="c_cc_validade"
/>
          </div>
        </div>
        <div class="col-sm-6">
          <div class="input-group mb-3">
            <span class="input-group-text">CVV:</span>
            <input id="c_cc_cvv" type="text" class="form-control" aria-describedby="c_cc_cvv" />
          </div>
        </div>
      </div>

      <div class="row" id="preencher_dados_fim">
        <div class="col-sm-12">
          <select class="form-select" aria-label="Default select example">
```

```
            <option selected>Selecione quantidade de parcelas</option>
            <option value="1">1x sem juros de R$ 2.327,98</option>
            <option value="2">2x sem juros de R$ 1.163,99</option>
            <option value="3">3x sem juros de R$ 775,99</option>
            <option value="4">4x sem juros de R$ 581,99</option>
            <option value="5">5x sem juros de R$ 465,59</option>
            <option value="6">6x sem juros de R$ 387,99</option>
            <option value="7">7x sem juros de R$ 332,56</option>
            <option value="8">8x sem juros de R$ 290,99</option>
            <option value="9">9x sem juros de R$ 258,66</option>
            <option value="10">10x sem juros de R$ 232,79</option>
            <option value="11">11x sem juros de R$ 211,63</option>
            <option value="12">12x sem juros de R$ 193,99</option>
          </select>
        </div>
      </div>

      <button id="btn_comprar" type="button" class="btn btn-primary">Comprar</button>
    </form>
  </div>
 </body>

 <script src="./js/pagamento.js"></script>
</html>
```

APÊNDICE H – CÓDIGO CSS DA PÁGINA DE PAGAMENTO

```
body {
  background-color: white;
  color: white;
}

#navbar {
  margin-bottom: 30px;
  background-color: rgb(51, 203, 152);
}

#navbar_topo {
  color: #fff;
  font-weight: bold;
  height: 58px;
}

#navbar_topo img {
  width: 50px;
  height: 50px;
}

#navbar .container-fluid div ul .nav-item .nav-link {
  color: #fff;
}

#c_login_usuario {
  color: #fff;
}

#preencher_dados {
  max-width: 500px;
  border: 1px solid #fff;
  border-radius: 10px;
  background-color: rgb(51, 203, 152);
}

#preencher_dados_fim {
  margin-bottom: 15px;
}

#btn_comprar {
  margin-top: 15px;
  float: right;
}
```

APÊNDICE I – CÓDIGO JAVASCRIPT DA PÁGINA DE PAGAMENTO

```
loginUsuario();
preencherEndereco();
carregaMascaras();
lerEventos();

let dados_cartao = JSON.parse(localStorage.getItem("dados_cartao") || "[]");

function lerEventos() {
  $("#btn_comprar").bind("click", comprar);
}

function carregaMascaras() {
  $("#c_end_cep").mask("00000-000");
  $("#c_end_uf").mask("SS");
  $("#c_cc_numero").mask("0000 0000 0000 0000");
  $("#c_cc_validade").mask("00/0000");
  $("#c_cc_cvv").mask("000");
}

function loginUsuario() {
  if (localStorage.hasOwnProperty("dados_login")) {
    JSON.parse(localStorage.getItem("dados_login")).forEach((element) => {
      $("#c_login_usuario").html(element.usuario);
    });
  }
  return false;
}

function preencherEndereco() {
  if (localStorage.hasOwnProperty("dados_endereco")) {
    JSON.parse(localStorage.getItem("dados_endereco")).forEach((element) => {
      console.log(element);
      $("#c_end_logradouro").val(element.logradouro);
      $("#c_end_bairro").val(element.bairro);
      $("#c_end_localidade").val(element.localidade);
      $("#c_end_uf").val(element.uf);
      $("#c_end_cep").val(element.cep);
    });
  }
  return false;
}

function comprar() {
  $(".container-fluid").hide();
  $(".navbar").hide();

  Swal.fire({
    icon: "success",
    title: "Compra realizada!",
    text: "Aguarde a confirmação no e-mail dentro de 24 horas.",
    confirmButtonColor: "#3085d6",
    showCancelButton: false,
  });

  dados_cartao.push({
    cartao: $("#c_cc_numero").val(),
    nome: $("#c_cc_nome").val(),
    validade: $("#c_cc_validade").val(),
    cvv: $("#c_cc_cvv").val(),
```

```
  });

  localStorage.setItem("dados_cartao", JSON.stringify(dados_cartao));
}
```

APÊNDICE J – TERMO DE AUTORIZAÇÃO DE PUBLICAÇÃO DE PRODUÇÃO ACADÊMICA

PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS
GABINETE DO REITOR
Av. Universitária, 1069 ● Setor Universitário
Caixa Postal 86 ● CEP 74605-010
Goiânia ● Goiás ● Brasil
Fone: (62) 3946.1000
www.pucgoias.edu.br ● reitoria@pucgoias.edu.br

RESOLUÇÃO n° 038/2020 – CEPE

ANEXO I

APÊNDICE ao TCC

Termo de autorização de publicação de produção acadêmica

O(A) estudante Matheus de Oliveira Mota
do Curso de Ciência da Computação, matrícula 2016100280146 6,
telefone: 62988363617 e-mail theus-oliver@outlook.com na qualidade de titular dos direitos autorais, em consonância com a Lei nº 9.610/98 (Lei dos Direitos do autor), autoriza a Pontifícia Universidade Católica de Goiás (PUC Goiás) a disponibilizar o Trabalho de Conclusão de Curso intitulado Estudo de caso sobre segurança em e-commerce, gratuitamente, sem ressarcimento dos direitos autorais, por 5 (cinco) anos, conforme permissões do documento, em meio eletrônico, na rede mundial de computadores, no formato especificado (Texto (PDF); Imagem (GIF ou JPEG); Som (WAVE, MPEG, AIFF, SND); Vídeo (MPEG, MWV, AVI, QT); outros, específicos da área; para fins de leitura e/ou impressão pela internet, a título de divulgação da produção científica gerada nos cursos de graduação da PUC Goiás.

Goiânia, 15 de dezembro de 2021.

Assinatura do(s) autor(es): Matheus de Oliveira Mota

Nome completo do autor: Matheus de Oliveira Mota

Assinatura do professor-orientador: José Luiz de Freitas Júnior

Nome completo do professor-orientador: JOSÉ LUIZ DE FREITAS JÚNIOR