TRÊS DICAS PARA EVITAR E-MAILS DE PHISHING E ATAQUES DE RANSOMWARE

Sejam massacres de grande proporções ou campanhas menores e mais direcionadas, todos os ataques bem-sucedidos de phishing e de ransomware com base em e-mail são perturbadores e danosos em algum nível. A simples realidade é que eles dependem de erro humano: para que os ataques cibernéticos tenham êxito, alguém, em algum lugar, precisa morder a isca. Os criminosos cibernéticos utilizam técnicas de engenharia social — algumas básicas e outras bastante sofisticadas — para manipular as emoções humanas e provocar uma resposta.

Às vezes, pode ser bastante desanimador, visto que nós, os alvos, precisamos estar certos o tempo todo, enquanto os atacantes só precisam estar certos uma vez. Contudo, a boa notícia é que pequenos passos podem vencer grandes distâncias no que se refere à proteção de dados, dispositivos e sistemas, no trabalho e em casa. Veja a seguir três dicas simples e práticas de conscientização quanto à segurança cibernética que você pode usar para identificar e evitar e-mails maliciosos:

Nº1 - Deixe de lado a leitura rápida e comece a estudar

Nós recebemos tantos e-mails que nos condicionamos a percorrer as mensagens com apenas um passar de olhos e a tomar decisões rápidas. Porém, ao fazermos isso, corremos riscos desnecessários. Pode haver indícios na mensagem, tanto na superfície quanto um pouco mais profundamente, que sirvam de alerta sobre coisas suspeitas. Por exemplo:

- **Endereços “De”, URLs e links incorporados podem se passar pelo que não são.** Não confie nesses itens só pela aparência (mesmo que um nome, logotipo ou outras características pareçam familiar e segura). No seu computador, posicione o cursor do mouse sobre esses elementos de conteúdo e examine a informação que aparece (frequentemente será exibido o verdadeiro destino de um endereço Web na parte inferior esquerda da janela do navegador). Em dispositivos móveis, use um “pressionamento longo” ou um “clique longo” e examine a informação da janela que aparecer. Se houver alguma discrepância entre o que você espera ver e o que realmente for apresentado, mantenha distância.
- **O conteúdo ou o tópico de uma mensagem pode não ser muito correto ou não ser totalmente relevante para você.** Esteja alerta caso o tom de um e-mail de um colega, amigo ou parente parecer inadequado ou simplesmente não “soar como ele”. Da mesma forma, certifique-se de questionar o recebimento de uma fatura ou notificação de envio que não faça sentido com base no seu histórico de pedidos. Leia atentamente o que está escrito; não pule os detalhes.
- **Erros ortográficos e gramaticais podem ser indícios de que o e-mail não vem de uma fonte confiável.** Isso é particularmente verdadeiro no caso de mensagens que parecem ser de uma pessoa ou organização idônea e bem conhecida.

Em geral, qualquer e-mail não solicitado — ou seja, qualquer e-mail que você não estava esperando receber — deve ser examinado com cuidado. Você deve estar **especialmente atento a qualquer e-mail que pareça ter sido criado para provocar**

uma resposta emocional — medo, surpresa, entusiasmo, preocupação — e que insista que você responda ou aja de alguma forma (clicar em um link, fazer o download de um arquivo, confirmar/alterar uma senha, etc.).

Nº2 - Pense bem

Após ler o e-mail, dê a si mesmo um tempo para assimilá-lo. Você deve se dar a oportunidade de agir de maneira ponderada em vez de apenas reagir imediatamente. Para conseguir deixar o hábito de ler superficialmente e reagir imediatamente, faça a si próprio algumas perguntas sobre qualquer e-mail que solicite uma resposta ou ação que possa comprometer sistemas, dispositivos ou dados confidenciais.

Por exemplo:

- *Eu estava esperando essa mensagem?* – Se a resposta for "não", faça mais perguntas.
- *Esse e-mail faz sentido?* – Se o tom parece estranho ou se as informações fornecidas não fazem sentido, pode muito bem ser phishing.
- *Eu estou sendo pressionado a agir precipitadamente ou por medo?* – Caso afirmativo, é um indício muito importante.
- *Isso parece bom demais para ser verdade?* – Se o que você está lendo é inacreditável, provavelmente é phishing.
- *E se for um e-mail de phishing?* – Esta é uma excelente pergunta a se fazer porque ela pode ajudá-lo a antever tudo o que pode acontecer caso você esteja lidando com um ataque de phishing. Você pode estar fazendo download de algum malware que possa corromper todos os seus arquivos? Você pode estar revelando uma senha ou um número de cartão de crédito para um criminoso? Você pode estar expondo as informações privadas dos seus colaboradores para um golpista?

Nº3 - Verificar, verificar e verificar

Tão importante que nunca é demais repetir.

É fundamental lembrar que, com fraudes de phishing, as coisas nunca são o que parecem. A realidade é que uma mensagem pode parecer e até soar legítima, mas ainda disparar um alarme. Por exemplo, um e-mail vindo de um endereço de TI corporativa que lhe instrui a fazer download de um novo software de segurança pode parecer confiável: ele parece real e tem o contexto certo. Mas esse seria o processo habitual do seu departamento de TI?

Se, após ler e pensar, você não estiver 100% confiante, siga algumas etapas adicionais para verificar se está lidando com uma solicitação legítima antes de clicar em um link, fazer download de um arquivo ou responder com dados confidenciais. Eis algumas maneiras de confirmar que as informações apresentadas em um e-mail são legítimas:

- em vez de clicar em um link, abra o seu navegador da Web, digite nele um URL conhecido e confiável e visite o site você mesmo.
- Em vez de responder a um e-mail ou ligar para um número contido na mensagem, faça sua própria investigação. Use um endereço de e-mail ou número de telefone que possa ser confirmado.
- Se você receber uma mensagem questionável de um colega ou amigo, entre em contato com ele ou ela através de outro canal (por exemplo, um telefonema ou mensagem de texto) para se certificar de que foi mesmo ele ou ela quem enviou.
- Consulte a sua equipe de TI para obter recomendações (e para avisá-los de que há uma possível ameaça de phishing ativa na rede da sua organização).

Leva só um minuto confirmar uma mensagem questionável, venha ela de um colaborador, departamento interno, instituição financeira ou outra fonte. Por outro lado, podem ser necessários dias ou semanas (ou até mais) para remediar as consequências de uma interação com um e-mail de phishing ou ransomware. Além disso, nem sempre é possível remediar as consequências.