Gestão Pessoal de Credenciais de Acesso a Serviços Digitais

Felipe Juris Jacques[1], **Eduardo Dalcin**[1]

[1] Especialização em Gestão de Tecnologia da Informação
Instituto Federal de Educação, Ciência e Tecnologia Farroupilha Campus Panambi
(IFFAR) – Caixa Postal 98787 – 740 – Panambi – RS – Brazil

Abstract. *The management of credentials to access digital services is an essential aspect of cybersecurity, involving practices and challenges that directly impact the protection of personal data and the integrity of digital services accounts. The users, when interacting with digital services, need to understand the risks associated with their exposure and the factors influencing the effectiveness of the security measures. Proper understanding of this context is critical for individuals and organizations make informed decisions about their digital security practices.*

Resumo. *A gestão de credenciais de acesso a serviços digitais é um aspecto essencial da segurança cibernética, envolvendo práticas e desafios que impactam diretamente a proteção de dados pessoais e a integridade das contas de serviços digitais. Os usuários, ao interagirem com serviços digitais, precisam compreender os riscos associados à sua exposição e os fatores que influenciam a eficácia das medidas de segurança. O entendimento adequado desse contexto é fundamental para que indivíduos e organizações tomem decisões informadas sobre suas práticas de segurança digital.*

1. Introdução

Em um mundo cada vez mais digital, onde a vida cotidiana depende de serviços digitais para comunicação, trabalho e até transações financeiras, a segurança das nossas credenciais de acesso nunca foi tão importante. No entanto, muitos ainda subestimam os riscos de senhas fracas e práticas inseguras, tornando-se alvos fáceis para ataques cibernéticos.

Este artigo busca desmistificar a segurança digital, mostrando de forma acessível como se tornar gestora de sua própria proteção *online*. Contando com exemplos práticos, dicas simples, e estudos relacionados, este artigo visa ajudar compreender os riscos e tomar decisões informadas sobre a segurança digital. Afinal, a segurança não depende apenas de grandes empresas ou sistemas complexos, ela começa com escolhas e conscientes feitas por cada usuário.

2. Credenciais de Acesso a Serviços Digitais

Qualquer serviço digital que exija autenticidade para identificar usuários utiliza credenciais de acesso. Embora cada serviço tenha credenciais únicas, eles compartilham alguns padrões comuns que os usuários conhecem. Além disso, os serviços digitais têm contratos que os usuários devem aceitar, mas a tecnologia por trás da segurança não é transparente para os usuários. No entanto, é responsabilidade do usuário operar corretamente e respeitar práticas de segurança comuns.

Ao se cadastrar, para possuir uma conta de usuário em um serviço digital, é comum fornecer informações pessoais básica de identificação do usuário. Esse cadastro dará origem a um conjunto de credenciais de acesso de uso indiviual, que é utilizado para ter acesso ao respectivo serviço digital, normalmente um identificador unico do usuário como telefone, CPF, nome ou e-mail e uma senha que deve ser forte e segura, de conhecimento exclusivo do usuário.

3. Processo de Autenticação

Quando um usuário acessa um serviço digital, ele faz isso por meio do processo de autenticação (*login*), fornecendo duas informações: uma identificação única (cpf, telefone, nome ou e-mail) e uma senha secreta.

A senha é a primeira barreira contra um acesso não autorizado. Por isso, é fundamental que a senha seja aleatória e sem informações pessoais que possam ser facilmente descobertas ou obtidas. Pois, deixar credenciais vulneráveis pode expor o usuário a riscos ilimitados, como roubo de informações, extorsão, invasão e mais.

3.1. Multi Fator de Autenticação

O multi fator de autenticação (MFA) é uma medida de segurança adicional que exige dois ou mais fatores de verificação para acessar uma conta ou recurso *online*, comum em serviços digitais, como bancos, redes sociais e sistemas corporativos. Isso aumenta a dificuldade de acesso não autorizado, fornecendo uma camada adicional de segurança contra roubo de identidade e fraude cibernética, pois mesmo com a senha, o atacante precisaria de fatores adicionais, como um código enviado ao *smartphone* ou e-mail, uma impressão digital ou outro tipo de verificação adicional.

3.2. Duplo Fator de Autenticação

O duplo fator de autenticação (2FA), autenticação em dois fatores (ADF) ou até mesmo verificação em duas etapas (TFA) é um tipo comum de medida adicional de segurança de multi fator de autenticação (MFA). Os serviços digitais que possuem o duplo fator de autenticação, normalmente utilizam uma chave baseada em OTP (*One-Time Password*), que exige um segundo fator além da senha, um código único que é gerado por um aplicativo no *smartphone* ou um dispositivo *token* (*token* de *hardware*). Isso torna mais difícil para os atacantes acessarem, pois mesmo que eles obtenham a senha, um novo código OTP será exigido.

O *smartphone* pode ser utilizado como um dispositivo de autenticação por meio de um aplicativo de preferencia do usuário, para gerar os códigos baseados em chaves OTP. Para utilizar esse tipo de autenticação no serviço digital que ofereça essa opção, é necessário, procurar pela configuração de segurança da conta do usuário e procurar a opção de ativar o duplo fator de autenticação ou algo relacionado ao termo. Será apresentado um código QR (QRCODE) para ser fotografado pelo aplicativo no *smartphone*, em seguida será necessário digitar o código gerado pelo aplicativo para ativar o duplo fator de autenticação.

Chaves baseadas em OTP para o duplo fator de autenticação permitem utilizar mais de um dispositivo e realizar cópias de segurança. Mas nem todo o serviço digital oferece o duplo fator de autenticação, ou mesmo esse tipo específico de multi fator

de autenticação, então é importante estar atento a política de segurança e recursos de recuperação de acesso de contas.

4. Multiplas Credenciais de Acesso

Ao ter várias credenciais, se faz necessário ter uma boa gestão pessoal de credenciais de acesso a serviços digitais. Isso requer conhecimentos básicos de segurança digital e até adoção de programas e aplicativos voltados a segurança. Em especial, anotar as credenciais de acesso e todos os detalhes relacionados em um lugar seguro como um caderno programa ou aplicativo.

5. Trabalhos Relacionados

5.1. Vazamentos de Dados

[de Araújo et al. 2016], em seu artigo sobre a influência da Lei de Zipf na escolha de senhas, relata vários incidentes de vazamento de informações de usuários de diversos serviços digitais de muitas empresas durante a história recente, muitos dos quais através da apropriação de senhas de usuários.

Vazamentos de dados serviços digitais ocorrem com frequência, por ataques cibernéticos. Existe um site chamado *"Have I Been Pwned"* [Hunt 2023] que cataloga bilhões de credenciais vazadas. O site foi criado pelo especialista em segurança Troy Hunt e é uma grande referência global para verificar vazamentos de dados.

Um vazamento de dados pode não revelar senhas de um serviço digital, pois muitas vezes as senhas são criptografadas por algum algoritmo de derivação de chave. [de Araújo et al. 2016] cita que "o inimigo conhece o sistema", assumindo que o algoritmo de derivação de chave seja público, utilizará de ataques de força bruta em dados vazados, através de busca exaustiva de todo tipo de combinação possível para descobrir o maior número de senhas possíveis.

Uma vez que as senhas são vazadas e descobertas, as credenciais de acesso estão vulneráveis a ataques. Ao ter conhecimento de vazamento de dados ou verificar no site de [Hunt 2023] que alguma credêncial foi vazada, é importante mudar a senha imediatamente.

5.2. Avaliação de Segurança de Senhas

[de Araújo et al. 2016], em seu artigo, analisa a criação de senhas seguras considerando a teoria da informação e a lei de Zipf. A lei de Zipf, que descreve a relação entre a frequência de ocorrência de palavras e sua posição em uma lista ordenada, reduz a entropia das senhas quando linguagens naturais são utilizadas, criando padrões que podem ser explorados por atacantes.

A pesquisa de [de Araújo et al. 2016] conclui que a estratégia mais eficaz para criar senhas robustas é a utilização de acrônimos, que consiste em combinar a primeira letra de cada palavra de uma frase, que aumenta a entropia por caractere em aproximadamente 80%. Essa estratégia chega proximo a entropia maxima, é possível melhorar ainda esta estratégia se também utilizar algarismos e caracteres não alfanuméricos. O estudo destaca a importância de escolher senhas que maximizem o espaço de busca para ataques de força bruta, especialmente em sistemas com restrições de comprimento.

5.3. Limitações de Segurança em Serviços Digitais

[de Araújo et al. 2016], relata limitações de segurança em algum serviços digitais na conclusão de seu artigo:

> Conforme observado em, 'Muitas vezes os sistemas restringem o comprimento da chave, por exemplo, a Microsoft restringe a 16 caracteres, muitas lojas de comércio eletrônico também restringem drasticamente o número de caracteres de uma senha. Lojas virtuais como Submarino e Americanas.com utilizam o máximo de 8 caracteres, enquanto Netshoes utiliza 15 e, ainda, Mercado Livre, 20. Mais grave ainda são os bancos que, além de restringir o tamanho de sua senha, restringem também o alfabeto, aceitando apenas dígitos de 0 a 9. Essa prática de restringir o tamanho e tipo de caracteres nas senhas pode levar à criação de senhas mais fracas e, portanto, mais vulneráveis a ataques. [de Araújo et al. 2016]

A pesquisa forense de [Berrios et al. 2023] analisa quinze aplicativos de duplo fator de autenticação em diferentes sistemas operacionais, investigando os dados que armazenam e como podem ser explorados. Os resultados revelam que muitos aplicativos guardam informações confidenciais, como chaves secretas e detalhes de contas, frequentemente sem criptografia robusta. A descoberta dessas chaves não criptografadas permitiu aos pesquisadores contornar o duplo fator de autenticação, demonstrando uma vulnerabilidade significativa. O estudo destaca a necessidade de maior segurança nos aplicativos.

5.4. Ataques de phishing

Phishing é um tipo de ataque cibernético onde criminosos tentam obter vantagem ou obter informações confidenciais, como senhas, informações pessoais e até detalhes de cartões de crédito, por meio de comunicações fraudulentas. Este termo deriva da palavra "fishing", que significa pescar em inglês, aludindo à ideia de lançar iscas para capturar vítimas desavisadas.

O artigo de [Grimes 2019] começa reconhecendo que as senhas sozinhas são cada vez mais insuficientes para proteger contas de usuários e dados. A crescente adoção do duplo fator de autenticação ou o multifator fator de autenticação, está se tornando essencial para a segurança cibernética. Apesar dos benefícios, [Grimes 2019] destaca que muitas soluções de multifator fator de autenticação são erroneamente consideradas invulneráveis. Ele argumenta que, com conhecimento e as técnicas certas, o multifator fator de autenticação pode ser contornado.

[Grimes 2019] descreve que os invasores exploram vulnerabilidades no software, protocolos, infraestrutura da solução do multifator fator de autenticação, engenharia social e até roubo de dispositivos:

- Roubo de *Cookies*: Um dos métodos mais comuns envolve o envio de e-mails de phishing que simulam uma página de autenticação legítima. Se o usuário inserir suas credenciais e um código do duplo fator de autenticação, o invasor pode roubar o cookie de sessão e usá-lo para acessar a conta sem precisar do código novamente.
- Sequestro de Assunto (*Subject Hijacking*): Em algumas soluções de multifator fator de autenticação, o atacante pode modificar o identificador do assunto, permitindo que ele acesse contas ou privilégios associados a um usuário diferente.

- Troca de SIM (SIM *Swap*): Os atacantes podem enganar as operadoras de telefonia móvel para transferir o número de telefone da vítima para um cartão SIM sob seu controle, permitindo que interceptem códigos de duplo fator de autenticação enviados por SMS.
- Mensagens de Recuperação de SMS Forjadas (*Forged SMS recovery messages*): Os atacantes podem usar informações básicas (como e-mail e número de telefone) para enviar mensagens SMS fraudulentas se passando por provedores de serviços, solicitando um código de recuperação ou induzindo o usuário a fornecer informações confidenciais.
- Duplicação de Geradores de Código (*Duplicate code generators*): Embora consideradas mais seguras, até mesmo soluções baseadas em TOTP (*Time-based One-Time Password*) podem ser vulneráveis se a "*seed*"secreta usada para gerar os códigos for comprometida ou se existirem vulnerabilidades na implementação do software ou applicativo.
- Sociais (engenharia social contra o usuário ou suporte): Manipulam indivíduos para que revelem seus códigos de duplo fator de autenticação ou concedam acesso não autorizado. O exemplo do e-mail de phishing para roubo de cookies também se enquadra nessa categoria, pois explora a falta de discernimento do usuário. Enganar o suporte técnico para que desabilite o multi fator de autenticação ou forneça códigos de acesso também é uma tática de engenharia social.
- Físicos (roubo ou duplicação de um fator físico): Envolvem a obtenção física do dispositivo usado para o multi fator de autenticação (por exemplo, um *smartphone* com um aplicativo autenticador) ou a duplicação de um *token* físico (se aplicável). O roubo de um smartphone com um aplicativo autenticador ativo permite que o invasor acesse contas protegidas por multi fator de autenticação. A duplicação de impressões digitais (embora tecnicamente difícil) ou outros fatores biométricos também representa uma ameaça.

No entanto, [Grimes 2019] enfatiza que, para mitigar os riscos associados aos ataques à ao multi fator de autenticação, é crucial educar os administradores e usuários finais sobre as várias maneiras pelas quais o multi fator de autenticação pode ser hackeado e sobre as melhores práticas para se protegerem.

O artigo [Grimes 2019] desmistifica a ideia de que a autenticação de dois fatores e multifator é uma solução de segurança infalível. Ao detalhar várias técnicas que os atacantes podem usar para contornar o multi fator de autenticação, o autor destaca a necessidade de uma compreensão mais profunda das vulnerabilidades inerentes a essas tecnologias e dos vetores de ataque. A principal mensagem é que a implementação do multi fator de autenticação deve ser acompanhada por uma forte conscientização e educação dos usuários para que eles possam reconhecer e evitar as diversas táticas de engenharia social e outros métodos de ataque. Em última análise, embora o multi fator de autenticação represente uma melhoria significativa em relação à autenticação de fator único, a vigilância e a educação contínua são essenciais para garantir a segurança das contas e informações.

6. Metodologia

A metodologia adotada é a pesquisa aplicada, que segundo [Gil 2019], a pesquisa aplicada, abrange estudos elaborados com a finalidade de resolver problemas identificados

no âmbito das sociedades em que os pesquisadores vivem. Da mesma forma, pesquisas aplicadas podem contribuir para a ampliação do conhecimento científico e sugerir novas questões a serem investigadas.

O público-alvo desta pesquisa são os usuários de serviços digitais, especialmente aqueles que compartilham dados pessoais *online* e utilizam plataformas digitais para fins, pessoais, profissionais ou até financeiros, que, portanto, necessitam de maior atenção e cuidado com a segurança digital.

Este estudo utilizou uma abordagem quantitativa para investigar as práticas de segurança digital dos usuários em relação às suas credenciais de acesso. A coleta de dados foi realizada de forma anônima, através de um questionário *online* elaborado na plataforma Microsoft Forms. O questionário abordava temas como o uso de senhas, autenticação em dois fatores, gestão de credenciais, entre outros, e foi divulgado em grupos de WhatsApp. A pesquisa garantiu a privacidade e confidencialidade das respostas, assegurando o anonimato dos participantes.

Realizado uma avaliação prática dos aplicativos de autenticação de dois fatores Google Authenticator, Microsoft Authenticator e Aegis em sistema Android, durante um período um semestre. Os aplicativos foram selecionados com base em sua popularidade e disponibilidade, bem como a presença de um aplicativo de código aberto (Aegis) para fornecer uma perspectiva mais diversificada. Durante o período de teste, foram avaliados os recursos oferecidos por cada aplicativo, incluindo a facilidade de uso, o gerenciamento de contas, os recursos de segurança adicionais e a usabilidade geral. Além disso, foram registrados os problemas e dificuldades encontrados durante o uso diário dos aplicativos, a fim de avaliar sua eficácia e eficiência em diferentes contextos.

Realizado uma busca para experimentar aplicativos para gerenciar virtualmente as senhas de serviços digitais baseada do nos sistemas operacionais Android e Windows.

7. Resultados e Discussão

7.1. Pesquisa de Campo

A pesquisa sobre hábitos e percepções relacionadas a senhas, autenticação de dois fatores e segurança digital teve 17 respostas. É possível extrair de 17 respostas individuais um resumo consolidado de uma pesquisa sobre o comportamento e a confiança dos usuários em relação às suas credenciais digitais e à segurança dos serviços *online*.

As respostas revelam uma variedade de práticas de gerenciamento de senhas e níveis de uso do duplo fator de autenticação. Houve incidentes de segurança digital relatados por uma parcela significativa dos entrevistados. A percepção geral sobre a segurança dos serviços digitais utilizados e a confiança nas próprias ações de gestão de credenciais variam, mas tendem a ser moderadamente positivas.

7.1.1. Força das Senhas

Os entrevistados utilizam diferentes estratégias para criar senhas.

- 35% (6 respostas) utilizam senhas ”muito grandes e totalmente aleatórias”;
- 18% (3 respostas) utilizam ”frases longas e criativas para usar como senha”;

- 18% (3 respostas) preferem ”senhas simples sempre que possível”;
- 29% (5 respostas) utilizam ”informações pessoais como senha para nunca esquecer”.

7.1.2. Vivência com Tecnologia

A maioria dos entrevistados possui uma vivência considerável com a tecnologia, seja através de estudo, trabalho ou uso geral. A maioria dos entrevistados indica vivência com tecnologia ”Mais de 10 anos”ou ”Até 10 anos”. Vários entrevistados trabalham na área de tecnologia ou estudam na área relacionada, indicando um potencial maior conhecimento sobre segurança.

7.1.3. Memorização de Acessos em Navegadores

A maioria dos entrevistados opta por digitar suas senhas completas e permanecer autenticados.

- 59% (10 respostas) digitam suas senhas ”uma única vez e permaneço autenticado”;
- 41% (7 respostas) permanecem autenticados ”apenas para o básico”.

7.1.4. Utilização do Duplo Fator de Autenticação

A maioria dos entrevistados utiliza o duplo faltor de autenticação em alguma forma. Google Authenticator e Microsoft Authenticator são os aplicativos de 2FA mais utilizados.

- A maioria das respostas para a pergunta 4 indicam ”Utilizo se necessário”ou ”Sempre utilizo”para SMS e Aplicativo no celular/2FA;
- Há uma menor utilização do dispositivo físico 2FA;
- 12 respostas indicam uso do Google Authenticator;
- 6 respostas indicam uso do Microsoft Authenticator.

7.1.5. Gerenciamento de Senhas e Credenciais

As pessoas utilizam diferentes métodos para lembrar suas senhas.

- 10 respostas indicam que ”Eu me recordo de minhas senhas”;
- 6 respostas indicam que memorizam as senhas ”no navegador e/ou no celular”;
- Uma pequena parcela anota em cadernos ou utiliza planilhas eletrônicas.

7.1.6. Experiências com Problemas de Credenciais Digitais

Uma parcela considerável dos entrevistados já enfrentou problemas com suas credenciais digitais.

- 4 respostas indicam ”Já tive meu login roubado”;

- 1 resposta indica que ”Já criaram uma conta falsa se passando por mim”;
- 0 respostas indicam ”Já tive prejuízo financeiro por problemas de segurança relacionado a minha conta”;
- 7 respostas indicam ”Não consegui utilizar algum serviço por causa da dificuldade de acesso digital”.

7.1.7. Percepção de Segurança dos Serviços Digitais

A maioria dos entrevistados avalia os serviços digitais que utiliza como seguros, com a média em 3.88 em uma escala de 1 a 5.

- 9 respostas deram nota 4;
- 5 respostas deram nota 3;
- 3 respostas deram nota 5.

7.1.8. Confiança na Gestão Pessoal de Credenciais

A confiança nas próprias ações de gestão de credenciais é ligeiramente menor do que a percepção da segurança dos serviços, com a média em 3.47 em uma escala de 1 a 5.

- 7 respostas deram nota 4;
- 3 respostas deram nota 5;
- 2 respostas deram nota 3;
- 2 respostas deram nota 2;
- 1 resposta deu nota 1.

7.1.9. Considerações Adicionais

A resposta do entrevistado 3, na seção 8, oferece uma sugestão para ”Jogar fora Hotmail e Outlook e usar tudo do Google com dados falsos”, o que reflete uma preocupação com a privacidade e a exposição de dados.

7.2. Avaliação Prática dos Aplicativos de Duplo Fator de Autenticação

Durante a avaliação prática dos aplicativos de duplo fator de autenticação, foram identificados pontos positivos e negativos em relação à usabilidade, segurança e eficácia dos aplicativos.

7.2.1. Google Authenticator

O Google Authenticator foi considerado o mais fácil de usar, com uma interface simples, auto explicativa e intuitiva. No entanto, o aplicativo não oferece recursos adicionais, cópias de segurança é exclusivamente em nuvem e sómente é permitido instalar o aplicativo em um aparelho GMS (Google Mobile Services).

Em um aparelho GMS, a memorização de senhas ou preenchimento automático de senhas oferecida pelo Google não tem relação com esse aplicativo, na verdade esse é um recurso do próprio aplicativo do Google.

7.2.2. Microsoft Authenticator

Microsoft Authenticator, por sua vez, possui uma interface mais complexa com poucas intruções de utilização do aplicativo. Há recursos adicionais para as contas de usuários Microsoft, como a possibilidade de inpecionar o historico de atividade e autenticar apenas confirmando a notificação no *smartphone*, sem a necessidade de digitar o código do duplo fator de autenticação. Há também diversos recursos diferentes, talvez o mais importante seja a possibilidade de memorização de senhas ou preenchimento automático de senhas.

Cópias de segurança das chaves de duplo fator de autenticação é exclusivamente em nuvem e somente é possível instalar o aplicativo em dispositivos GMS. A Microsoft oferece recursos corporativos, então para quem utilizar esse aplicativo para proteger sua conta corporativa, precisa usar uma conta pessoal para realizar o cópias de segurança das chaves de duplo fator de autenticação, também é possível utilizar outros aplicativos para essa finalidade, mas essa opção está um pouco escondida.

Assim como o Microsoft Authenticator tem diversos recursos, há diversas instabilidades relacioanado diretamente as contas de usuário Microsoft. Em uma tentativa de instalar o aplicativo com uma conta de usuário que ainda não havia duplo fator de autenticação, foi solicitado que a conta fosse verificada pelo proprio aplicativo ainda não configurado, alternativamente era possível apenas digitar a senha, tornando a experiência confusa. Ainda na mesma tentativa, ao finalizar o processo de autenticação, houve um erro de comunicação entre o aplicativo e o servidor, impossibilitando a utilização do aplicativo.

Figura 1. Erro de comunicação entre do aplicativo Microsoft Autenticator

Outro erro ocorreu ao tentar configurar uma outra conta de usuário que já utilizava

o duplo fator de autenticação para utilizar os recursos extras de autenticação, fucionando de uma forma diferente, onde durante um processo de autenticação, será solicitado uma confirmação de notificação no *smartphone*. A aplicativo recebeu instruções para ativar o Bluetooth, embora atipico para esse tipo de autenticação, ao tentar efetuar a autenticação, o aplicativo não respondeu e em tentativas posteriores, ocorria erro no aplicativo. No final, houve transtornos para recuperar o acesso a conta de usuário, pois nem mesmo os metodos extras de autenticação funcionaram.

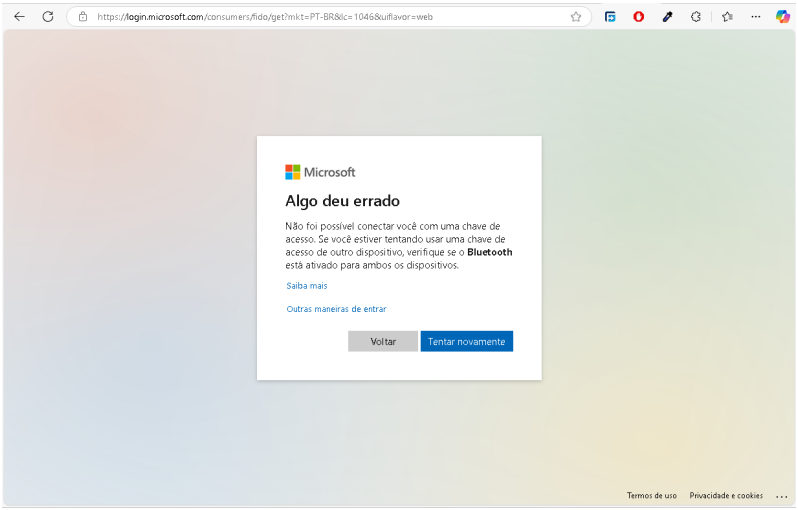

Figura 2. Erro no duplo fator de autenticação da Microsoft

7.2.3. Aegis

Já o Aegis, por ser um aplicativo de código aberto, oferece maior transparência e controle sobre os dados do usuário, mas possui uma interface de configuração e arquivos que pode ser menos amigável para usuários mais leigos. Nele é possível adicionar e gerenciar chaves de autenticação de dois fatos, exportar e importar cópias de segurançats para diversos aplicativos ou em formato de arquivos, inclusive em formato criptografado.

A maior vantagem do Aegis é a possibilidade de instalar o aplicativo por meio da loja de aplicativos de código aberto F-Droid, uma alternativa ao Google Play Store, permitindo que o mesmo possa ser intalado em dispositivos Android sem GMS ou AOSP (Android *Open Source Project*). Vale destacar que o aplicativo tem instruções de recomendações e avisos para lembrar o usuário de realizar cópias de segurança e mais.

7.3. Avaliação de Aplicativos de Gerenciamento de Senhas

No sistema operacional Android com GMS o Google automaticamente oferece um popup para salvar a senha no momento em que é digitada no processo de autenticação de algum aplicativo ou serviço. Como o Google não é especificamente um aplicativo de segurança, pode parecer um pouco escondido a opção de gerenciar as senhas pelas configurações de conta. Além do gerenciamento de senhas com sincronização em nuvem, é possível adicionar anotações, exportar e importar em formato de plianilha CSV sem criptografia.

O mesmo pop-up do Android utilizado pelo Google pode ser substituido por aplicativos de terceiros, como o Microsoft Authenticator, citado anteriormente que oferece

recursos adicionais para gerenciar senhas. Também permite adicionar anotações, exportar e importar em formato de plianilha CSV sem criptografia.

No sistema operacional Windows não há opção nativa ou pré instalada para salvar senhas, dependendo de programas de terceiros para salvar senhas. Navegadores de internet normalmente oferecem uma opção nativa para salvar senhas, mas com poucos recursos extras de segurança ou gerenciamento. Infelismente os navegadores de internet não solicitam uma senha mestre para liberar a autenticação ou até mesmo para visualizar a senha.

7.3.1. KeePass

O KeePass é um aplicativo ou programa de código aberto para computadores pessoais. Diferente dos aplicativos citados anteriormente, o KeePass não é um aplicativo para dispositivos móveis como tablets ou *smartphone*, mas sim um aplicativo desktop, que pode ser instalado em qualquer dispositivo com sistema operacional Windows. Existem também versões para outros sistemas operacionais como Linux, Mac OS e até BSD, desenvolvido por contribuidores não oficiais.

Por padrão o KeePass é em inglês, necessitando de plugins de tradução para outras idiomas. Embora a interface aparente ser para computadores mais antigos, não se trata de um aplicativo desatualizado, mas sim um aplicativo com uma interface única, compatível com qualquer sistema operacional recente. Além de que a interface é amigável para gerenciar senhas, com maior foco no gerenciamento das anotações e com sugestões inteligentes de senhas fortes. Porém, sem integração com o sistema operacional, ou seja, nele, o usuário vai apenas realizar anotações, sem possibilidade de auto completar senhas em processos de autenticação e sem sincronização com outros dispositivos.

O KeePass permite salvar as senhas em formato de arquivos com criptografia, os arquivos são salvos localmente pelo qual o usuário deve se compromenter em salvar em um local seguro e manter cópias de segurança em outros locais. Entretanto, o próprio aplicativo oferece e sugere a possibilidade de imprimir uma cópia de segurança do arquivo de senhas.

7.3.2. KeeWeb

No site oficial de KeePass exístem vários aplicativos que são contribuições não oficiais de KeePass, como KeeWeb que é um aplicativo de código aberto compatível com KeePass, em que é possível utilizar o mesmo banco de dados do KeePass. Diferente dos aplicativos citados anteriormente, o KeeWeb não é um aplicativo nativo, mas sim um aplicativo web progressivo, multi plataforma, que pode ser instalado em qualquer dispositivo com navegador de internet. Assim como KeePass, não há integração com o sistema operacional para auto completar senhas em processo de autenticação.

Por padrão o KeeWeb é em inglês, também necessitando de plugins de tradução para outros idiomas, porém com a praticidade de poder instalar os plugins diretamente pelo aplicativo. O KeeWeb apresenta uma interface moderna e amigável para gerenciar senhas, com o mesmo foco no gerenciamento das anotações assim como no KeePass.

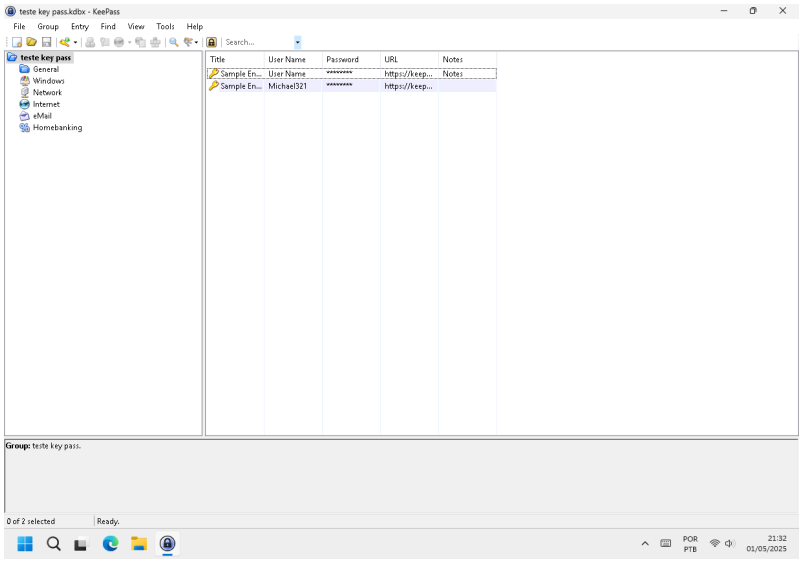

Figura 3. Programa de gerenciamento de senhas KeePass

O KeeWeb permite salvar as anotações de senhas com ou sem criptografia, os arquivos ficam dentro da memoria do navegador de internet e podem ser exportados localmente em formato de arquivos. Há um diferencial nesse aplicativo que permite exportar os arquivos em nuvens de serviços de terceiros em que o usuários tiver preferencia.

Utilizar aplicativos de gerenciamento de senhas, apresentou grande praticidade, especialmente para os serviços que não se mantem autenticados, solicitam a autenticação com frequencia ou perdem a autenticação por defeito. Porém os aplicativos de gerenciamento de senhas e navegadores de internet não são perfeitos, em alguns casos, apresnetam o popup sob a caixa de entrada do login, senha ou botões. Já o KeeWeb, quando não configurado para o mesmo idioma do dispositivo, é prejudicado no sistema operacional Android, por ser um aplicativo web progressivo, o Google Chrome insiste em traduzir o aplicativo e até mesmo as senhas, tornando as senhas inválidas.

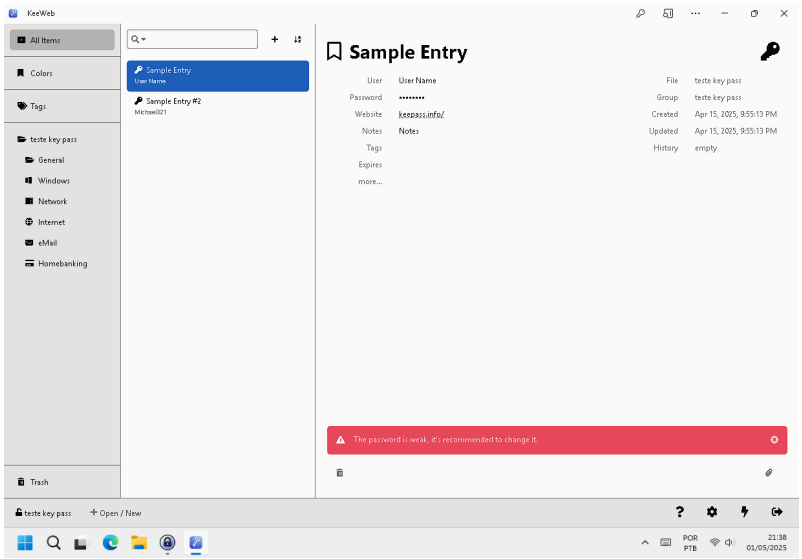

Figura 4. Aplicativo de gerenciamento de senhas KeeWeb

8. Considerações Finais

8.1. Resultados da Pesquisa de Campo

A pesquisa revela que, embora a maioria dos entrevistados utilize o duplo fator de autenticação e tenha uma percepção razoável da segurança dos serviços, ainda há espaço para melhoria na força das senhas e na gestão pessoal de credenciais. Os incidentes de segurança relatados por uma parcela significativa dos participantes reforçam a importância de práticas de segurança digital mais robustas e da conscientização sobre os riscos. A sugestão de um entrevistado sobre o uso de dados falsos destaca uma preocupação com a privacidade que pode influenciar o comportamento do usuário em relação à segurança.

8.2. Resultados de Programas e Aplicativos

O duplo fator de autenticação baseado em OTP é uma forte camada adicional de segurança para proteger as contas dos usuários. No entanto, nem todos os serviços digitais oferecem essa tecnologia, além de ser praticamente restrita para dispositivos móveis e chaves físicas. Inclusive é necessário realizar cópias de sergurança para evitar complicações, mas nem todo programa, aplicativo ou serviço digital reforça essa prática.

Embora existam aplicativos e programas variados de segurança pessoal, não é tão simples de escolher o aplicativos ou programa mais adequando para o uso pessoal já que a complexidade tecnica é um obstáculo.

É improvável que uma pessoa possa memorizar muitas credenciais de acesso, especialmente com alta entropia de senhas. Optar por anotar as informações em um caderno requer menos desafios de informatização, porém é mais trabalhoso e necessita de atenção ao representar caracteres especiais, letras maiúsculas ou minúsculas para evitar erros. Enquanto que anotar as informações em formato digital é mais fácil, mas requer conhecimento de informatização, uso de programas ou aplicativos de terceiros e cuidado onde os dados são armazenados.

Especialmente se tratando de aplicativos ou programas para anotar senhas, há poucas opções de referências, ainda mais com a transparência dos sistemas operacionais e navegadores de internet com opções nativas ou pré instaladas, normalmente com pouco recursos de segurança e gerenciamento. Os principais navegadores de internet oferecem recursos simples para armazenar informações básicas das credenciais de acesso, alguns até com a possibilidade de sincronizar as informações entre dispositivos. Por outro lado, para se ter mais controle de informações e recursos de seguraça, existem programas e aplicativos de terceiros, oferecendo diversas vantagens. Experimentar cada aplicativo ou programa para encontrar o mais adequado exige bastante tempo e organização.

De qualquer forma, deve-se evitar anotar senhas em lugares inapropriados como aplicativos de bloco de notas, aplicativos de mensagens em geral ou até em formato de contatos de telefones, pois todos esses recursos não são criptografados e normalmente não são projetados para esses fins e podem ser explorados por usuários mal intencionados ou vulnerabilidades de segurança.

8.3. Considerações Sobre a Segurança

Por mais sofisticados que os serviços digitais possam ser, não existe garantias de segurança. Cada estratégia de segurança é uma camada a mais, uma barreira adicionado

contra ataques. Ao mesmo tempo, cada camada adiciona complexidade, necessitando de anotações, cópias de segurança e até aplicativos confiaveis, do contrário, as camadas de segurança que deviam proteger o usuário, pode se tornar um obstáculo para o próprio usuário.

A conscientização sobre golpes é crucial, pois o conhecimento é a primeira linha de defesa contra os ataques cibernéticos. É importante estar atento a mensagens e propagandas que possam ser enganosas, solicitando dados confidênciais ou fornecendo algo suspeito. Ao receber um código de autenticação sem solicitar, não o informe a ninguém e altere a senha, pois pode ser uma tentativa de invasão.

Todo o serviço que é bem feito, vai usar um algoritmo de derivação de chave e nunca vai salvar as senhas das credenciais de forma aberta. Logo, se o mesmo limita o comprimento ou variabilidade de caracteres do cadastro da senha, é um grande indicativo de que o serviço não está preocupado com a segurança dos dados dos usuários. Mesmo assim, senhas devem ter alta entropia, ou seja, devem ser longas e misturar todas as opções digitáveis do teclado, pois a senha é a primeira barreira de segurança.

Referências

Berrios, J., Mosher, E., Benzo, S., Grajeda, C., and Baggili, I. (2023). Factorizing 2fa: Forensic analysis of two-factor authentication applications. *Forensic Science International: Digital Investigation*, 45.

de Araújo, L. C., Sansão, J. P. H., and Yehia, H. C. (2016). Influência da lei de zipf na escolha de senhas. *Revista Brasileira de Ensino de Física*, 38(1).

Gil, A. C. (2019). *Como Elaborar Projetos de Pesquisa*. Editora Atlas, São Paulo, 6 edition.

Grimes, R. (2019). The many ways to hack 2fa. *Network Security*, 2019(9).

Hunt, T. (2013–2023). Have i been pwned. Acesso em: 9 abril. 2025.