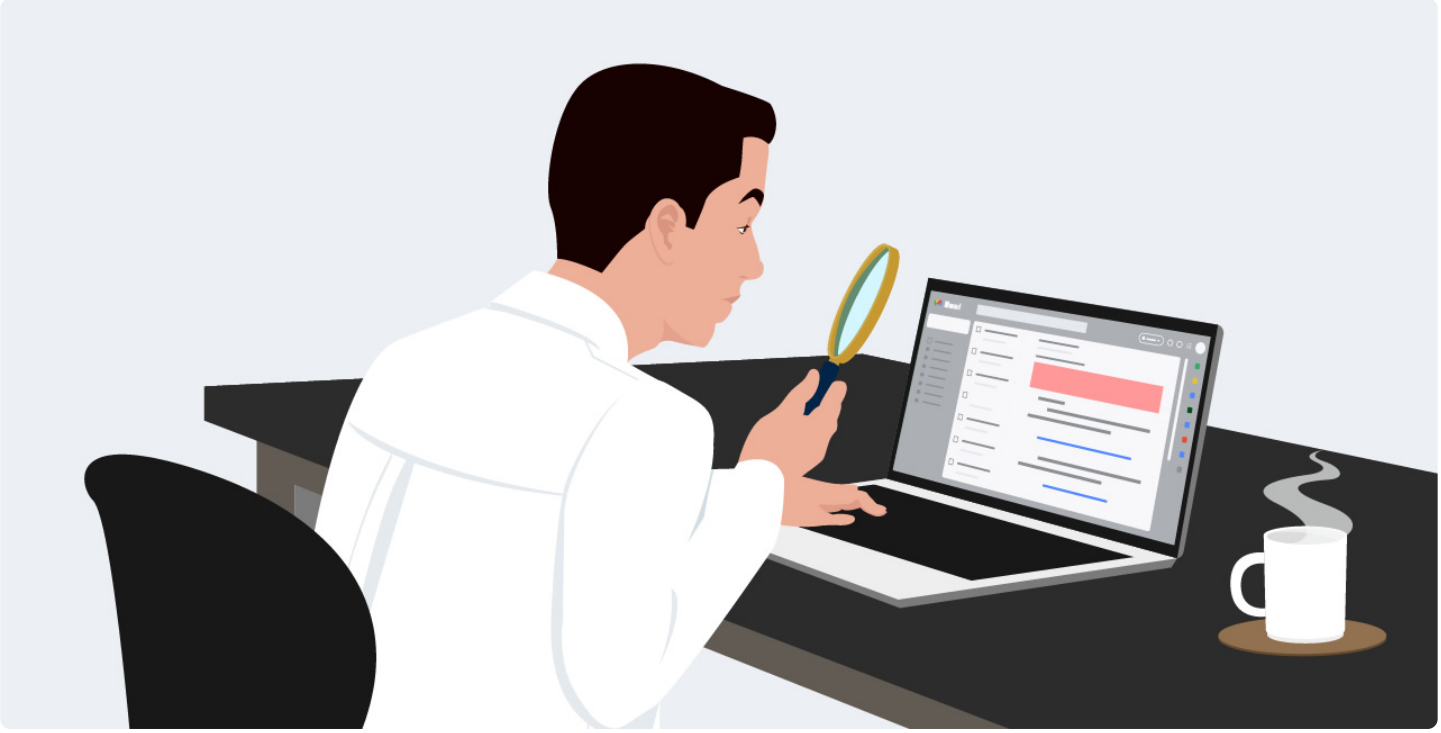
Saiba como identificar um e-mail malicioso e proteja seu e-mail pessoal e do seu consultório

O e-mail pode ser um canal de comunicação valioso para instituições de saúde, mas também é um dos principais vetores de ameaças para crimes cibernéticos.

Com o setor de saúde servindo como alvo popular de ataques, é especialmente crítico que os médicos e funcionários de consultórios, clínicas e hospitais aprendam a reconhecer os sinais de alerta.



E-mails maliciosos estão evoluindo

Os ataques cibernéticos baseados em e-mail estão em ascensão. Houve mais de 260.000 ataques de *phishing* apenas em julho de 2021, que foi o número mensal mais alto no histórico de relatórios do *Anti-Phishing Working Group* (APWG).

Phishing é uma técnica de engenharia social usada para enganar usuários e obter informações confidenciais, como nome de usuário, senha e detalhes do cartão de crédito. São comunicações falsificadas que parecem vir de uma fonte confiável.

O *phishing* por e-mail continua sendo uma das estratégias mais comuns usadas para induzir as vítimas a compartilhar informações confidenciais, mas mais cibercriminosos começaram a usar táticas cada vez mais sofisticadas que podem ser particularmente difíceis de detectar.

Uma abordagem utilizada é o comprometimento de e-mail comercial, que é quando um agente de ameaça se faz passar por um executivo de alto nível para convencer um funcionário a compartilhar informações confidenciais ou realizar uma transferência fraudulenta de dinheiro. Outro método é o *spear phishing*, em que os invasores coletam informações específicas sobre um indivíduo para estabelecer credibilidade e fazer com que um golpe pareça ainda mais legítimo.

A pandemia global também provocou um aumento nos e-mails maliciosos, com ataques aumentando 11% somente em 2020. Além de explorar as fraquezas em ambientes remotos, os cibercriminosos estão lançando esquemas de e-mail que capitalizam diretamente os medos em torno da COVID-19. Em março de 2021, um golpe de pesquisa pós-vacina foi usado para roubar dados pessoais dos consumidores. Os *hackers* também assumiram controle com sucesso de redes de TI, alegando serem o CDC e outros grupos de saúde proeminentes.

Apesar desses avanços contínuos, saber o que procurar em e-mails para identificar aqueles maliciosos pode ajudar a diminuir o risco. A seguir descrevemos alguns identificadores importantes para médicos e demais profissionais de saúde manterem em mente.

Verifique se há inconsistências

Os cibercriminosos costumam alterar os nomes de exibição do e-mail para fazer com que a mensagem pareça vir de uma fonte confiável. Para ficar atento, revise o nome e o endereço de e-mail antes de responder a um e-mail. Um endereço de e-mail de aparência legítima também pode ter algumas letras ausentes ou trocadas após uma inspeção mais detalhada, portanto, fique atento aos pequenos detalhes.

Além disso, fique atento às discrepâncias entre o endereço de e-mail e o nome de domínio (parte que vem após o @). Se um e-mail afirma ser de uma determinada empresa, mas o domínio mostra algo diferente, isso é uma grande dica.

Desconfie de links ou anexos não solicitados

Os anexos de e-mail não solicitados podem ocultar softwares nocivos, como *malware* e *ransomware*, que permitem que os cibercriminosos infectem redes e obtenham acesso a informações confidenciais. Portanto, é aconselhável ser cauteloso desde o início e evitar completamente a abertura de anexos de fontes desconhecidas.

Links maliciosos também podem ser incorporados ao corpo de um e-mail, portanto, sempre tenha cuidado. Passe o mouse sobre o link sem clicar para ver se o texto e o destino real estão alinhados. Links encurtados e URLs com números no final são mais alguns motivos para pausar e evitar clicar.

Procure por escrita ou linguagem estranhas

Um e-mail mal escrito é sempre motivo de suspeitas. Isso pode incluir linguagem quebrada, erros gramaticais, palavras com erros ortográficos ou uma estrutura inconsistente das frases.

Saudações genéricas como “cliente valioso” e assinaturas vagas também podem ser sinais de alerta, pois uma organização válida normalmente se refere aos destinatários pelo nome e inclui informações de contato. Se um remetente afirma ser alguém que você conhece, desconfie de quaisquer diferenças perceptíveis na linguagem ou no tom.

Cuidado com pedidos urgentes

Os cibercriminosos frequentemente tentam assustar as vítimas para que compartilhem informações confidenciais. Isso significa que um e-mail malicioso pode avisá-lo para agir rapidamente e mencionar as consequências de não fazê-lo.

Um e-mail que instila uma sensação de pressão ou urgência é automaticamente um mau sinal. Organizações legítimas também não solicitarão informações confidenciais por e-mail, como credenciais de login ou números de documentos.

Maneiras de se proteger contra ameaças futuras

Para evitar ser vítima de um e-mail malicioso, algumas boas práticas são recomendadas:

- Se você não tiver certeza se uma solicitação de um e-mail é legítima, verifique as comunicações anteriores ou entre em contato diretamente com a empresa ou pessoa para verificar. Evite usar as informações de contato informadas no próprio e-mail recebido.
- Nunca forneça informações internas sobre sua organização, a menos que tenha certeza de que um indivíduo tem a autoridade adequada para acessá-las.
- Não compartilhe dados pessoais ou financeiros por e-mail nem responda a solicitações dessas informações.
- Instale e mantenha software antivírus, *firewalls* e filtros de e-mail para reduzir algumas dessas tentativas.
- Utilize os recursos *anti-phishing* do seu e-mail e navegador web ou contrate um serviço terceirizado para maior segurança.

- Aplique a autenticação multifator (método de autenticação eletrônica no qual um usuário tem acesso a um site ou aplicativo somente após apresentar com sucesso duas ou mais evidências para um mecanismo de autenticação).

Quando se trata de e-mails maliciosos, educar seus funcionários sobre como identificar os sinais de alerta é um passo inteligente na direção certa. No entanto, é importante ter em mente que o erro humano é inevitável.

É por isso que os profissionais de saúde devem tomar medidas extras para proteger dados confidenciais, concentrando-se no fortalecimento das medidas de segurança de e-mails recebidos. Essas medidas proativas impedirão que e-mails maliciosos cheguem às caixas de entrada dos funcionários em primeiro lugar.

Artigo original disponível em:
"Saiba como identificar um e-mail malicioso e proteja seu e-mail pessoal e do seu consultório " - **HiDoctor® Blog**

Centralx®