PHISHX

Dicas de cibersegurança

Dicas para proteger suas contas e informações

A segurança da informação é um tópico cada vez mais relevante em nossos dias, especialmente à medida que as ameaças cibernéticas continuam a evoluir e se tornar cada vez mais sofisticadas.

A exposição de informações sensíveis pode ter um impacto significativo nas organizações, como perda financeira, dano à reputação e violação de privacidade.

Portanto, é fundamental estar cientes dos riscos cibernéticos e implementar medidas eficazes de segurança da informação. Aqui fornecemos as principais dicas e práticas recomendadas para proteger informações e sistemas valiosos, ajudando a garantir a segurança dos seus dados.

Você está utilizando as boas práticas para senhas?

.Algumas vezes, acabamos esquecendo que as boas senhas são aquelas que não se relacionam com nosso cotidiano. Precisamos ter muito cuidado para que nossas senhas não sejam fáceis de adivinhar.

Por isso, é importante criar senhas fortes, incluindo letras maiúsculas e minúsculas, números e caracteres especiais. Além disso, é recomendável não usar senhas óbvias, como datas de nascimento ou nomes de familiares.

Outra dica importante é não utilizar as mesmas senhas em várias contas, pois isso pode aumentar o risco de comprometimento dessas contas caso uma senha seja comprometida.

Não se esqueça de fazer todas atualizações

As atualizações são projetadas para corrigir falhas de segurança conhecidas, melhorar a estabilidade e adicionar recursos novos e importantes.

Dessa forma, quando os sistemas e softwares não são atualizados, as vulnerabilidades conhecidas podem ser exploradas por cibercriminosos, resultando em perda de dados, roubo de informações e violação de privacidade.

As atualizações também podem melhorar a segurança do sistema, adicionando novas camadas de proteção, melhorando a criptografia de dados e fortalecendo os controles de acesso.

Treine para pensar antes de clicar

Muitas vezes, quando estamos conferindo e-mails ou navegando pela internet, ficamos distraídos e acabamos clicando sem pensar em algum link ou anexo desconhecido. Isso pode ser um grande risco, pois podemos estar fazendo download de um sistema malicioso ou até mesmo permitindo que cibercriminosos acessem nossas informações.

Esse tipo de ataque se chama phishing e é uma técnica usada por criminosos cibernéticos para enganar pessoas para revelar informações confidenciais, como senhas, informações bancárias e detalhes de cartões de crédito. Geralmente são realizados por meio de mensagens fraudulentas ou sites falsos que parecem legítimos.

Seus dados estão sempre desprotegidos!

.Desenvolva um senso de ceticismo em relação à proteção dos seus dados. Infelizmente, podemos estar em risco em qualquer lugar, inclusive quando utilizamos redes públicas de internet.

Por isso, é essencial ativar os mecanismos de autenticação multifatorial. Eles funcionam exigindo não apenas uma senha, mas também uma segunda forma de autenticação, como um código enviado por mensagem de texto ou um token de segurança.

Mantenha seu celular protegido

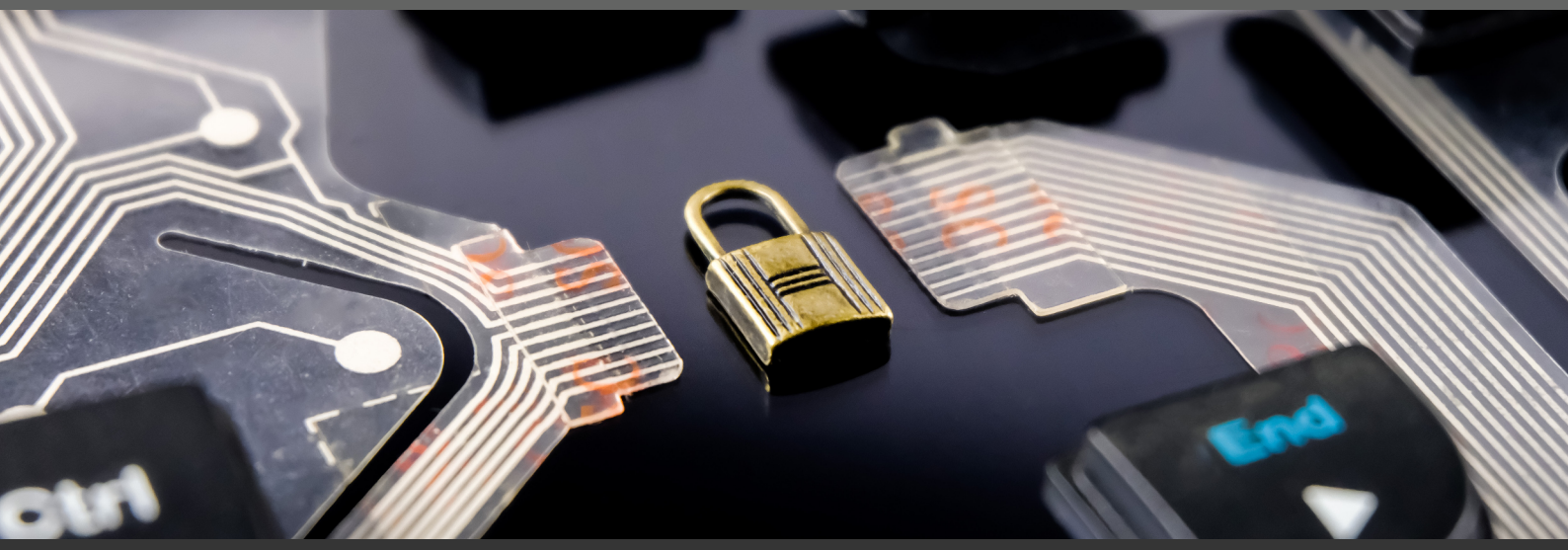
.Dispositivos móveis, como smartphones e tablets, são cada vez mais utilizados para acessar informações sensíveis, como e-mails corporativos, dados bancários e informações de clientes.

Uma das medidas mais importantes é usar senhas fortes para proteger o acesso ao dispositivo, bem como para bloquear aplicativos específicos com informações sensíveis. Além disso, é importante criptografar dados sensíveis, como arquivos financeiros e senhas, para impedir o acesso não autorizado em caso de perda ou roubo do dispositivo.

Como manter sua mesa limpa

Suas anotações, arquivos e documentos podem oferecer muitas informações para olhos atentos. Por isso, é essencial evitar guardar senhas em papéis e, até mesmo, manter sua tela virada para locais com muito movimento.

Tudo isso pode ser uma forma de comprometer informações sensíveis, que podem ser utilizadas para acessar contas e também comprometer a sua privacidade.



PHISHX | phishx.io

Redes Sociais