PHISHX

5 regras para evitar ataques de Phishing

Phishing

A cada ano, milhões de pessoas ao redor do mundo são vítimas de ataques de phishing. Esses golpes cibernéticos, que tentam roubar informações pessoais como senhas, números de cartão de crédito e dados sensíveis, estão se tornando cada vez mais sofisticados. No entanto, com algumas regras simples, você pode se proteger e evitar cair em armadilhas.

Regra 1: Verifique se você se cadastrou e já recebeu mensagens desse canal de comunicação

Uma das primeiras coisas a considerar ao receber uma mensagem suspeita é verificar se você realmente se cadastrou para receber comunicações do remetente. Muitas vezes, os ataques de phishing usam nomes de empresas conhecidas para enganar as vítimas.

Se você nunca se inscreveu para receber e-mails ou mensagens de uma determinada empresa, isso pode ser um sinal claro de que a mensagem é fraudulenta. As empresas legítimas só enviam comunicações para aqueles que se inscreveram ou têm algum tipo de relacionamento existente com a empresa.

Por isso, é importante manter um registro das empresas e serviços para os quais você se inscreveu. Isso pode ser feito usando uma planilha simples ou um aplicativo de gerenciamento de senhas.

Se você começar a receber mensagens de uma nova empresa que você não reconhece, investigue se outras pessoas estão recebendo mensagens semelhantes. Muitas vezes, uma rápida pesquisa online pode revelar se a mensagem é parte de uma campanha de phishing.

Regra 2: Identifique e reconheça a origem e o remetente

Um dos métodos mais comuns de phishing envolve a falsificação de endereços de e-mail e nomes de remetentes. Verificar a legitimidade do remetente pode ajudar a identificar mensagens fraudulentas antes que você seja vítima.

Uma boa dica é inspecionar o endereço de e-mail do remetente cuidadosamente. Muitos golpistas usam endereços que são muito parecidos com os legítimos, mas com pequenas variações, como uma letra trocada ou um domínio diferente.

Se você não tiver certeza sobre a autenticidade de uma mensagem, entre em contato diretamente com a empresa ou pessoa por meio de um canal oficial, como o site oficial da empresa ou um número de telefone conhecido.

Regra 3: Verifique se a mensagem está dentro do contexto e conteúdo esperado

Mensagens de phishing frequentemente contêm informações que estão fora do contexto esperado ou têm um conteúdo que não faz sentido. Verificar se a mensagem faz sentido no contexto do seu relacionamento com o remetente pode ajudar a identificar fraudes.

Mensagens que solicitam informações pessoais ou financeiras de forma inesperada ou fora do contexto são sinais de alerta de possíveis tentativas de phishing. Se a mensagem parecer estranha ou fora do comum, é melhor ser cauteloso.

Para identificar ataques de phishing, compare a mensagem suspeita com outras comunicações que você recebeu do mesmo remetente anteriormente. Se a mensagem for inconsistente ou parecer diferente das anteriores, pode ser um indício de phishing.

Lembre-se de ter atenção e desconfiar de urgências. Mensagens que exigem ação imediata ou ameaçam com consequências se não houver resposta rápida são frequentemente usadas por golpistas para pressionar as vítimas a agir sem pensar.

Regra 4: Verifique links ou anexos antes de clicar

Links e anexos são ferramentas comuns usadas em ataques de phishing para distribuir malware ou redirecionar as vítimas para sites falsos. Por esse motivo, verificar a autenticidade desses elementos antes de clicar pode evitar muitos problemas.

Clicar em links ou baixar anexos de fontes não verificadas pode resultar na instalação de malware em seu dispositivo ou na revelação de informações pessoais em um site fraudulento.

Antes de clicar, passe o mouse sobre o link para ver o URL completo. Verifique se o endereço é familiar e legítimo. URLs encurtadas ou estranhas são sinais de alerta.

Além disso, existem serviços online que permitem verificar a segurança de um link. Use essas ferramentas para garantir que o link não leva a um site malicioso.

Nunca abra anexos de remetentes desconhecidos. Mesmo se o remetente for conhecido, se o anexo for inesperado ou suspeito, confirme diretamente com o remetente antes de abrir.

Regra 5: Se ainda houver dúvidas, solicite a opinião de um colega ou do time responsável na sua organização

Se, depois de seguir todas as etapas anteriores, você ainda estiver em dúvida sobre a autenticidade de uma mensagem, não hesite em buscar ajuda. Compartilhar suas preocupações com um colega ou com a equipe de segurança da informação pode fornecer uma segunda opinião valiosa.

O trabalho em equipe e a comunicação aberta são essenciais para manter a segurança cibernética. Outras pessoas podem ter mais experiência ou ferramentas para verificar a autenticidade de uma mensagem suspeita.