



ENGENHARIA DA COMPUTAÇÃO

ANA KAILANY COSTA DE SOUSA
ARTUR JARDEL SOARES GOMES
GUSTAVO ALMEIDA VASCONCELOS

PASS_C_WORD:
MANUAL DO USUÁRIO

SOBRAL - CE

2022

1. PASS_C_WORD

O aplicativo tem como objetivo gerenciar e armazenar, isso de forma segura, senhas pessoais de usuários, assim, automatizando esse processo e tornando a relação entre indivíduos e senhas mais prática.

2. Telas

- **Inicial;**

Contém um menu, onde de acordo com a escolha do usuário dentre as opções ([1] – Cadastrar-se; [2] – Logar; [3] – Sair.), pode ser feito o redirecionamento para outra tela.

Figura 1 – Tela inicial



Fonte: Aplicativo PASS_C_WORD.

- **Cadastro de usuário;**

Nesta tela é feito o cadastro de usuários, onde estes podem, posteriormente, fazer login para cadastrar senhas.

Figura 2 – Tela de cadastro de usuário

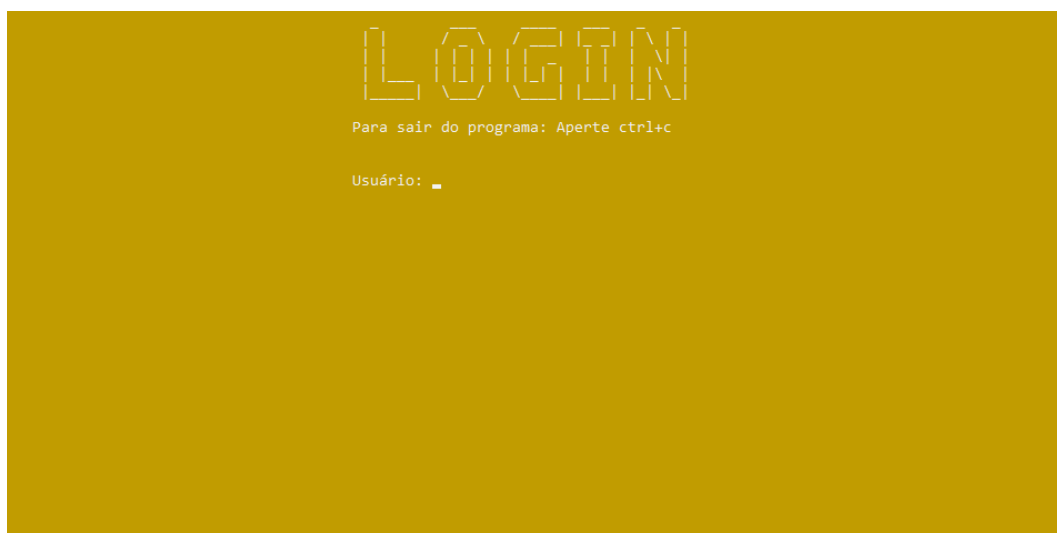


Fonte: Aplicativo PASS_C_WORD.

- **Login;**

Onde usuários cadastrados podem “logar”, para, assim, poderem cadastrar suas senhas pessoas.

Figura 3 – Tela de login



Fonte: Aplicativo PASS_C_WORD.

- **“Logado”;**

Quando um indivíduo faz o login e esse condiz com seus dados de usuário, ele é redirecionado para a tela “logado”. Onde esse(a) poderá, se escolher “1” poderá cadastrar uma nova senha, “2” para visualizar suas senhas salvas em um arquivo txt e “3” para sair (voltar para a tela inicial – *Figura 1*).

Figura 4 – “Logado”



Fonte: Aplicativo PASS_C_WORD.

- **Visualização de senhas;**

Onde o usuário consegue visualizar suas senhas salvas.

Figura 5 – Tela de visualização de senhas



Fonte: Aplicativo PASS_C_WORD.

- **“Saindo..”.**

Quando se faz a saída do aplicativo, opção “3” da *Figura 1*.

Figura 6 – Tela “Saindo”



Fonte: Aplicativo PASS_C_WORD.

3. Dinâmica do aplicativo

O aplicativo utiliza-se de métodos de “renderização” e elementos para deixar a experiência do usuário mais dinâmica e atrativa, onde podem ser citados: cores chamativas, fluidez entre as telas e formatações de textos seguindo diferentes estruturas.

4. Funcionalidades

As principais funcionalidades do aplicativo são:

- Cadastrar usuários;
- Cadastrar senhas;
- Visualizar senhas;
- Dados criptografados.

5. Dicas para senhas seguras

1. Use caracteres especiais e letras maiúsculas:

Tornar a senha complexa diversificando a sua composição com diferentes caracteres como: #; \$; @; &, entre outros e letras maiúsculas, é fundamental para se

obter uma senha mais segura. Isso fica evidente com o fato de alguns sites ou softwares obrigarem os usuários a utilizarem durante o cadastro.

2. Evite sequências numéricas e a sua data de nascimento:

Muitos usuários colocam suas senhas como sequências numéricas, como 1234, ou até mesmo data de nascimento. Por mais absurdo que seja, ainda é muito comum, sendo a facilidade de lembrar a principal motivação, evitar optar por essas combinações, é uma das primeiras tentativas dos criminosos que buscam acessar seus dados.

3. Varie o máximo que puder de uma senha para outra:

Evite repetir senhas, variando as senhas de um aplicativo para outro, pois impede que mais dados possam ser acessados por criminosos que tenham acesso a sua senha. É importante nesse quesito a utilização de um gerenciador, pois além de guardar criptografado essas senhas, armazena de forma organizada, para caso você esqueça. O Pass_C_Word tem essa função, trazendo praticidade para o usuário.

4. Implementar a autenticação de dois fatores:

Outra maneira de deixar a sua senha mais segura, além das apresentadas até o momento, é a autenticação de dois fatores, que basicamente trata-se do envio de uma mensagem adicional, como um código, para algum aparelho que somente o usuário tenha acesso, necessitando do código em questão e da senha cadastrada para o acesso.

5. Instalar a identificação por biometria ou Face ID:

Hoje em dia é muito comum a utilização da biometria ou Face ID como mecanismo de segurança, o que é bastante recomendado, nesses casos, o aparelho celular pede somente uma vez a senha, guarda, e fica utilizando somente mecanismos pessoais de cada usuário, deixando o acesso mais pessoal e consequentemente seguro.

6. Use um gerenciador de senhas:

Outra dica muito crucial, é a utilização de um gerenciador de senhas, pois além de garantir a criação de senhas fortes e seguras, com diferentes caracteres e combinações para cada conta online, ele garante o armazenamento seguro destas, através de um sofisticado sistema de criptografia, em síntese, ele realiza todo o trabalho que você teria de seguir todas as recomendações para se ter uma senha segura.

7. Não compartilhe sua senha com estranhos:

Apesar de óbvia, essa última dica ainda é uma problemática. Sites, bancos e aplicativos, nunca pedem sua senha através de mensagens de textos, ligações ou algo do tipo, somente nas telas de login apropriada, onde sua senha será devidamente criptografada, atitudes como essas são comuns para possíveis criminosos, por isso é de extrema importância que a sua palavra chave seja apenas de seu conhecimento.

REFERÊNCIAS

CORBETT, Liz. **Dia Mundial da Senha: um breve resumo (da longa) história das senhas - The LastPass Blog. The LastPass Blog.** Disponível em: <<https://blog.lastpass.com/pt-br/2022/05/dia-mundial-da-senha-um-breve-resumo-da-longa-historia-das-senhas/>>. Acesso em: 1 jul. 2022.

BORGES, Diego. **7 dicas para criar senhas seguras. Tecmundo.com.br.** Disponível em: <<https://www.tecmundo.com.br/seguranca/236359-7-dicas-criar-senhas-seguras.htm>>. Acesso em: 1 jul. 2022.

MACEDO, Joyce. **Aprenda como e por que você deve usar um gerenciador de senhas. Canaltech.** Disponível em: <<https://canaltech.com.br/seguranca/aprenda-como-e-por-que-voce-deve-usar-um-gerenciador-de-senhas/>>. Acesso em: 2 jul. 2022.