PHISHX

Como se proteger contra mensagens suspeitas

Comunicação no mundo digital

No mundo digital em que vivemos hoje, a comunicação por meio de mensagens eletrônicas tornou-se uma parte essencial da nossa vida cotidiana. No entanto, com o aumento do uso de e-mails, mensagens de texto e redes sociais, também aumentou a presença de mensagens externas e suspeitas que buscam roubar informações pessoais, disseminar golpes ou até mesmo instalar softwares maliciosos em nossos dispositivos.

Então vamos aprender um pouco mais sobre como as pessoas podem identificar essas mensagens. Dessa forma, você pode se proteger das ameaças cibernéticas e garantir sua segurança e privacidade.

O que são mensagens externas e suspeitas?

Mensagens externas são comunicações não solicitadas que podem ser enviadas por e-mail, mensagens de texto, redes sociais ou outras plataformas digitais.

Essas mensagens geralmente têm a intenção de enganar as pessoas, fazendo com que elas sejam induzidas a fornecer informações confidenciais, clicar em links maliciosos ou baixar arquivos infectados.

Algumas dessas mensagens podem se passar por instituições financeiras, empresas conhecidas, agências governamentais ou até mesmo contatos pessoais. A seguir, apresentamos algumas dicas para identificar essas mensagens e evitá-las.

Por que precisamos verificar o remetente?

Uma das maneiras mais fáceis de identificar mensagens suspeitas é verificar o remetente da mensagem. Normalmente, essas mensagens possuem endereços de e-mail estranhos ou diferentes, que podem conter erros de ortografia ou parecerem similares a endereços legítimos, mas com pequenas alterações.

Por exemplo, um e-mail de phishing que se passa por uma empresa conhecida como "amazon-support@example.com" pode ser um indicativo de uma mensagem suspeita. Sempre verifique cuidadosamente o endereço do remetente antes de abrir a mensagem ou clicar em links.

No caso de mensagens de texto ou por aplicativos digitais, verifique se o número corresponde ao da pessoa. Atualmente, é muito comum golpes que buscam se passar por pessoas que trocaram de número de telefone.

Desconfie de mensagens urgentes e ameaçadoras

Mensagens que tentam criar um senso de urgência ou ameaçam consequências negativas caso você não tome uma ação imediata são sinais claros de que algo está errado.
Essas táticas são frequentemente usadas por golpistas para pressionar os destinatários a agir impulsivamente, sem pensar nas possíveis consequências.

Empresas e instituições legítimas raramente enviam mensagens urgentes e ameaçadoras. Portanto, se você receber uma comunicação assim, é melhor desconfiar e verificar sua autenticidade antes de agir.

Como identificar mensagens falsas

Mensagens falsas podem conter erros de ortografia, gramática ou informações inconsistentes. Preste atenção ao texto da mensagem, pois muitos golpistas não se preocupam em revisar suas mensagens cuidadosamente.

Além disso, esteja atento a solicitações de informações pessoais, como senhas, números de cartão de crédito, dados bancários, transferências monetárias ou outras informações confidenciais. Instituições legítimas raramente solicitam esse tipo de informação por e-mail.

Não clique em links ou faça download de anexos suspeitos

Uma das táticas mais comuns usadas em golpes digitais é o uso de links maliciosos ou anexos infectados. Esses links podem levar você a sites de phishing que coletam suas informações pessoais ou podem instalar malware em seu dispositivo.

Por isso, nunca clique em links ou faça download de anexos de mensagens suspeitas, a menos que você esteja absolutamente certo de sua origem e segurança. Mesmo assim, é recomendado digitá-los manualmente na barra de endereços do navegador.

Verifique a autenticidade das mensagens

Se você receber uma mensagem que parece suspeita, entre em contato com a empresa, instituição ou pessoa que supostamente enviou a mensagem por meio de um canal oficial conhecido.

Por exemplo, se você recebeu um e-mail de uma empresa que solicita informações pessoais, entre no site oficial da empresa, evitando clicar em links do e-mail, e procure um canal de suporte ou contato para verificar se a mensagem é legítima.

Utilize ferramentas de segurança

Muitas vezes, é difícil identificar mensagens falsas apenas com o olho nu, especialmente porque os golpistas estão sempre aprimorando suas táticas. Dessa maneira, é essencial contar com ferramentas de segurança confiáveis para proteger-se contra ameaças cibernéticas. Mantenha um software antivírus atualizado em seu dispositivo e utilize extensões de segurança em seu navegador para ajudar a bloquear sites maliciosos.

PHISHX | phishx.io

Redes Sociais