Proteja-se contra phishing

Phishing (pronunciado: fishing) é um ataque que tenta roubar seu dinheiro ou a sua identidade fazendo com que você revele informações pessoais, tais como números de cartão de crédito, informações bancárias ou senhas em sites que fingem ser legítimos. Criminosos cibernéticos normalmente fingem ser empresas confiáveis, amigos ou pessoas conhecidas em uma mensagem de email falsa, que contém um link para um site de phishing.

Aprenda a identificar um email de phishing

Phishing é uma forma popular de crime cibernético porque é efetivo. Criminosos têm sido bem-sucedidos em usar emails, mensagens de texto ou mensagens diretas nas redes sociais ou em videogames para que as pessoas respondam com as informações pessoais. As melhores defesas são a conscientização e a capacidade de saber o que procurar.

Aqui estão algumas maneiras de reconhecer um email de phishing:

- **Chamada urgente à ação ou ameaças** - Suspeite de emails que afirmam que você deve clicar, ligar ou abrir um anexo imediatamente. Muitas vezes eles alegarão que você terá que agir agora para reivindicar uma recompensa ou evitar uma penalidade. Criar um falso senso de urgência é um truque comum de ataques de phishing e golpes. Eles fazem isso para que você não pense muito sobre isso ou consulte um consultor de confiança que possa alertá-lo.

  Dica: Sempre que você vir uma mensagem pedindo uma ação imediata, pare um pouco e observe cuidadosamente a mensagem. Você tem certeza que ela é real? Vá devagar e esteja seguro.

- **Remetentes novos ou não frequentes** - Embora não seja incomum receber um email de alguém pela primeira vez, especialmente se o remetente não pertence à sua organização, isso poderá ser um sinal de phishing. Quando receber um email de alguém que você não reconhece ou que o Outlook identifica como um novo remetente, examine-o cuidadosamente antes de prosseguir.
- **Erro de ortografia e gramática** - Empresas ou organizações profissionais geralmente têm uma equipe editorial para garantir aos clientes um conteúdo profissional e de alta qualidade. Se uma mensagem de email apresentar erros ortográficos ou gramaticais óbvios, pode ser um golpe. Às vezes, esses erros são o resultado de uma tradução inadequada de um idioma estrangeiro e, às vezes, são deliberados na tentativa de escapar dos filtros que tentam bloquear esses ataques.
- **Saudações genéricas** - uma organização que trabalha com você deve saber o seu nome e, atualmente, é fácil personalizar um email. Se o email começar com um genérico

"Prezado senhor ou senhora", isso é um sinal de alerta de que pode não ser realmente o seu banco ou site de compras.

- **Links suspeitos ou anexos inesperados** - Se suspeitar que uma mensagem de email é uma fraude, não abra nenhum link ou anexo que houver. Em vez disso, passe o mouse sobre o link, mas não clique, para ver se o endereço corresponde ao link que foi digitado na mensagem. No exemplo a seguir, passar o mouse sobre o link revela o verdadeiro endereço da Web na caixa com o plano de fundo amarelo. Observe que a sequência de números de endereço IP não se parece nada com o endereço web da empresa.

Dica: No Android, pressione o link para obter uma página de propriedades que revelará o verdadeiro destino do link. No iOS, faça o que a Apple chama de "Light, long-press".

- **Domínios de email divergentes** - Se o email alega ser de uma empresa confiável, como a Microsoft ou seu banco, mas o email está sendo enviado de outro domínio de email como Yahoo.com ou microsoftsupport.ru, provavelmente é um golpe. Também esteja atento a erros de ortografia muito sutis no nome de domínio legítimo. Por exemplo, micros0ft.com, onde o segundo "o" foi substituído por um 0 ou rnicrosoft.com, onde o "m" foi substituído por um "r" e um "n". Esses são truques comuns de golpistas.

Os criminosos cibernéticos também podem fazer com que você visite sites falsos com outros métodos, tais como mensagens de texto ou ligações telefônicas. Criminosos cibernéticos sofisticados organizam call centers para ligar ou mandar SMS automaticamente para os números de possíveis alvos. Estas mensagens muitas vezes incluem avisos para que você digite um número PIN ou algum outro tipo de informação pessoal.

Se você receber um email de phishing

- Nunca clique em links ou anexos em emails suspeitos. Se você receber uma mensagem suspeita de uma organização e temer que a mensagem possa ser legítima, acesse o navegador da web e abra uma nova guia. Em seguida, vá para o site da organização a partir de seu favorito salvo ou por meio de uma pesquisa na Web. Ou ligue para a organização usando um número de telefone listado no verso de um cartão de membro, impresso em uma fatura ou extrato, ou que você encontra no site oficial da organização.
- Se a mensagem suspeita parece vir de uma pessoa que você conhece, entre em contato com essa pessoa por outros meios, como mensagem de texto ou chamada telefônica, para confirmar.
- Denuncie a mensagem (veja abaixo).
- Exclua.

Como denunciar um golpe de phishing

- **Microsoft Office Outlook** - Com a mensagem suspeita selecionada, escolha **Relatar mensagem** na faixa de opções e selecione **Phishing**. Esta é a maneira mais rápida de denunciá-la e remover a mensagem da sua Caixa de Entrada, e nos ajudará a melhorar nossos filtros para que você veja menos mensagens como essas no futuro. Para obter mais informações, confira Usar o suplemento Relatar mensagem.
- **Outlook.com** - Marque a caixa de seleção ao lado da mensagem suspeita na caixa de entrada do Outlook.com. Selecione a seta ao lado do **Lixo eletrônico** e, em seguida, selecione **Phishing**.

Observação: Se estiver usando um cliente de email diferente do Outlook, escreva um novo email para phish@office365.microsoft.com e inclua o email de phishing como anexo. Não encaminhe o email suspeito; precisamos recebê-lo como anexo para que possamos examinar os cabeçalhos da mensagem.

Se você estiver em um site suspeito:

Enquanto você estiver em um site suspeito no Microsoft Edge, selecione o ícone **Mais(...)** > Ajuda e **comentários** > Site **não seguro**.

O que fazer se você acha que caiu no golpe?

Se você suspeita que pode ter caído inadvertidamente em um ataque de phishing, há algumas coisas que você deve fazer.

1. Enquanto está fresco na sua mente, escreva o máximo de detalhes do ataque de que você se lembrar. Em particular, tente anotar qualquer informação como nomes de usuário, números de conta ou senhas que você possa ter compartilhado.
2. Altere imediatamente as senhas das contas afetadas, e em qualquer outro lugar que você possa usar a mesma senha. Quando estiver trocando as senhas, você deverá criar senhas únicas para cada conta, e você pode querer consultar Criar e usar senhas fortes.
3. Confirme se você tem a autenticação multifator (também conhecida como verificação em duas etapas) ativa para todas as contas que puder. Veja O que é: Autenticação multifator
4. Se este ataque afetar suas contas de trabalho ou escola, você deve notificar o pessoal do suporte da TI no seu trabalho ou escola sobre o possível ataque. Se você compartilhou informações sobre seus cartões de crédito ou contas bancárias, convém entrar em contato com essas empresas também para alertá-las sobre possíveis fraudes.
5. Se você perdeu dinheiro ou foi vítima de roubo de identidade, denuncie às autoridades locais. Os detalhes da etapa 1 serão muito úteis para eles.