Kennedy Sevilha

Dicas sobre Cibersegurança

Proteção Simplificada.

Sumario

Top 10 Dicas

Use Senhas Fortes

O que é uma senha forte?

Uma senha forte deve ter pelo menos 12 caracteres, incluindo letras maiúsculas e minúsculas, números e símbolos. Evite usar informações pessoais como datas de nascimento ou nomes.

- Em vez de usar "123456" ou "senha123", crie uma senha como "S3gur@2024!".

Ative a Autenticação em Dois Fatores (2FA)

O que é 2FA?

A autenticação em dois fatores adiciona uma camada extra de segurança, exigindo não só a senha, mas também um código enviado para seu telefone ou email.

- Ao fazer login em seu email, além da senha, você precisará inserir um código enviado por SMS.

Cuidado com Phishing

O que é phishing?

Phishing é uma tentativa de obter informações pessoais através de emails ou mensagens que parecem ser de fontes confiáveis.

- Se você receber um email do seu banco pedindo para confirmar seus dados clicando em um link, não clique. Entre em contato diretamente com o banco para verificar a autenticidade.

Mantenha Seus Softwares Atualizados

Por que atualizar é importante?

As atualizações corrigem falhas de segurança que podem ser exploradas por hackers.

- Sempre instale as atualizações do sistema operacional, navegadores e aplicativos assim que disponíveis.

Use Redes Wi-Fi Seguras

O que são redes seguras?

Evite redes Wi-Fi públicas para acessar informações sensíveis. Se necessário, use uma VPN (Rede Virtual Privada).

- Ao usar Wi-Fi público em um café, evite acessar seu banco online. Use a VPN para criptografar sua conexão.

Desconfie de Anexos e Links Desconhecidos

Por que ser cauteloso?

Anexos e links podem conter malware que infecta seu dispositivo.

- Antes de abrir um anexo de um email inesperado, confirme com o remetente se ele realmente enviou aquele arquivo.

Faça Backup Regularmente

O que é backup?

Backup é a cópia de segurança dos seus dados importantes para evitar perdas em caso de ataques ou falhas.

- Use um disco externo ou serviços de nuvem como Google Drive para salvar cópias de fotos, documentos e outros arquivos importantes.

Proteja seus Dispositivos com Senhas e PINS

Por que proteger dispositivos?

Bloquear seus dispositivos com senhas impede o acesso não autorizado, mesmo que eles sejam perdidos ou roubados.

- Ative o bloqueio por PIN ou impressão digital em seu smartphone.

Cuidado com o Que Compartilha nas Redes Sociais

Por que ser cuidadoso?

Informações pessoais divulgadas nas redes sociais podem ser usadas por criminosos para roubo de identidade.

- Evite compartilhar sua localização em tempo real ou detalhes específicos sobre sua rotina diária.

Esteja Sempre Informado

Por que se informar?

A cibersegurança está em constante evolução. Manter-se atualizado sobre novas ameaças e melhores práticas é crucial.

- Siga blogs de tecnologia e segurança, como o blog da Kaspersky ou da Norton, para se manter informado.