O EFEITO PLACEBO DA SEGURANÇA DAS INFORMAÇÕES NA INTERNET

Rafael de Oliveira Domenegueti[1]

Alexandre Gomes da Silva[2]

Resumo

A crescente utilização da internet é fato incontestável, tendo as mais variadas consequências para a sociedade e introduzindo uma série de consequências novas para as relações. Este artigo tem como objetivo descrever o conceito de efeito placebo aplicado no contexto digital, apresentando recomendações e boas práticas para garantir a segurança na navegação na internet e proteção de dados pessoais. A justificativa para este estudo é a crescente preocupação dos usuários na internet com a privacidade e segurança, especialmente após casos de vazamento de dados pessoais de grandes empresas. Como metodologia utilizada foram aplicadas pesquisas de natureza exploratória, para identificar o efeito placebo e temas correlatos com segurança de dados, ataques cibernéticos, tipificando os principais mecanismo usados, além de apresentar competências essenciais relacionadas à segurança e privacidade digital de usuários na internet. Os resultados indicam a necessidade de adotar precauções significativas para garantir a navegação segura, como por exemplo, a utilização de senhas robustas e complexas. Além disso, empresas têm demonstrado uma crescente preocupação em assegurar que seus softwares sejam de fácil compreensão, mesmo para usuários com menor familiaridade técnica. Torna-se fundamental que usuários nas redes estejam cientes dos riscos existentes e adotem medidas de segurança para proteger seus dados pessoais na internet.

Palavras-chave: Boas práticas. Navegação segura. Proteção de dados. Segurança.

Abstract

The growing utilization of the internet is an undeniable fact, with varied consequences for society and introducing a series of new implications for relationships. This article aims at describing the concept of the placebo effect as applied in the digital context, providing recommendations and best practices to ensure safe browsing and the protection of personal data. The justification for this study lies in the increasing concern of internet users regarding privacy and security, particularly in the aftermath of major data breaches involving personal information from prominent companies. Exploratory research methodologies were employed to identify the placebo effect and topics related to data security, cyber attacks, typifying key mechanisms used, and presenting essential competencies related to the digital security and privacy of internet users. The results indicate the imperative need to

[1] Graduando em Análise e Desenvolvimento de Sistemas pela Fatec Dr. Thomaz Novelino – Franca/SP. Endereço eletrônico: rafaeldomenegueti627@gmail.com.

[2] Professor Esp. Fatec Dr. Thomaz Novelino – Franca/SP. Endereço eletrônico: alexandre.silva251@fatec.sp.gov.br

adopt significant precautions to ensure safe browsing, such as the use of robust and complex passwords. Furthermore, companies have shown a growing commitment to ensure that their software is user-friendly, even for individuals with limited technical familiarity. It is crucial for users on networks to be aware of existing risks and to implement security measures to protect their personal data on the internet.

Keywords: *Data protection. Good practices. Safe browsing. Security.*

1 Introdução

A crescente utilização da internet tem proporcionado inúmeras facilidades e benefícios para a sociedade, mas também tem gerado preocupações em relação à segurança e privacidade dos usuários. Com o aumento de casos de vazamento de dados pessoais de grandes empresas, torna-se cada vez mais importante adotar medidas de segurança para garantir uma navegação segura na internet. Contudo, essa transformação também introduziu novas complexidades, sendo que a velocidade acelerada das inovações tornou a tarefa de acompanhar as últimas tecnologias um desafio substancial, particularmente para indivíduos carentes de um domínio especializado neste domínio.

Empresas têm demonstrado uma crescente preocupação em assegurar que seus softwares sejam de fácil compreensão, mesmo para usuários com menor familiaridade técnica. Esse esforço busca instilar uma percepção de segurança e comodidade dos usuários, ainda que muitas vezes inadvertidamente essas organizações estejam adquirindo informações sensíveis, tais como CPF, endereço de e-mail e, possivelmente, senhas potencialmente empregadas em outras plataformas.

No mês de junho de 2012, a rede social LinkedIn foi alvo de uma invasão cibernética que resultou na exposição de senhas pertencentes a mais de 167 milhões de usuários. Superando até mesmo o vazamento da Adobe de 2013 que expôs 152 milhões de senhas.

No mês de agosto de 2022, a Secretaria Nacional do Consumidor (SENACON) em nosso país, emitiu uma penalidade financeira no valor de 6,6 milhões de reais à empresa Meta, controladora do Facebook. Esta ação foi tomada em decorrência da constatação de práticas ilícitas de compartilhamento de informações, ocorridas no âmbito do teste de personalidade intitulado "*This Is Your Digital Life*" (tradução livre: “Esta é sua Vida Digital”).

Nesse contexto, o objetivo do presente trabalho trata de descrever o conceito de efeito placebo aplicado no contexto digital, apresentando recomendações e boas práticas para garantir a segurança na navegação na internet e proteção de dados pessoais.

Para tanto, torna-se necessário explicar como as corporações propagam uma sensação ilusória de segurança entre seus usuários, ocultando frequentemente a ocorrência de vazamentos de dados, mesmo entre as entidades de grande porte. A constatação desses dados por hackers frequentemente ocorre sem o conhecimento do proprietário dos dados em questão.

A metodologia utilizada envolveu pesquisas de natureza exploratória, para identificar o efeito placebo e temas correlatos com segurança de dados, ataques cibernéticos, tipificando os principais mecanismo usados, além de apresentar competências essenciais relacionadas à segurança e privacidade digital de usuários na internet.

Além disso, foram estabelecidas recomendações relevantes, destinadas a preservar a segurança das informações pessoais, bem como indicação de futuros estudos levantando informações sobre novos métodos de segurança, para informar a comunidade sobre novas formas de proteção no ambiente virtual.

2 Efeito placebo na segurança online

Nesta seção, aprofundaremos nossa compreensão do fenômeno conhecido como "efeito placebo" e exploraremos sua aplicação no contexto crucial da segurança online, destacando a relevância desse conceito no ambiente digital.

2.1 Definição do efeito placebo

A expressão "efeito placebo" refere-se a uma substância que, em si mesma, não possui ação farmacológica (Trounce, 1977), sendo um termo amplamente empregado na medicina para descrever medicamentos que carecem de eficácia farmacológica em seus usuários.

Embora seja comumente associado ao impacto psicológico, acredita-se agora que o efeito placebo transcende a esfera puramente mental. Conforme observado por Henry K. Beecher em sua obra intitulada "*The Powerful Placebo*" (tradução livre:

"O Poderoso Placebo" 1955), aproximadamente 35% dos pacientes envolvidos em 15 ensaios clínicos abordando diversas doenças experimentaram uma melhora considerável no alívio da dor após a administração de placebos (Bastos; Kirsztajn, 2011).

2.2 Aplicação no contexto da segurança na internet

No cenário cada vez mais interconectado da era digital, a aplicação do "efeito placebo" transcende as fronteiras da medicina e emerge como um conceito relevante no âmbito da segurança online. Para os usuários que não possuem conhecimento técnico ou acesso ao código fonte dos sistemas e aplicativos que utilizam, a sensação de segurança é predominantemente mediada pela interface gráfica e pela experiência de uso.

Conforme evidenciado em estudos como o artigo intitulado "*Consumer perception of interface quality, security, and loyalty in electronic commerce*" (Chang; Chen, 2009), a segurança na internet não se limita à implementação técnica de protocolos e medidas de proteção. Ela engloba, a percepção do cliente em relação à segurança global da transação, abrangendo aspectos como os métodos de pagamento, os mecanismos de armazenamento e transmissão de informações pessoais, bem como a integridade das plataformas e serviços online.

Nesse contexto, os usuários se guiam pela interface gráfica e na aparente confiabilidade de um aplicativo ou serviço. O "efeito placebo" na segurança online sugere que a percepção de segurança pode ser influenciada pela apresentação visual, pela usabilidade e pela reputação percebida, tornando a compreensão desse fenômeno crucial para abordar questões críticas de confiança e proteção de dados na era digital.

3 Fundamentos da segurança na internet

Nesta seção, abordaremos a compreensão dos fundamentos da segurança cibernética e as principais ameaças e riscos.

3.1 Fundamentos da segurança cibernética

Segundo o site Bughunt (Bughunt, 2021), os princípios da segurança da informação são:

> • Confidencialidade: é o que garante o acesso das informações apenas às pessoas autorizadas, ou seja, não disponibiliza esse acesso a indivíduos, entidades ou processos não autorizados.
> • Integridade: é o que garante a veracidade das informações, indicando que os dados não podem ser alterados sem autorização.
> • Disponibilidade: é o que garante que os dados e sistemas estejam disponíveis para pessoas autorizadas quando se tornar necessário.
> • Autenticidade: é o que garante a verdadeira autoria da informação, ou seja, que os dados são de fato provenientes de determinada fonte.

A figura 1 mostra uma pessoa inserindo um cartão de crédito em um caixa eletrônico. Esta é uma situação comum na vida cotidiana, mas que também pode representar um risco à segurança cibernética. Os caixas eletrônicos são alvos frequentes de ataques cibernéticos. Os criminosos podem usar técnicas para roubar informações pessoais e financeiras das vítimas.

Figura 1 – Segurança cibernética

Fonte: Página do Estadão e.Investidor (Rocha, 2023)

4 Tipos de ataques cibernéticos e seus efeitos

Os ataques cibernéticos são ações maliciosas executadas por indivíduos ou grupos com o propósito de comprometer sistemas, redes ou dispositivos de computador (Baker, 2023).

Esses ataques manifestam-se em diversas formas, cada uma com suas próprias características e repercussões. A seguir, alguns dos principais tipos de ataques cibernéticos e os impactos que provocam.

4.1 Phishing

O phishing consiste na técnica em que os perpetradores enviam comunicações eletrônicas fraudulentas, tais como emails ou mensagens de texto, que aparentam ser originárias de fontes confiáveis, como instituições bancárias ou empresas legítimas. Essas mensagens frequentemente contêm links maliciosos ou solicitam informações pessoais, como senhas e números de cartão de crédito (Baker, 2023).

O phishing pode resultar no roubo de informações confidenciais, incluindo credenciais de acesso e dados financeiros. As vítimas podem ser induzidas a realizar ações prejudiciais, como a transferência de fundos para contas controladas pelos atacantes.

4.2 Malware

Malware é uma designação ampla englobando diversos tipos de software malicioso, como vírus, worms, trojans e spyware. Esses programas são concebidos para infiltrar-se em sistemas e executar operações nocivas sem o consentimento do usuário (Baker, 2023).

Os efeitos do malware podem variar, mas geralmente incluem a coleta de informações confidenciais, a destruição de dados, o roubo de recursos do sistema e a disseminação para outros dispositivos.

4.3 Spoofing

O spoofing é uma técnica de ataque cibernético que se concentra na falsificação ou mascaramento de informações para induzir em erro sistemas, redes ou indivíduos, criando uma aparência de autenticidade enganosa. O termo "spoofing" deriva da palavra em inglês "spoof," que significa falsificação ou imitação. Essa estratégia pode ser aplicada de diversas formas, cada uma visando atingir um objetivo específico (Baker, 2023).

Os ataques de spoofing podem ter sérios impactos, abrangendo desde o comprometimento de sistemas críticos e o roubo de informações sensíveis até a disseminação de malware e a manipulação de comunicações.

A falsificação de identidade e a ocultação de dados podem induzir ações prejudiciais por parte das vítimas, comprometendo a confiabilidade das informações e expondo indivíduos e organizações a riscos significativos de segurança cibernética.

4.4 Ataques de negativa de serviço (DDoS)

Os ataques de negativa de serviço (DDoS) sobrecarregam um sistema, servidor ou rede com um volume excessivo de tráfego, tornando-o inacessível para usuários legítimos (Baker, 2023).

Os efeitos dos ataques DDoS abrangem a interrupção de serviços online, o tempo de inatividade, a perda de receita e a deterioração da reputação da empresa ou organização alvo. Tais ataques podem ser empregados como distrações para outros ataques cibernéticos de maior gravidade.

5 Percepção de segurança online

A avaliação da segurança em um ambiente online é encapsulada pelo conceito de "segurança percebida", que denota a percepção de segurança que um usuário experimenta ao utilizar um serviço online. Nesta seção, discutiremos como essa percepção é moldada (Chang; Chen, 2009).

5.1 Como as pessoas percebem e avaliam sua segurança ao utilizar a internet

A partir da perspectiva da psicologia ambiental (Chang; Chen, 2009), o ambiente físico provoca respostas cognitivas que influenciam a percepção das pessoas em relação ao local e às pessoas presentes. No entanto, no contexto online, essa "atmosfera" é substituída pela interface digital. Portanto, uma interface que seja esteticamente agradável e bem-organizada gera uma sensação de conforto e confiança no usuário.

De acordo com a teoria da Inferência (Baker et al., 2002), as ideias são formadas sobre o desconhecido com base em informações preexistentes.

Em outras palavras, quando não se tem acesso a todas as informações necessárias, as pessoas formulam julgamentos com base no que podem observar. Consequentemente, uma plataforma que apresenta um excesso de informações na tela pode criar uma falsa percepção de desordem no sistema.

5.2 Fatores que contribuem para a sensação de segurança ou insegurança

Vários fatores contribuem para a criação de uma sensação positiva de segurança por parte dos usuários. Estes incluem conveniência (facilidade de navegação), interatividade (facilidade de comunicação bidirecional com os clientes), personalização (capacidade de adaptação às preferências individuais dos clientes) e identidade visual (a imagem geral adquirida por meio de elementos como ferramentas, fontes, gráficos, cores e padrões, Chang; Chen, 2009).

Desta forma, um site que atenda a esses requisitos pode ser considerado "confortável" para os usuários, promovendo a lealdade e a percepção de segurança.

No caso de um site que não cumpra esses critérios, os usuários podem não ter uma percepção positiva da plataforma. Por exemplo, se um site apresenta botões com design completamente díspar ou cores que não estão em harmonia, os usuários podem perceber inconsistência e, como resultado, sentir uma falta de segurança em relação ao sistema.

6 Consequências do efeito placebo na internet

No contexto da escassez de informações disponíveis para os utilizadores, estes se encontram em uma posição vulnerável, sobretudo no que concerne à segurança na Internet. Esta vulnerabilidade se evidencia através de casos notáveis envolvendo empresas de renome, como o LinkedIn (Rohr, 2016) e o Facebook (G1, 2022), que tiveram a exposição de dados de seus clientes como resultado de brechas na segurança.

Nestas circunstâncias, os utilizadores que confiaram seus dados pessoais a essas plataformas enfrentam o risco iminente de terem suas informações expostas, tornando-se alvos mais acessíveis para indivíduos mal-intencionados que empregam técnicas de invasão para atingir seus objetivos.

Portanto, é evidente que a ocorrência de um incidente como a exposição de dados pode transformar um utilizador em um alvo suscetível a ataques.

É importante notar que muitos desses utilizadores, particularmente aqueles que carecem de conhecimentos especializados em tecnologia, frequentemente permanecem alheios a esses ataques. Mesmo quando têm conhecimento das violações de segurança, muitos não compreendem completamente a gravidade da situação nem sabem como agir diante dela.

7 Recomendações e boas práticas

A utilização da internet, à primeira vista, pode parecer uma vasta terra sem lei. Entretanto, uma análise mais aprofundada revela a necessidade de adotar precauções significativas a fim de garantir uma navegação segura. Nesta seção, discutiremos como maximizar a experiência na internet sem comprometer a segurança de nossos dados.

7.1 Senhas

A segurança da navegação na internet depende, em grande medida, da robustez e complexidade das senhas empregadas. As senhas desempenham um papel crucial ao garantir que o acesso seja restrito ao seu proprietário legítimo, protegendo, assim, a confidencialidade e a integridade dos dados (Bughunt, 2021).

No contexto de ataques de força bruta, nos quais diversas combinações de possíveis senhas são testadas consecutivamente, as senhas que possuem uma diversidade limitada de caracteres especiais revelam-se vulneráveis e suscetíveis a violações.

Uma estratégia eficaz na criação de senhas envolve a utilização de diversos tipos de caracteres especiais, como demonstrado no exemplo "Exemplo@123". Ao adotar esse enfoque, combina-se letras maiúsculas e minúsculas, números e caracteres especiais. Considerando uma senha composta por 8 caracteres e uma gama de 93 caracteres possíveis, a análise combinatória revela um total de 5.595.818.096.650.401 possibilidades de senhas, sendo a senha em questão apenas uma entre tantas (Matthews, 2023)

Figura 2 – Complexidade de senhas

Número de caracteres	Apenas números	Letras em caixa baixa	Letras em caixa alta e baixa	Números, letras em caixa alta e baixa	Números, letras em caixa alta e baixa, símbolos
4	Instantâneo	Instantâneo	Instantâneo	Instantâneo	Instantâneo
5	Instantâneo	Instantâneo	Instantâneo	Instantâneo	Instantâneo
6	Instantâneo	Instantâneo	Instantâneo	Instantâneo	Instantâneo
7	Instantâneo	Instantâneo	2 segundos	7 segundos	31 segundos
8	Instantâneo	Instantâneo	2 minutos	7 minutos	39 minutos
9	Instantâneo	10 segundos	1 hora	7 horas	2 dias
10	Instantâneo	4 minutos	3 dias	3 semanas	5 meses
11	Instantâneo	2 horas	5 meses	3 anos	34 anos
12	2 segundos	2 dias	24 anos	200 anos	3 mil anos
13	19 segundos	2 meses	1000 anos	12 mil anos	202 mil anos
14	3 minutos	4 anos	64 mil anos	750 mil anos	16 milhões de anos
15	32 minutos	100 anos	3 milhões de anos	46 milhões de anos	1 bilhão de anos
16	5 horas	3 mil anos	173 milhões de anos	3 bilhões de anos	92 bilhões de anos
17	2 dias	69 mil anos	9 bilhões de anos	179 bilhões de anos	7 trilhões de anos
18	3 semanas	2 mil anos	467 bilhões de anos	11 trilhões de anos	438 trilhões de anos

Fonte: Página da Hostgator (Pires, 2023).

Atualmente, existem programas desenvolvidos com o propósito de gerenciar senhas, armazenando-as de forma segura. No entanto, é importante destacar que esses aplicativos também estão sujeitos a possíveis comprometimentos de segurança.

Para mitigar esse risco, uma prática recomendada é incorporar uma sequência de caracteres confidenciais, conhecida apenas pelo usuário, ao final da senha gerada pelo programa. Por exemplo, caso o programa gere a senha "/123#JDdsaSa", pode-se adicionar uma "tag" confidencial, resultando em "/123#JDdsaSa-TAG_SUPER_SECRETA".

7.2 Navegação segura

É fundamental compreender que a manutenção da segurança na internet requer a adoção de medidas para evitar exposições desnecessárias a riscos. A

utilização de sites confiáveis e a divulgação apenas das informações estritamente necessárias constituem práticas prudentes. É importante enfatizar que nenhum site confiável solicitará senhas de terceiros (Harán, 2021).

Além disso, deve-se estar preparado para lidar com possíveis incidentes de vazamento de dados, uma vez que nenhum sistema é completamente imune a ameaças. Para minimizar os danos em caso de violação, é aconselhável utilizar senhas diferentes para cada serviço, criando assim um eficaz sistema de controle de danos.

7.3 Instalação de aplicativos

Ao instalar aplicativos, é recomendável sempre optar por fontes confiáveis. Isso implica em baixar aplicativos diretamente dos sites oficiais dos desenvolvedores ou das lojas de aplicativos de plataformas reconhecidas, como Google Play, Apple Store ou Microsoft Store (Aver, 2021).

8 Educação e conscientização sobre segurança online

A discussão em torno da prevenção no uso da internet tem ganhado destaque nos últimos anos, frequentemente associada às preocupações relacionadas a invasões e vazamentos de dados. Em resposta a essas preocupações, foi promulgada a Lei Geral de Proteção de Dados, 13.709, (Brasil, 2018), com o objetivo de salvaguardar os direitos dos usuários e estabelecer um arcabouço legal sólido para a proteção de dados pessoais (Cert.br, 2023).

Com o intuito de promover a conscientização e sensibilização acerca dos riscos presentes na internet, em 2017 teve início um projeto de extensão no Instituto de Computação da Universidade Federal de Mato Grosso (UFMT), intitulado "Cartilha de Segurança e Privacidade Digital" (Cert.br, 2023).

O projeto teve como principal propósito servir como um veículo informativo sobre os riscos relacionados à segurança e à privacidade digital dos usuários da Internet. Simultaneamente, buscou-se traçar um perfil simplificado do comportamento desses usuários na UFMT em relação a algumas competências essenciais relacionadas à segurança e privacidade digital, tais como a compreensão

dos termos de uso e políticas de privacidade, a prática de troca regular de senhas e o comportamento seguro na Web.

Considerações Finais

Com o aumento significativo de incidentes envolvendo a exposição de informações pessoais de usuários na era digital, torna-se imprescindível que todos os indivíduos que fazem uso da internet e de serviços prestados por terceiros compreendam profundamente a maneira pela qual os criminosos atuam, as ferramentas e técnicas que empregam, bem como as estratégias eficazes de proteção.

O presente estudo tem como propósito principal apresentar o conceito de efeito placebo associado com a segurança na internet e conscientizar os usuários sobre os perigos inerentes à utilização das redes e, igualmente importante, oferecer orientações concretas sobre como preservar sua segurança nesse ambiente virtual em constante evolução.

A pesquisa em questão baseou-se na análise aprofundada de diversos casos de violações de segurança e exploração de dados, com o intuito de fornecer uma base sólida de informações e diretrizes para a promoção de uma experiência mais segura na internet.

O aumento significativo de incidentes envolvendo a exposição de informações pessoais de usuários na era digital torna imprescindível que sejam desenvolvidos novos trabalhos para melhorar a segurança da internet.

Um dos principais objetivos desses trabalhos é atualizar as informações e diretrizes de segurança. As formas de ameaças aos usuários estão em constante mudança. É importante que os usuários estejam sempre informados sobre as últimas informações e diretrizes de segurança, para que possam tomar medidas para proteger suas informações pessoais.

Trabalhos futuros podem investigar novos métodos de segurança, para informar a comunidade sobre novas formas de proteção. A pesquisa em questão demonstrou casos de violações de segurança que ocorreram no passado. Novos métodos de segurança se tornam necessários para prevenir futuras violações.

Por fim, é importante avaliar a eficácia das medidas de segurança que são atualmente usadas. Isso poderá ser feito por meio de futuras pesquisas empíricas ou de simulações de ataques.

Referências

AVER, H. **Por que você deve evitar aplicativos desconhecidos**. Disponível em: <https://www.kaspersky.com.br/blog/unknown-apps-android/18082/>. Acesso em: 9 out. 2023.

BAKER, K. **Most Common Types of Cyber Attacks Today | CrowdStrike**. 13 Fevereiro 2023. Disponível em: <https://www.crowdstrike.com/cybersecurity-101/cyberattacks/most-common-types-of-cyberattacks/>. Acesso em: 9 out. 2023.

BASTOS, M. G.; KIRSZTAJN, G. M. Doença renal crônica: importância do diagnóstico precoce, encaminhamento imediato e abordagem interdisciplinar estruturada para melhora do desfecho em pacientes ainda não submetidos à diálise. **Brazilian Journal of Nephrology**, p. 33(1), 27 jan. 2011.

BEECHER, H. K. (1955). **The powerful placebo.** The Journal of the American Medical Association, 159(17), 1602-1606.

BRASIL. **LGPD - Lei Geral de Proteção de Dados Pessoais | Serpro**. 2018. Disponível em: <https://www.serpro.gov.br/lgpd>. Acesso em: 9 out. 2023.

BUGHUNT. **Quais são os 4 princípios da segurança da informação?** 13 out 2021. Disponível em: <https://blog.bughunt.com.br/principios-da-seguranca-da-informacao/>.

CERT.BR. **Cartilha de Segurança para Internet**. Disponível em: <https://cartilha.cert.br/>. Acesso em: 7 out. 2023.

CHANG, H.; CHEN, S. Consumer perception of interface quality, security, and loyalty in electronic commerce. **Information & Management**, out. 2009.

G1 GLOBO**. Facebook é multado em R$ 6,6 milhões por vazamento de dados de brasileiros em 2018**. Grupo Globo, 2022. Disponível em: <https://g1.globo.com/tecnologia/noticia/2022/08/23/facebook-e-multado-em-r-66-milhoes-por-vazamento-de-dados-de-brasileiros-em-2018.ghtml>. Acesso em: 9 out. 2023.

HARÁN, J. M. **10 regras básicas de segurança para navegar na internet**. Disponível em: <https://www.welivesecurity.com/br/2021/12/01/10-regras-basicas-de-seguranca-para-navegar-na-internet/>. Acesso em: 9 out. 2023.

MATTHEWS, R. **Senhas fortes: dicas, exemplos e como gerenciá-las**. Disponível em: <https://nordvpn.com/pt-br/blog/senhas-fortes/>. Acesso em: 11 out. 2023.

Objetivo e abrangência — Lei Geral de Proteção de Dados. Disponível em: <https://www.mpf.mp.br/servicos/lgpd/o-que-e-a-lgpd/objetivo-e-abrangencia>.

PIRES, J. **7 dicas que irão ajudar a proteger seu site WordPress de malwares**. Disponível em: <https://www.hostgator.com.br/blog/7-dicas-que-irao-ajudar-a-proteger-seu-site-wordpress-de-malwares/>. Acesso em: 9 out. 2023.

ROCHA, B. **Como sacar dinheiro do Nubank no caixa eletrônico?** Disponível em: <https://einvestidor.estadao.com.br/educacao-financeira/como-sacar-dinheiro-do-nubank-no-caixa-eletronico/>. Acesso em: 9 out. 2023.

ROHR, A. **Vazamento do LinkedIn ressurge com 167 milhões de senhas | G1 - Tecnologia e Games**. Disponível em: <https://g1.globo.com/tecnologia/blog/seguranca-digital/post/vazamento-do-linkedin-ressurge-com-167-milhoes-de-senhas.html>. Acesso em: 9 out. 2023.

TROUNCE, J. R. PHARMACOLOGY: **The Basis of Therapeutics**. 5th ed. Edinburgh: Churchill Livingstone, 1977.