OUCH! | Julho de 2018

SANS SECURITY AWARENESS

OUCH!

A Publicação Mensal de Sensibilizaçao de Segurança para Usuários de Computadores

Ataques e Golpes Por Telefone

Visão Geral

Quando você pensa em criminosos cibernéticos, provavelmente pensa em um mentor maligno atrás de um computador enviando ataques sofisticados pela Internet. Mesmo havendo criminosos utilizando tecnologias como email ou de mensagens instantâneas, também existem os que usam o telefone para enganar suas vítimas. Há duas grandes vantagens em utilizar o telefone. Primeiro, diferente do email, existem poucas tecnologias para monitorar chamadas telefônicas capazes de detectar e parar um ataque. Segundo, é muito mais fácil para um atacante transmitir emoção pelo telefone, o que torna mais provável que consigam enganar suas vítimas. Vamos ver como identificar e parar esses ataques.

Como funcionam os ataques por telefone ?

Primeiro você tem que entender o que os atacantes buscam. Normalmente seu dinheiro, informações ou acesso ao seu computador (ou tudo isso junto). Eles fazem isso enganando você para forçá-lo a fazer o que querem. Eles ligam para pessoas ao redor do mundo, criando situações que parecem muito urgentes. A intenção é desestabilizá-lo e assustá-lo para que não pense com clareza. E então apressam-lhe para que cometa um erro. Alguns dos exemplos mais comuns são:

A pessoa finge ser do departamento de fiscalização ou de impostos do governo, dizendo que você tem impostos pendentes de pagamento. Eles explicam que se você não pagar naquele momento, você será preso. E então lhe pressionam para pagar utilizando seu cartão de crédito pelo telefone. Isso é um golpe. Muitos órgãos do governo nunca ligam para as pessoas. Todas as notificações de impostos são enviadas por correspondência regular, pelo correio;

A pessoa finge ser do departamento de suporte técnico da Microsoft e explica que seu computador está infectado. Uma vez que lhe convença disso, começa a pressionar para que compre um software ou conceda acesso remoto ao seu computador. A Microsoft não vai ligar para a sua casa;

Você recebe uma mensagem automática no correio de voz dizendo que sua conta bancária foi cancelada. E que precisa ligar de volta para um determinado número para reativá-la. Quando você liga, um atendente automático pede que confirme sua identidade fazendo algumas perguntas pessoais. Isso não é realmente o seu banco e eles estão apenas gravando suas informações para aplicarem uma falsificação de identidade.

Protegendo-se

A maior defesa que você tem contra ataques por telefone é você mesmo. Mantenha essas informações em mente:

- Sempre que alguém ligar e criar um tremendo senso de urgência, pressioná-lo a fazer alguma coisa, suspeite fortemente. Mesmo que a ligação pareça legítima a princípio, mas comece a parecer estranha, você pode parar e dizer "não" a qualquer momento;
- Se acredita que uma ligação é um ataque, simplesmente desligue. Se você quiser confirmar que a ligação era legítima, vá à página de Internet da organização (por exemplo, o banco), obtenha o número de atendimento telefônico e ligue você mesmo para eles. Assim você saberá de fato que está falando com a organização real;
- Nunca confie no identificador de chamada. Os atacantes frequentemente falsificam o número de origem para que pareça estar vindo de uma organização legítima, ou para que tenha o mesmo número de região do seu telefone;
- Nunca permita que uma pessoa obtenha controle temporário do seu computador ou lhe convença a fazer um download de software. É assim que eles infectam seu computador;
- Se você receber uma chamada de telefone de alguém que não conhece pessoalmente, deixe cair na caixa postal. Assim poderá rever as chamadas desconhecidas no seu próprio tempo. Melhor ainda, em alguns telefones você pode habilitar esse recurso por padrão utilizando a função "não perturbe".

Golpes e ataques pelo telefone estão em ascensão. Você é a melhor defesa para detectá-los e pará-los.

Editor Convidado

Jen Fox *presta serviços de conscientização de segurança, engenharia social e análise de risco como Consultora de Segurança Sênior na All Covered. Encontre a Jen no Twitter como* @j_fox.

Recursos

Informação ao consumidor sobre Identidade, Privacidade e Segurança Online (nos EUA, em Inglês):
https://www.consumer.ftc.gov/topics/privacy-identity-online-security
Relatar um golpe por telefone (nos EUA): https://www.ftccomplaintassistant.gov/#crnt
Engenharia Social: https://www.sans.org/u/Fi5
Onde denunciar crimes virtuais: lista de delegacias especializadas no Brasil:
http://idciber.eb.mil.br/index.php?option=com_content&view=article&id=793:onde-denunciar-crimes-virtuais-lista-de-delegacias-especializadas&catid=78&Itemid=301