Sua edição mensal de conscientização de segurança

Golpes Personalizados

Visão Geral

Criminosos cibernéticos continuam inventando novas e criativas formas de enganar as pessoas. Um novo tipo de golpe está ganhando popularidade, o golpe personalizado. Criminosos cibernéticos encontram ou compram informações sobre milhões de pessoas e então utilizam essa informação para personalizar seus ataques. Vamos mostrar abaixo como esses golpes funcionam e mostrar um exemplo comum. Quanto mais você souber sobre esses golpes, mais fácil será identificar e pará-los.

Como funciona?

Golpes por e-mail ou telefone não são novos. Criminosos cibernéticos vêm tentando enganar pessoas há anos. Exemplos incluem "você ganhou na loteria" ou a infame fraude de pagamento adiantado (fraude Nigeriana). Contudo, nesses métodos tradicionais os criminosos cibernéticos não sabem quem eles estão atingindo. Eles simplesmente criam uma mensagem genérica e enviam para milhões de pessoas. O fato de serem tão genéricos, faz com que sejam fáceis de detectar. Um golpe personalizado é diferente. Os criminosos fazem uma pesquisa primeiro e então criam uma mensagem personalizada para cada vítima pretendida. Eles fazem isso encontrando ou comprando um banco de dados com nomes de pessoas, senhas, telefones ou outros detalhes. Esse tipo de informação está facilmente disponível através de todos os sites de Internet já hackeados. Também está disponível normalmente em sites de mídia social e em registros de governo disponíveis publicamente. Os criminosos miram então todos aqueles dos quais têm informação.

Um truque comum utilizado pelos criminosos é amedrontar ou extorqui-lo para que envie dinheiro para eles. O ataque acontece assim: eles descobrem ou compram informações de usuário e senha de sites hackeados. Então encontram sua informação de conta nessa base de dados e enviam para você (e para todos que estiverem na base de dados) um e-mail com informações pessoais sobre você, incluindo sua senha utilizada no site hackeado. Os criminosos dizem que sua senha é uma "prova" de terem hackeado seu computador ou dispositivo, o que é obviamente uma mentira. E dizem que ao hackear seu computador, eles também pegaram seu histórico de acesso a pornografia online. O e-mail então ameaça compartilhar essas evidências de atividades embaraçosas com sua família e amigos caso você não pague o valor da extorsão.

O ponto é que, em quase todas as situações como essa, o criminoso cibernético nunca hackeou seu sistema. Eles nem sequer sabem quem você é e quais sites de Internet você tem visitado. O golpista está simplesmente tentando utilizar os poucos detalhes que têm sobre você para amedrontar e fazê-lo acreditar que hackearam seu computador ou dispositivo, enganando-o assim para fazer o pagamento desejado. Lembre-se que esses criminosos utilizam as mesmas técnicas para um golpe por telefone.

O que devo fazer?

Reconheça que e-mails ou ligações como essa são golpes. É natural sentir-se amedrontado quando alguém possui informações pessoais sobre você. Porém, lembre-se que ele está mentindo. O ataque é parte de uma campanha massiva e automatizada e não um ataque direto contra você. Está cada vez mais fácil para os criminosos cibernéticos hoje, encontrar ou comprar informações pessoais. Então esteja preparado para receber mais golpes como esse no futuro. Algumas pistas para identificá-los:

⚠

- **Sempre que receber e-mails, mensagens ou chamadas de telefone altamente urgentes, suspeite bastante. Ou se alguém estiver utilizando emoções como medo ou urgência ou tentando apressá-lo para cometer um erro;**
- **Quando alguém estiver pedindo pagamento em BitCon, gift cards (cartões pré-pagos de consumo em lojas ou serviços online) ou outros métodos de pagamento não rastreáveis;**
- **Quando receber um e-mail suspeito, procure no Google para ver se outra pessoa relatou um ataque parecido.**

Finalmente, o bom senso é sua melhor defesa. Contudo, sempre recomendamos que utilize uma senha única e longa para cada conta online. Não consegue se lembrar de todas as senhas? Utilize um gerenciador de senhas. Adicionalmente, habilite a verificação em duas etapas sempre que possível.

Editor Convidado

Lenny Zeltser *é um veterano de segurança cibernética. Ele cria soluções anti-malware na Minerva Labs e dá aulas de segurança no SANS Institute. Sua experiência inclui também serviços de segurança gerenciada e consultoria. Siga-o em* zeltser.com/blog *e no Twitter* @lennyzeltser.

Recursos

Engenharia Social:	https://www.sans.org/u/MUU
Pare esse Phishing:	https://www.sans.org/u/MUZ
Pesquise Sobre Você Online:	https://www.sans.org/u/MV4
Gerenciamento de Senhas:	https://www.sans.org/u/MV9