Educação Profissional Paulista

Técnico em **Ciência de Dados**

Secretaria da Educação

SÃO PAULO
GOVERNO DO ESTADO

Introdução à informática

Navegação na internet e segurança on-line

Aula 2

Código da aula: [DADOS]ANO1C1B3S22A2

Secretaria da Educação
SÃO PAULO
GOVERNO DO ESTADO

Introdução à informática

Mapa da Unidade 5 Componente 1

semana 11

Sistemas operacionais (parte II)

semana 15

Produtividade com software (parte I)

semana 19

Produtividade com software (parte II)

Você está aqui!

semana 22

Navegação na internet e segurança on-line

Introdução à informática

Mapa da Unidade 5 Componente 1

Você está aqui!

22

Navegação na internet e segurança on-line

Aula 2

Código da aula: [DADOS]ANO1C1B3S22A2

Objetivos da aula

- Aprender sobre senhas e como usá-las da melhor forma.

Recursos didáticos

- Recurso audiovisual para exibição de vídeos e imagens;
- Acesso ao laboratório de informática e/ou à internet.

Duração da aula

50 minutos.

Competências técnicas

- Aprender a se comunicar e a pensar de forma crítica e analítica.

Competências socioemocionais

- Trabalhar em equipe, compartilhando conhecimentos, contribuindo com ideias e colaborando para alcançar objetivos comuns.

Construindo o **conceito**

Por que senhas fortes são importantes?

- **Senha** é uma **chave** que permite **autenticar o acesso de um usuário a uma plataforma**, garantindo que seja legítimo. Há outras formas de autenticação, como biometria, por exemplo.
- Essas chaves são a primeira linha de defesa contra acessos não autorizados às suas contas on-line.
- Uma **senha forte** pode ser a diferença entre **proteger suas informações** pessoais e ser vítima de roubo de identidade ou fraude financeira.

Construindo o **conceito**

	Como as senhas são roubadas?	Como se prevenir?
Ataques de força bruta (*brute force*)	Coloca-se um programa com estrutura similar a um laço forte para testar todas as possibilidades de senha de um usuário.	A solução é usar senhas fortes, para evitar que seja possível fazer esse tipo de ataque.
Engenharia social	Consiste em um ataque focado em como os humanos funcionam. Exemplos de ataques desse tipo consistem em descobrir dados da vítima (usando redes sociais ou vazamentos na internet), como aniversário, nomes de pets, nomes de parentes e, então, testá-los (ou variações deles) como senha.	Nossa melhor defesa é não usar a mesma senha em todos os lugares e não usar informações pessoais como parte de senhas.

Elaborado especialmente para o curso.

Construindo o **conceito**

O que torna uma senha forte?

Uma senha forte é:

- ✓ geralmente longa, complexa e única;
- ✓ deve incluir uma combinação de letras maiúsculas e minúsculas, números e símbolos.

Reforçando: **evite informações facilmente acessíveis**, como datas de nascimento, nomes de animais de estimação ou sequências simples como “1234”.

TEMPO QUE UM HACKER LEVA PARA DESCOBRIR SUA SENHA POR FORÇA BRUTA

Número de caracteres	Somente números	Letras minúsculas	Letras maiúsculas e minúsculas	Números, letras maiúsculas e minúsculas	Números, letras maiúsculas e minúsculas e símbolos
4	Imediatamente	Imediatamente	Imediatamente	Imediatamente	Imediatamente
5	Imediatamente	Imediatamente	Imediatamente	Imediatamente	Imediatamente
6	Imediatamente	Imediatamente	Imediatamente	1 segundo	5 segundos
7	Imediatamente	Imediatamente	25 segundos	1 minuto	6 minutos
8	Imediatamente	5 segundos	22 minutos	1 hora	8 horas
9	Imediatamente	2 minutos	19 horas	3 dias	3 semanas
10	Imediatamente	58 minutos	1 mês	7 meses	5 anos
11	2 segundos	1 dia	5 anos	41 anos	400 anos
12	25 segundos	3 semanas	300 anos	2 mil anos	34 mil anos
13	4 minutos	1 ano	16 mil anos	100 mil anos	2 milhões de anos
14	41 minutos	51 anos	800 mil anos	9 milhões de anos	200 milhões de anos
15	6 horas	mil anos	43 milhões de anos	600 milhões de anos	15 bilhões de anos
16	2 dias	34 mil anos	2 bilhões de anos	37 bilhões de anos	1 trilhão de anos
17	4 semanas	800 mil anos	100 bilhões de anos	2 trilhões de anos	93 trilhões de anos
18	9 meses	23 mil anos	6 trilhões de anos	100 trilhões de anos	7 quatrilhões de anos

Fonte: HIVE SYSTEMS, 2024. Disponível em: https://www.hivesystems.com/blog/are-your-passwords-in-the-green?utm_source=header
Acesso em: 28 jun. 2024.
Elaborado especialmente para o curso.

Construindo o **conceito**

Métodos de criação de senhas

Use frases: escolha uma frase que seja significativa para você e utilize as iniciais, números e substituições de caracteres para criar uma senha.

Exemplo: “Eu nasci em 1990 no Rio de Janeiro!” pode se tornar “EnE1!9nRdJ!”.

Use um gerador de senhas para criar senhas aleatórias e fortes. Essas ferramentas garantem que suas senhas sejam imprevisíveis e resistentes a ataques de adivinhação.

Dica

Algumas opções de gerenciadores de senha são: LastPass, 1Password, RoboForm. O LastPass disponibiliza um gerador gratuito, confira no link abaixo:
PÁGINA inicial. *Last Pass*, [s.d.]. Disponível em: https://www.lastpass.com/pt/features/password-generator. Acesso em: 21 jun. 2024.

Construindo
o **conceito**

Boas práticas de gerenciamento de senhas

- **Gerenciadores de senhas** podem armazenar e criptografar suas senhas. Eles também podem ajudar a gerar e recuperar senhas complexas quando necessário, facilitando a manutenção de várias senhas fortes.
- **Alterar suas senhas regularmente** pode ajudar a proteger suas contas contra violações de segurança. No entanto, isso deve ser equilibrado com a necessidade de manter senhas que você possa lembrar ou gerenciar.

Colocando em **prática**

Geração de senhas fortes

1. Individualmente, faça um exercício de geração de senhas. Você deve **inventar 10 senhas fortes**. Registre tudo em um documento de texto.

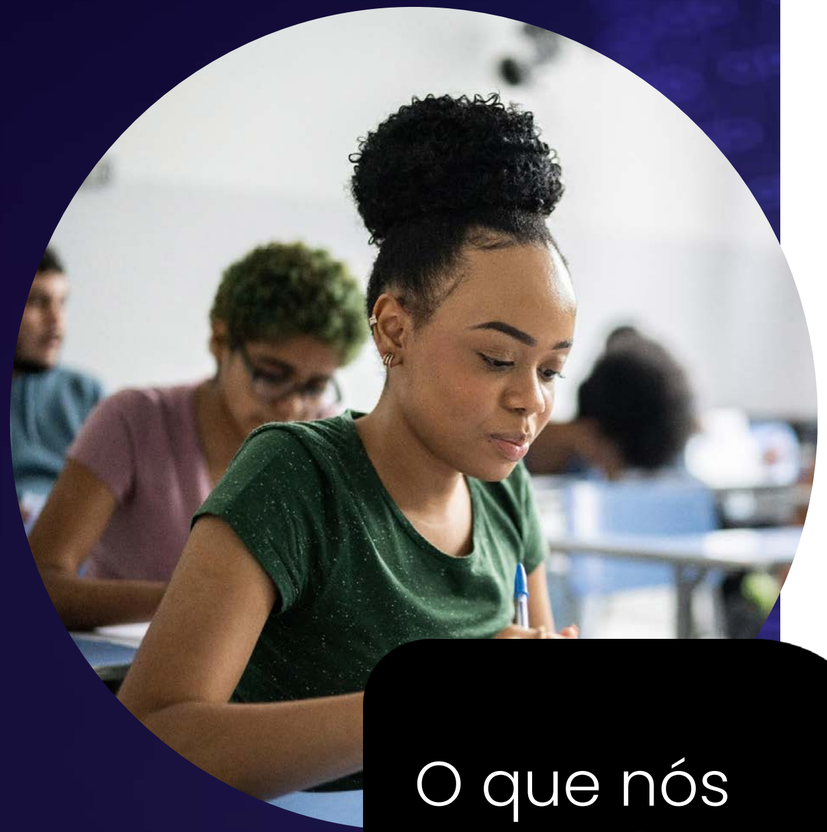
2. Importante! Não use as senhas da atividade nos seus usuários, elas servem apenas para praticar a metodologia.

3. Ao finalizar, envie o documento para o Ambiente Virtual de Aprendizagem (AVA).

Documento de texto

Até o final da aula

Individual



© Getty Images

O que nós **aprendemos hoje?**

Então ficamos assim...

1. Entendemos como senhas funcionam, sua importância e quais as estratégias de ataques envolvendo senhas;

2. Destacamos porque é crucial criar senhas fortes para a segurança on-line e aprofundamos métodos eficazes para sua geração, incluindo o uso de frases de senha, combinações de caracteres variados, como letras maiúsculas, minúsculas, números e símbolos;

3. Discutimos sobre as melhores práticas para administrar as palavras-chave, como o emprego de gerenciadores de senhas para armazenar e organizar essas informações de forma segura.

Saiba mais

Cansado de ter que criar senhas novas a todo momento? Descubra se seus dados já foram expostos em algum vazamento on-line com essa ferramenta gratuita:

PÁGINA inicial. *Haveibeenpwned*, [s.d.]. Disponível em: https://haveibeenpwned.com/. Acesso em: 21 jun. 2024.

Referências da aula

HIVE SYSTEMS, 2024. Disponível em: https://www.hivesystems.com/blog/are-your-passwords-in-the-green?utm_source=header. Acesso em: 28 jun. 2024.

MASCARENHAS NETO, P. T.; ARAÚJO, W. J. *Segurança da Informação*: uma visão sistêmica para implantação em organizações. João Pessoa: UFPB, 2019. Disponível em: http://www.editora.ufpb.br/sistema/press5/index.php/UFPB/catalog/book/209. Acesso em: 21 jun. 2024.

Identidade visual: Imagens © Getty Images

Educação Profissional Paulista

Técnico em **Ciência de Dados**

Secretaria da Educação

SÃO PAULO
GOVERNO DO ESTADO