

# SENHAS

- \* Como podem ser descobertas
- \* Riscos principais
- \* Cuidados a serem tomados



# Sua senha pode ser descoberta:

- Quando usada em:
  - \* Computadores infectados
  - \* Computadores Invadidos
  - \* Sites falsos (phishing)
- Por meio de tentativas de adivinhação
- Ao ser capturada enquanto trafega na rede
- Por meio de acesso ao arquivo onde foi armazenada
- Com uso de técnicas de engenharia social
- Pela observação da movimentação:
  - \* Dos seus dedos no teclado
  - \* Dos cliques do mouse em teclados virtuais





# RISCOS PRINCIPAIS

**HACKED**

**SENHAS**

## Riscos principais (1/4)

\* Da posse da sua senha um invasor pode:

- Acessar a sua conta de correio eletrônico e:

- Ler e/ou apagar seus e-mails
- Furtar sua lista de contatos e enviar e-mails em seu nome
- Pedir o reenvio de senhas e outras contas
  - e assim conseguir acesso a elas
- Trocar a sua senha
  - dificultando que você acesso novamente sua conta
- Enviar mensagens contendo:
  - spam
  - boatos
  - phishing
  - códigos maliciosos



**SENHAS**

## Riscos principais (2/4)

\* Da posse da sua senha um invasor pode:

- Acessar o seu computador e:

- Apagar seus arquivos
- Obter informações sensíveis
- Instalar códigos e serviços maliciosos
- Usar o computador para esconder a identidade do invasor



**SENHAS**

## Riscos principais (3/4)

\* Da posse da sua senha um invasor pode:

- Acessar sua rede social e:

- Denegrir a sua imagem
- Explorar a confiança de seus amigos
- Tornar públicas informações privadas
- Trocar a sua senha, dificultando que você acesse seu perfil
- Enviar mensagens em seu nome



**SENHAS**

## Riscos principais (4/4)

\* Da posse da sua senha um invasor pode:

- Acessar sua conta bancária
- Acessar o seu site de comércio eletrônico e:
  - Alterar informações de cadastro
  - Fazer compras em seu nome
  - Verificar informações sobre suas compras interiores
- Acessar seu dispositivo móvel e:
  - Furtar sua lista de contatos e suas mensagens
  - Acessar e/ou copiar fotos e vídeos
  - Bloquear o acesso ao dispositivo
  - Apagar os dados armazenados no dispositivo



**SENHAS**

# Cuidados a serem tomados



**SENHAS**

# Elaboração de senhas(1/2)

\* Evite usar:

- Dados pessoais:

- Nome, sobrenome
- Contas de usuário, datas
- Números de documentos, telefones ou placas de carros

- Dados disponíveis em redes sociais e páginas web:

- Sequências de teclado

- Palavras presentes em listas publicamente conhecidas

- Músicas, times de futebol
- Personagens de filmes
- Dicionários de diferentes idiomas



**SENHAS**

## Elaboração de senhas(2/2)

\* Use:

- Números aleatórios:
  - Quanto mais ao acaso forem os números, melhor
- Grande quantidade de caracteres
  - Quanto mais longa sua senha, melhor
- Diferentes tipos de caracteres
  - Quanto mais “bagunçada” for a sua senha, melhor



**SENHAS**

## Uso de senhas (1/3)

### \* Não exponha suas senhas

- Certifique-se de não estar sendo observado ao digitá-las
- Não as deixem anotadas em locais onde possam ver:
  - Papel sobre a mesa ou colado no monitor
- Evite digitá-las em dispositivos de terceiros
- Não forneça suas senhas para outras pessoas



**SENHAS**

## Uso de senhas (2/3)

### \* Evite:

- Salvar as suas senhas no navegador web
- Usar opções, como:
  - “Lembre-se de mim”
  - “Continuar conectado”
- Usar a mesma senha para todos os serviços que acessa
- Não use senhas de acesso profissional para acessar assuntos pessoais (e vice-versa)

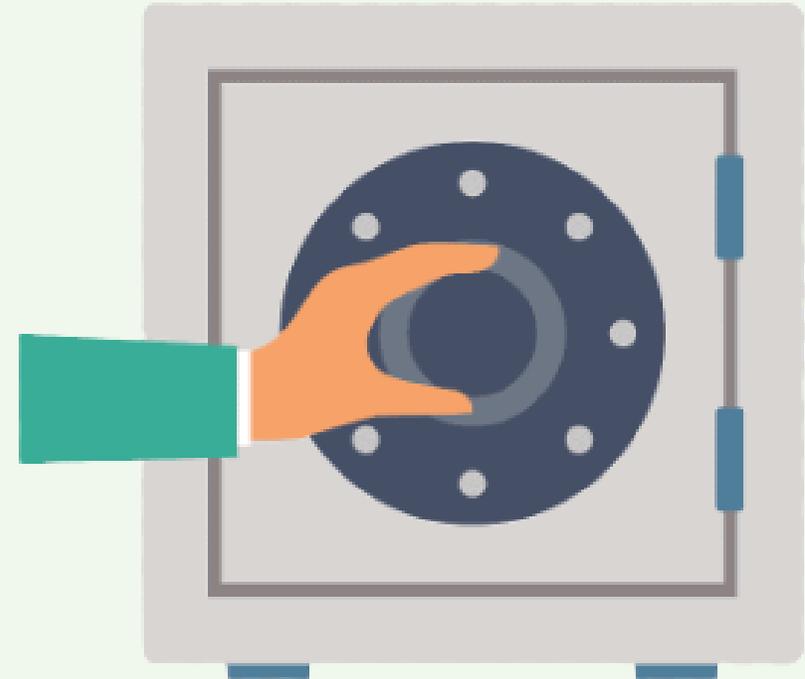


**SENHAS**

## Uso de senhas (3/3)

\* Armazene suas senhas de forma segura:

- Use programas gerenciadores de senhas
- Anote-as em um papel e guarde em local seguro
- Grave-as em um arquivo criptografado

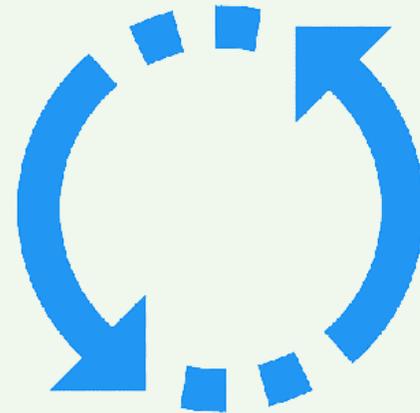


**SENHAS**

# Alteração de senhas

\* Altere suas senhas:

- Imediatamente caso tenha sido descoberta
- Rapidamente se perder um computador onde elas estejam gravadas
- Regularmente: nos demais casos



**SENHAS**

## Recuperação de senhas (1/2)

\* Configure opções de recuperação de senhas:

- Um endereço de e-mail alternativo
- Uma pergunta de segurança
- Uma dica de segurança
- Um número de telefone celular

\* Ao usar perguntas de segurança:

- Evite escolher questões cujas respostas sejam facilmente adivinhadas
- Uma pergunta de segurança
- Procure criar suas próprias questões (de preferência com respostas falsas)



## Recuperação de senhas (2/2)

- \* Ao usar dicas de segurança, escolha aquelas que sejam:
  - Vagas o suficiente para que ninguém consiga descobri-las
  - Claras o bastante para que você consiga entendê-las
- \* Ao solicitar o envio de suas senhas por e-mail:
  - Procure alterá-las o mais rápido possível
  - Cadastre um e-mail que você acesse regularmente



**Semef**  
Secretaria Municipal



Prefeitura de  
**Manaus**