A Publicação Mensal de Sensibilizaçao de Segurança para Usuários de Computadores

Pare esse Phishing

Visão Geral

Serviços de e-mail e mensagens instantâneas (como Skype, Twitter ou Snapchat) são uma das principais formas de nos comunicarmos. Nós não só usamos essas tecnologias diariamente para trabalhar, mas também para manter contato com amigos e família. O fato de tantas pessoas dependerem dessas tecnologias diariamente, fez com que elas se tornassem um dos principais meios de ataque utilizados por atacantes cibernéticos, para um ataque chamado phishing. Saiba o que é o phishing, como identificar e pará-lo, independentemente de estar no trabalho ou em casa.

O que é Phishing

Phishing é um tipo de ataque que usa serviços de e-mail ou mensagem para enganar e fazê-lo tomar uma ação que não deveria, como clicar em um link malicioso, compartilhar sua senha ou abrir um anexo infectado em um e-mail. Atacantes trabalham duro para tornar essas mensagens convincentes e tocar seu emocional com sentimento de urgência ou curiosidade. Eles podem fazer com que pareça ter vindo de um amigo ou de algum serviço que conheça, como uma empresa confiável que você usa frequentemente. Ou talvez adicionem logos do seu banco ou forjem o endereço de e-mail para que a mensagem pareça legítima. Os atacantes então enviam essas mensagens para milhões de pessoas. Eles não sabem quem morderá a isca. Tudo que sabem é que quanto mais mensagens enviarem, mais pessoas se tornarão vítimas.

Proteja-se

Em quase todos os casos, abrir e ler uma mensagem ou e-mail não traz problemas. Para um ataque de phishing funcionar, é preciso que você seja conduzido a fazer alguma coisa. Felizmente existem pistas que identificam um ataque. Aqui vão as mais comuns:

- Um tremendo senso de urgência, demandando “ação imediata” antes que alguma coisa ruim aconteça, como uma ameaça de fechar uma conta ou enviá-lo para a prisão. O atacante quer lhe apressar para conduzi-lo ao erro;
- Pressão para você contornar ou ignorar políticas ou procedimentos de trabalho;
- Um forte senso de curiosidade ou algo muito bom para ser verdade (não, você não ganhou na loteria);

- Uma saudação genérica como “Caro Cliente”. Muitas companhias ou amigos utilizam seu nome ao contatá-lo;
- Pedidos de informações altamente sensíveis como o número do seu cartão de crédito ou senha ou qualquer outra informação que o remetente já devesse conhecer;
- Uma mensagem dizendo vir de uma organização oficial, mas com linguagem pobre ou erros de escrita ou ainda utilizando endereços de e-mail pessoais como @gmail.com;
- Uma mensagem vinda de um e-mail oficial (como seu chefe) mas com endereço de resposta para uma conta de e-mail pessoal de outra pessoa;
- Uma mensagem vinda de alguém que você conhece, mas o tom da mensagem ou a escrita simplesmente não parece ser daquela pessoa. Se você suspeitar, ligue para ela e verifique se ela realmente enviou a mensagem. É fácil para um atacante cibernético criar uma mensagem que pareça ter vindo de um amigo ou colega de trabalho.

Finalmente, o bom senso é sua melhor defesa. Se uma mensagem ou e-mail parece estranho, suspeito ou muito bom para ser verdade, ele pode ser um ataque.

Editor Convidado

Tonia Dudley desenvolve e implementa programas de Conscientização de Segurança desde 2011, incluindo um programa premiado de treinamento para phishing. Você pode encontrá-la em www.linkedin.com/in/toniadudley.

Recursos

Engenharia Social:	https://www.sans.org/u/Cb1
Ajudando Outros a se Proteger:	https://www.sans.org/u/Cb6
E -mails, o que fazer e o que não fazer:	https://www.sans.org/u/Cbg
CEO Impostor:	https://www.sans.org/u/Cbl
Traduções e Arquivos OUCH!:	https://www.sans.org/u/Cbq

License