PHISHX

Como manter seus acessos seguros

Boas senhas são o começo

Boa parte de nossa segurança começa quando criamos e mantemos senhas seguras e protegidas:

• Uma senha forte deve estar mais próxima de uma frase do que de uma palavra, e seu comprimento deve ser o maior possível.

• Uma senha forte deve ser uma combinação de caracteres, letras maiúsculas, letras minúsculas e números.

• Primeiro, escreva uma senha aleatória e depois, letra por letra, continue alterando o tipo de cada caractere.

• Senhas são individuais, temporárias e únicas, não repita senhas ou compartilhe com ninguém.

• Para manter sua identidade online segura e protegida, você precisa continuar alterando suas senhas em intervalos regulares.

Não execute arquivos desnecessários

Para ter uma senha segura, evite senhas com:

• Palavras comum: qualquer palavra ou combinação que possa ser encontrada em um dicionário.

• Pequenas variações: tenha cuidado ao usar variações muito leves de palavras ou nomes comuns.

• Contexto: não use senhas que reflitam algo sobre você, como o nome de pessoas ou lugares que você conhece.

• Sequência do teclado: esqueça o uso de uma sequência baseada em letras adjacentes ao teclado.

• Similar ou a mesma senha: não mantenha a mesma senha para todas as suas contas.

Atualize o seu perfil

Verifique sempre suas informações de contato estão atualizadas, para que todos os provedores de seus serviços possam entrar em contato, através de notificações ou processos de reativação de acessos, com você de forma rápida, segura e eficiente.

É essencial que você verifique suas informações de contato periodicamente e mantenha-as atualizadas se fizer alterações no seu endereço, telefone ou e-mail.

Ao receber uma notificação de novo acesso que não tenha feito, acesse o portal do seu provedor para entender o que aconteceu e, caso necessário, atualizar sua senha e demais configurações.

Gerencie suas senhas

Tal como dependemos de nossa agenda para lembrar os aniversários e contatos, use um gerenciador de senhas em seus dispositivos para manter suas senhas complexas ainda mais seguras.

Além de armazenar as suas senhas, esses aplicativos podem ajudar a criar senhas fortes aleatórias, de acordo com as dicas e padrões de segurança, bem como lembrar você de atualizar as mesmas com frequência.

Outro ponto adicional é ter assinaturas para identificar se alguma conta ou senha pessoal sua foi descoberta, ou se houveram problemas com algum serviço que você utiliza, informando que você deve trocar suas senhas e acessos.

Múltiplos Fatores

A autenticação deve ser multifatorial, por exemplo quando usamos dois fatores (2FA) ou mais (MFA), para aumentar a segurança de nossos acessos.

Você deve habilitar autenticação em múltiplos fatores em todos os aplicativos, serviços e sistemas que você utilizar no seu trabalho e vida pessoal.
Os fatores podem incluir o seguinte:

• Uma informação que só você conhece: sua senha segura e única.

• Algo que você possui: um aplicativo gerador de código em seu celular.

• Algo que você é: seu rosto ou impressão digital.

• Onde você está: sua localização por um GPS ou seu ponto de acesso à rede.

Não fique logado

Tão importante quanto acessar de forma segura, é também terminar o seu acesso quando não for mais usar, saindo do aplicativo ou sistema.

Quando usar um dispositivo compartilhado, lembre-se de sair das suas contas e evite marcar a caixa "Mantenha-me conectado" ao efetuar o acesso.

Caso fique longe do seu dispositivo, mas retornará, bloqueie a tela para que ninguém consiga acessar os dados sem realizar a autenticação segura