ANÁLISE DA EFICÁCIA DOS COFRES DE SENHA FRENTE ÀS VULNERABILIDADES DO COMPORTAMENTO DO USUÁRIO

Erick Cassimiro Pereira[1]

Julio Cesar Carou Felix de Lima[2]

Olinda Nogueira Paes Rizzo[3]

Resumo

Introdução

A crescente integração da tecnologia no cotidiano transformou a maneira como a sociedade interage, trabalha e armazena informações. Desde transações financeiras até comunicações pessoais, a vida digital moderna exige o uso de múltiplas senhas e credenciais para garantir o acesso seguro a uma vasta gama de serviços online, quando todos os dados estão sendo armazenados gerando um toda uma certidão de quem é você tornando essas informações o ativo com maior valor dentro da internet.

Uma vez que o Black Hat (Hacker) possui todos os seus dados fica fácil para ele saber qual a melhor forma de ataque. O Black Hat são os hackers com intenções maliciosas que obtêm acesso não autorizado a redes e sistemas de computador visando explorar vulnerabilidades de segurança em software ou sistemas corporativos. Essa prática geralmente tem o a intenção de obter algum ganho financeiro sobre a vítima. A problemática central reside na tendência dos usuários a adotarem práticas de gerenciamento de senhas inseguras, como a criação de senhas fracas ou a reutilização da mesma credencial em diferentes plataformas, visando a conveniência em detrimento da segurança (Lenz, 2023).

Este comportamento cria uma superfície de ataque extensa expondo um cenário de alta vulnerabilidade (Silva, 2018), como aponta a pesquisa de campo realizada para este estudo embora que a amostra seja limitada para generalizações estatísticas, os dados coletados neste estudo sugerem que, mesmo em um pequeno grupo, as práticas de reutilização de senhas são prevalentes, alinhando-se com as preocupações levantadas na literatura sobre o tema onde alarmantes 76% dos entrevistados admitiram utilizar a mesma senha para vários aplicativos.

Como mitigação dessa vulnerabilidade, temos os gerenciadores, ou "cofres de senha", softwares especializados cujo objetivo é armazenar e proteger as credenciais do usuário de forma centralizada e segura. Essas ferramentas não apenas facilitam o gerenciamento de múltiplas senhas complexas e únicas, mas também se fundamentam em robustas tecnologias de criptografia para garantir a confidencialidade dos dados. Utilizando padrões globais como o AES (Advanced Encryption Standard) e modelos de segurança avançados como o "zero-knowledge", os cofres de senha asseguram que as informações permaneçam cifradas e inacessíveis até mesmo para os provedores do serviço, representando uma barreira formidável contra acessos não autorizados.

Contudo ataques continuam a acontecer mesmo com tantas ferramentas no mercado, os atacantes fazem a utilização da mais antiga ferramenta que possuímos a engenharia social ou “A Arte de Enganar”, nesse modelo os ataques são direcionados ao elo mais fraco da cadeia de segurança, o ser humano .Por isso ataques de engenharia social vem crescendo cada vez mais no Brasil. “Nos últimos três meses do ano, foram registrados 63,8 milhões de links maliciosos, um aumento de 12% em relação ao começo do ano. O documento mostra

[1]Graduando em Engenharia da Computação da Universidade Santo Amaro, SP. E-mail: erick.cassimiro20@gmail.
[2] Professor Mestre, Universidade Santo Amaro, SP. E-mail: jclima@prof.unisa.br.
[3] Professora Mestra, Universidade Santo Amaro, SP. E-mail: orizzo@prof.unisa.br.

que o campeão de golpes são os links em apps de mensagem como WhatsApp" (Wakka, 2017, n.p).
Dentro desse modelo de engenharia social temos o Ataque de Phishing sendo ele o mais utilizado. O phishing é um tipo de ataque cibernético que usa e-mails, mensagens de texto, telefonemas ou sites fraudulentos para enganar as pessoas a compartilhar dados confidenciais, baixar malware ou se expor a crimes cibernéticos de outras formas.
Este trabalho tem como objetivo analisar a contribuição prática dos cofres de senha na proteção de credenciais e fundamentar a discussão. Os dados preliminares reforçam a relevância do tema, observou-se baixa troca de credenciais de forma periódica (24%) e adoção limitada de gerenciadores (56% não utilizam), quadro que potencializa o impacto de vazamentos e ataques oportunistas. Tendo em mãos dados tão preocupantes o artigo se sustenta na tentativa de analisar os benefícios da utilização dos Cofres de Senha bem como a forma com que os crackers atacam para aumentar a proteção uma vez que sabemos o perfil do atacante.

Objetivo

O objetivo deste trabalho é analisar a eficácia dos cofres de senha como ferramenta de mitigação de riscos, investigando a lacuna entre as robustas tecnologias de criptografia que eles empregam e as práticas de segurança dos usuários que levam a vulnerabilidades persistentes. Mostrando ao leitor as vertentes de se utilizar um cofre de senha e porque se deve utilizar um, além de manter as suas senhas sempre atualizadas, para evitar com que suas informações acabem vazando para potenciais invasores e como agir nesses casos. Além de apresentar a forma em que os Black Hats agem, quais métodos eles utilizam para conscientizar e aumentar o conhecimento referente a segurança e proteção.

Metodologia

O artigo ira se basear em uma pesquisa utilizando como referência artigos, livros, dissertações, teses e sites de produtos envolvendo cybersegurança. O Artigo contou com uma pesquisa elaborada com o objetivo de coletar como hoje as pessoas utilizam cofres de segurança, a pesquisa foi elaborada ao longo de vinte dias, a começar na data 31 de agosto de 2025 e 19 de setembro de 2025, A fim de aumentar o acesso aos entrevistados, essa pesquisa foi elaborada no Forms (Microsoft) Contendo 4 perguntas, 1.Você utiliza algum cofre de senha? 2. Você utiliza a mesma senha para diversos aplicativos ou sites? 3. Você faz a troca da senha regulamente? se essa pergunta fosse respondida com "Sim" era aberta uma 4p, 4. A cada quantos meses?, se a pergunta 3 fosse respondida como não, a pesquisa se encerrava nela. E como forma de divulgação foi utilizado as redes sociais para envio do link. Nesse período foram coletados 25 amostras.
Foi utilizado como critério de avaliação e filtragem dos artigos analisados os que continham assuntos voltados a Criptografia, Hacker e Segurança de Senhas. Deixando de fora artigos que não apresentavam temas voltados para conceitos de segurança. utilizando como fonte de pesquisa artigos publicados em sites de universidades, IEEE, Scielo Brasil, sites governamentais, sites que oferecem serviços de Cybersegurança e Livros publicados entre os anos de 2010 e 2025.

Resultados e Discussão

Para analisar como anda a segurança de credenciais dos Brasileiros, foi elaborado um questionário: https://forms.office.com/r/e93XPEFgBM, onde o intuito foi avaliar se as pessoas utilizam cofres de senha, se mantem uma senha padrão para todos os apps e se fazem a troca da senha regularmente.
Foi obtido um total de 25 repostas onde podemos avaliar, conforme a Tabela 1, 44% dos entrevistados não utilizam qualquer tipo de cofre de senhas. Este dado pode ser analisado

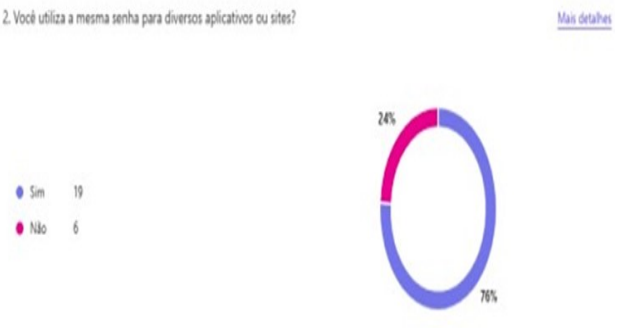
por algumas vertentes, podendo ser a ausência da ferramenta especializada para gerenciar múltiplas senhas complexas praticamente força o usuário a adotar atalhos inseguros ou a uma combinação de fatores, como a falta de conscientização sobre a existência de ferramentas gratuitas, a percepção de que são complicadas de usar, ou uma subestimação geral dos riscos de um vazamento de dados.

Tabela 1. Você utiliza algum cofre de senha?

Fonte: Autor, 2025.

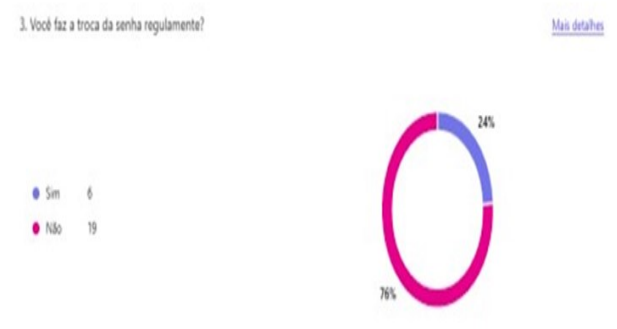
A consequência direta da não utilização de gerenciadores é evidenciada na Tabela 2, que aponta que alarmantes 76% dos participantes reutilizam a mesma senha para diversos sites ou aplicativos. Esta é a vulnerabilidade mais crítica identificada, pois válida a tese de que, na ausência de uma ferramenta, a conveniência dita o comportamento. Na prática, isso significa que a segurança de contas de alto valor (como e-mails e serviços financeiros) está atrelada à segurança do serviço menos protegido em que o usuário se cadastrou. Essa prática expõe os indivíduos diretamente a ataques de *credential stuffing*, onde invasores utilizam credenciais vazadas de um site para tentar acesso em inúmeros outros, maximizando o impacto de uma única falha de segurança.

Tabela 2. Você utiliza a mesma senha para diversos aplicativos ou sites?



Fonte: Autor, 2025.

A situação de risco é agravada pelos dados da Tabela 3, que mostram que 76% dos entrevistados não trocam suas senhas regularmente. Se um usuário já reutiliza suas credenciais, a falta de rotação de senhas prolonga indefinidamente a janela de exposição de uma credencial vazada. Uma senha comprometida há cinco anos pode, portanto, continuar sendo a chave de acesso para os serviços atuais do usuário. Embora as políticas de troca obrigatória de senhas sejam hoje debatidas, com novas diretrizes do NIST sugerindo a troca apenas em caso de vazamento, o hábito de nunca reavaliar a própria segurança, como indicado pelos dados, demonstra uma postura passiva frente às ameaças digitais.



Fonte: Autor, 2025.

A tabela 4 só era apresentada para os entrevistados, caso a pergunta 3 representada pela tabela 3 fosse respondida, dessa forma tivemos 6 respostas, onde uma pessoa afirma que faz a troca semestralmente, duas fazem a troca a cada 3 meses e duas fazem a troca mensalmente.

Tabela 4. A cada quantos meses?

4. A cada quantos meses?

6 Respostas

ID ↑	Nome	Respostas
1	anonymous	Semestral
2	anonymous	A cada 1 mês
3	anonymous	1 mês
4	anonymous	3
5	anonymous	3 meses
6	anonymous	4 mês

Fonte: Autor, 2025.

Em síntese, os resultados formam uma narrativa clara e preocupante: a baixa adoção de cofres de senha (Tabela 1) leva diretamente à prática massiva de reutilização de credenciais (Tabela 2), cujo risco é perpetuado pela ausência de uma política de manutenção de senhas (Tabela 3). Fica demonstrada, portanto, a lacuna investigada neste trabalho: existe uma tecnologia de proteção robusta e acessível, mas sua eficácia é neutralizada por um comportamento de usuário que prioriza a simplicidade em detrimento da segurança. O elo mais fraco não está na criptografia, mas na psicologia humana.

Considerações Finais

Este trabalho teve como objetivo central analisar a eficácia dos cofres de senha, investigando a lacuna entre a robustez da tecnologia e as práticas de segurança dos usuários. A revisão bibliográfica e a pesquisa de campo permitiram concluir que, embora os gerenciadores de senha modernos ofereçam um arsenal tecnológico formidável com criptografia avançada, sua eficácia é ineficaz frente a uma expressiva lacuna de adoção e por comportamentos de risco profundamente arraigados nos usuários. A pesquisa revelou que a maioria dos participantes adota práticas inseguras, como a massiva reutilização de senhas, criando uma superfície de ataque perigosamente ampla. Fica evidente que a principal ameaça não reside em falhas criptográficas das ferramentas, mas na decisão do usuário de priorizar a conveniência em detrimento da segurança, tornando-o o "elo mais fraco" e um alvo vulnerável a ataques de engenharia social. Assim, a existência da ferramenta, por si só, não garante proteção. É fundamental reconhecer que o estudo possui uma amostra reduzida que não permite generalizações estatísticas para o cenário nacional, mas oferece um forte indicativo de tendências comportamentais. Por fim, este estudo reforça que o desafio da segurança de credenciais é sociotécnico. A solução não está apenas em desenvolver tecnologias mais seguras, mas em promover a conscientização e a educação digital, capacitando os usuários a se tornarem uma linha de defesa ativa, e não a principal porta de entrada para ciberataques .

Palavras-chave

Criptografia; Hacker; Cofre de senha; Cybersegurança.

Referências

BENHAMMADI, Farid; BEY, Kadda Beghdad. Password hardened fuzzy vault for fingerprint authentication system. Image and Vision Computing, v. 32, n. 10, p. 746-754, 2014.

CERVINSKI, Natan. Importância da Segurança da Informação e Backup. 2016. Disponível em: https://www.academia.edu/67822415/Import%C3%A2ncia_da_Seguran%C3%A7a_da_Informa%C3%A7%C3%A3o_e_Backup. Acesso em: 23 ago. 2025.

GALVÃO, A. Engenharia social: uma análise de ameaças e cuidados aos funcionários das agências bancárias de Santarém e Itaituba - Pará. In: CONGRESSO INTERNACIONAL DE CIÊNCIA E TECNOLOGIA E DESENVOLVIMENTO, 2., 2017, Santarém. Anais... Santarém: UFOPA, 2017. Disponível em: https://www.researchgate.net/publicion/319551455_ENGENHARIA_SOCIAL_UMA_ANALISE_DE_AMEACAS_E_CUIDADOS_AOS_FUNCIONARIOS_DAS_AGENCIAS_BANCARIAS_DE_SANTAREM_E_ITAITUBA_-_PARA. Acesso em: 28 set. 2025.

LENZ, Diego Emanuel. Cyber security: os cuidados na elaboração e armazenamento de senhas pessoais. 2023. Trabalho de Conclusão de Curso (Graduação em Engenharia de Software) - Universidade Tecnológica Federal do Paraná, Pato Branco, 2023. Disponível em: https://repositorio.utfpr.edu.br/jspui/bitstream/1/36588/1/cybersecurityarmazenamentosenhas.pdf. Acesso em: 03 set. 2025.

MARQUES, Mateus Caracciolo. Gerenciadores de senha: segurança e usabilidade. 2023. Trabalho de Conclusão de Curso (Graduação em Ciência da Computação) -Universidade Federal de Pernambuco, Recife, 2023. Disponível em: https://repositorio.ufpe.br/bitstream/123456789/51319/4/TCC%20Mateus%20Caracciolo%20Marques.pdf. Acesso em: 18 ago. 2025.

MITSUNAGA, Sérgio Seidji; PEREIRA, Thiago Ramos Nunes. A importância do backup em pequenas empresas: o backup em empresas de contabilidade de Americana. Revista Integrada de Ciência e Tecnologia, v. 5, n. 1, 2018. Disponível em: http://ricps.eastus2.cloudapp.azure.com/handle/123456789/3258. Acesso em: 13 set. 2025.

SILVA, Hemuryel Lennon Leonel da. Segurança da informação: estudo de caso sobre o vazamento de senhas - ano de 2017. 2018. Trabalho de Conclusão de Curso (Curso Superior de Tecnologia em Gestão de Segurança Empresarial) - Universidade Tecnológica Federal do Paraná, Curitiba, 2018. Disponível em: https://riut.utfpr.edu.br/jspui/bitstream/1/17295/1/CT_GESER_X_2018_03.pdf. Acesso em: 18 ago. 2025.

SOUZA, Wellington de. Aplicação da álgebra moderna nos fundamentos da criptografia: cifras de césar e cifras de hill. 2022. Trabalho de Conclusão de Curso (Licenciatura em Matemática) - Universidade Federal do Tocantins, Arraias, 2022. Disponível em: https://umbu.uft.edu.br/bitstream/11612/5090/1/WELLINGTON%20DE%20SOUSA%20MARTINS%20-%20TCC%20-%20MATEM%c3%81TICA.pdf. Acesso em: 27 set. 2025.

WAKKA, W. Número de ataques cibernéticos no Brasil quase dobrou em 2018. Canaltech, 07 ago. 2018. Disponível em: https://canaltech.com.br/seguranca/numero-deataques-ciberneticos-no-brasil-quase-que-dobrou-em-2018-119600/. Acesso em: 28 set. 2025.

VASCONCELOS, João Victor Alves, Teste de Invasão: O segredo por trás de como funciona uma invasão hacker, a metodologia de invasão utilizada por hackers. Disponível em: https://sol.sbc.org.br/index.php/connect/article/view/27956. Acesso em: 13/09/2025.

IBM. Banco Bradesco, Systems Hardware z, Storage. [S. l.]: IBM, [202-?]. Disponível em: <https://www.ibm.com/br-pt/case-studies/banco-bradesco-systemshardware-z- storage>. Acesso em: 25.09.2025.

IBM. IBM z17. [S. l.]: IBM, [2025?]. Disponível em:]<https://www.ibm.com/br-pt/products/z17>. Acesso em: 27.09.2025.

IBM. IBM z17: O primeiro mainframe totalmente projetado para a era da IA. [S. l.]:IBM Newsroom Brasil, 8 abr. 2025. Disponível em: <https://brasil.newsroom.ibm.com/2025-04-08-IBM-z17-O-primeiro-mainframetotalmente-rojetado-para-a-era-da-IA?. Acesso em: 27.09.2025.

IBM. Mainframe. [S. l.]: IBM, [202-?]. Disponível em: < https://www.ibm.com/brpt/think/topics/mainframe>. Acesso em: 25.09.2025.

IBM. Mainframe Application Modernization Patterns for Hybrid Cloud. Disponível em: <https://www.redbooks.ibm.com/redbooks/pdfs/sg248532.pdf>. Acesso em: 27.09.2025.

IBM. Modernização de aplicativos legados. [S. l.]: IBM, [202-?]. Disponível em: <https://www.ibm.com/br-pt/think/topics/legacy-application-modernization>. Acesso em: 27.09.2025.

IBM. Getting Started Journey to Modernization with IBM Z. [S. l.]: IBM, [202-?]. Disponível em: <https://www.redbooks.ibm.com/redpapers/pdfs/redp5627.pdf>. Acesso em: 27.09.2025.

MATSU. Modernização de mainframe gera US$ 12 bi em economias de custos coletivos. [S. l.]: IBM, [202-?]. Disponível em: <https://itforum.com.br/noticias/modernizacao-mainframe-12-bi-economias/>. Acesso em: 26.09.2025.