Manual de Segurança Digital

FASCÍCULO

PROTEÇÃO DE CONTAS NAS REDES SOCIAIS

Secretaria de Segurança da Informação e Cibernética/GSI/PR

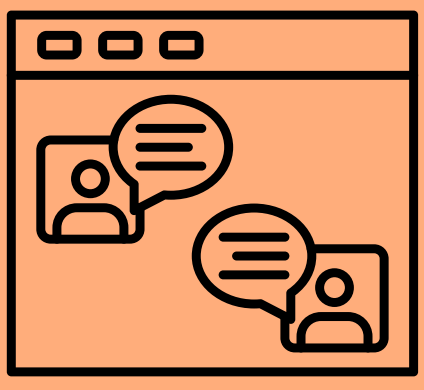
2023

NA ATUALIDADE É DIFÍCIL CONHECER UMA PESSOA OU EMPRESA QUE NÃO ESTEJA PRESENTE EM MÍDIAS SOCIAIS, POIS SÃO MEIOS ESSENCIAIS PARA INTERAGIR COM PESSOAS E AGREGAR RELACIONAMENTOS INTERPESSOAIS E PROFISSIONAIS.

Tópicos abordados:

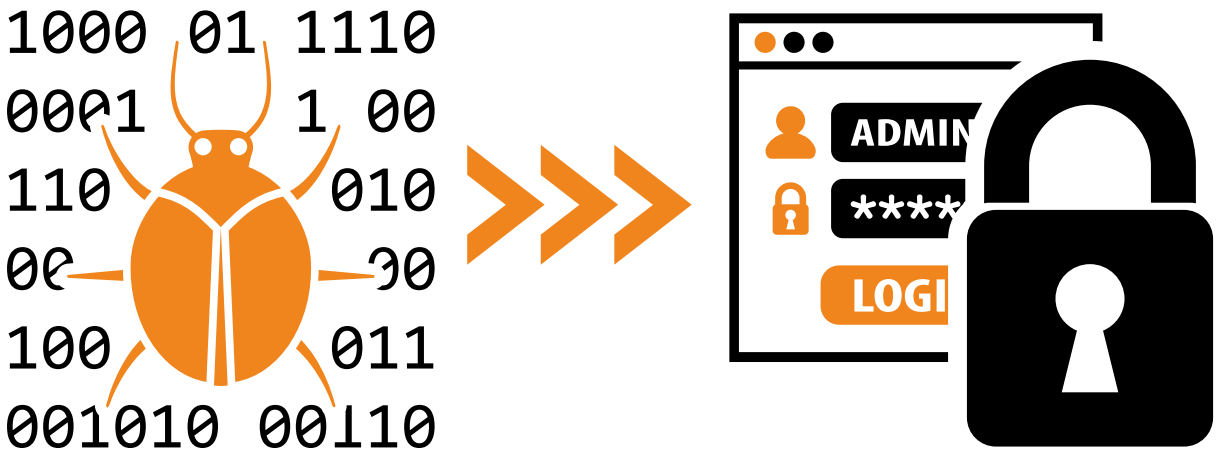
- como os cibercriminosos conseguem acesso a conta;
- dicas do que fazer:
  - criar senha forte;
  - usar uma senha para cada *site*;
  - ativar a autenticação de dois fatores;
  - configurar a opção de receber alertas de *login* em sua conta;
  - sair da Rede Social em computadores públicos;
  - escolher amigos de confiança;
  - observar as extensões e/ou programas instalados.

O aumento da popularidade em perfis nas redes sociais aumenta o perigo de cair em golpes *online* praticados por cibercriminosos. Sendo assim, aprender a utilizar esses canais com segurança é relevante para manter sua privacidade e confiabilidade nas informações disponibilizadas.



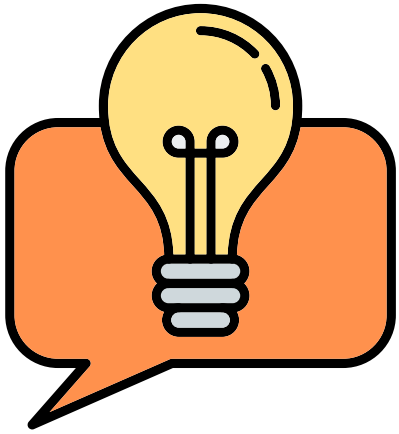
COMO OS CIBERCRIMINOSOS CONSEGUEM ACESSO A CONTA

Normalmente, os cibercriminosos conseguem acesso a uma conta porque a senha é fácil, pode ter sido utilizada em outro serviço ou vazou. Existe, também, a possibilidade de algum aplicativo malicioso que esteja conectado a sua conta ter permissão de acessar seu perfil e mensagens, tendo acesso a dados pessoais ou mesmo a sua senha.



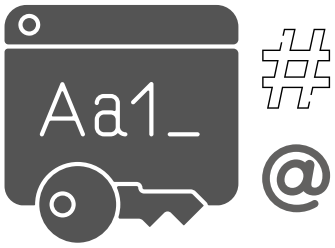
DICAS DO QUE FAZER

Os usuários podem observar algumas dicas básicas, do que fazer e do que não fazer, para manter a sua conta segura (veja as dicas a partir da próxima página).



CRIAR SENHA FORTE

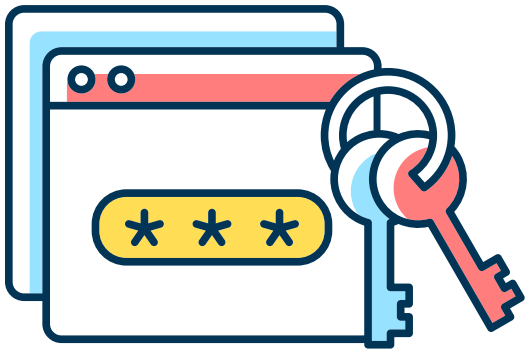
Quanto maior for a senha e quanto maior a variedade de caracteres (letras minúsculas e maiúsculas, números e caracteres especiais, como !@#), maior a segurança contra ataques de sequestro de senha.



A senha não deve incluir nenhuma informação pessoal do usuário, como endereço ou número de telefone. Também é melhor não incluir nenhuma informação que possa ser acessada nas redes sociais, como nomes de crianças ou animais de estimação, e não deve conter letras ou números consecutivos.

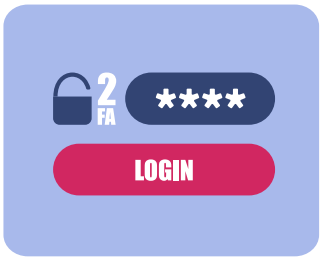
USAR UMA SENHA PARA CADA *SITE*

É uma boa prática utilizar senhas diferentes para cada conta. Utilize um gerenciador de senhas para ajudar a guardar as senhas de aplicativos e *sites* que você gerou ou criou. Existem diversas opções gratuitas e pagas, só é preciso entender qual delas corresponde a suas expectativas.



ATIVAR A AUTENTICAÇÃO DE DOIS FATORES

Habilite a autenticação do dispositivo, a autenticação de dois fatores (2FA). Para proteção máxima, habilite o uso de autenticação biométrica (face ou impressão digital).

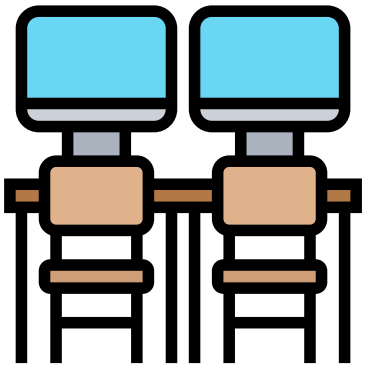


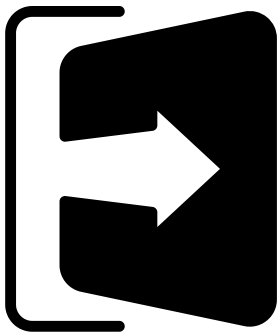
CONFIGURAR A OPÇÃO DE RECEBER ALERTAS DE *LOGIN* EM SUA CONTA

Esta configuração é relevante para alertar quando uma pessoa acessar sua conta; caso avalie que houve acesso indevido, faça alteração de senha para evitar problemas em sua conta.

SAIR DA REDE SOCIAL EM COMPUTADORES PÚBLICOS

Caso tenha que acessar a rede social em um computador que não seja o seu próprio, é relevante que faça *logout* (clique em Sair) quando não for mais usar sua conta. Dessa forma, não corre o risco de a próxima pessoa que usar o computador utilizar sua conta e fazer publicações fazendo-se passar por você.





ESCOLHER AMIGOS DE CONFIANÇA

A maioria dos aplicativos de redes sociais oferecem a opção de escolher um número de amigos para ficarem cada um com um código de segurança diferente. Sendo assim, se você perder o acesso à conta, poderá pedir o código a um dos amigos e conseguir acessar seu perfil, mesmo que alguém malicioso tenha mudado sua senha.

OBSERVAR AS EXTENSÕES E/OU PROGRAMAS INSTALADOS.

Não menos importante, verifique extensões do seu navegador e programas mal-intencionados que podem existir no dispositivo computacional que esteja utilizando.