Engenharia Social

Nestes últimos tempos um golpe antigo tem retornado à tona... Muitos já se depararam com o e-mail do Príncipe Nigeriano que precisa fugir do país com uma quantia alta de dinheiro e precisa da sua ajuda para repassar esses valores ou com e-mails de alguém que diz que você estava no testamento de algum parente distante e que eles tem algumas quantias para você.

Depois vieram os golpes de falso sequestro onde o criminoso liga para sua casa e diz que raptou alguém e pede para que você deposite um certo valor pra libertar a pessoa.

Não diferente desses dois golpes acima, agora está na moda que o "Príncipe Nigeriano" tem o nome de uma pessoa conhecida que está passando por dificuldades e te pede dinheiro para salvá-lo de alguma enrascada no exterior. Os dados parecem verídicos, exceto que aquele e-mail é um e-mail falso criado gratuitamente como se fosse da pessoa. Esse tipo de golpe, já antigo, é chamado de "Engenharia Social", onde o criminoso se faz passar por outra pessoa para ganhar algum dinheiro com isso.

Você pode se perguntar: Como o criminoso sabe tudo sobre aquela pessoa? Como ela sabe que nós somos amigos? Como ela sabe meu nome?

A resposta é fácil: Existem diversas maneiras de se obter esses dados. Algumas mais comuns seguem abaixo:

1. Você pode cruzar informações públicas das Redes Sociais
2. Quebrando ou roubando de e-mail e estudando um pouco os e-mails trocados pela pessoa
3. Hackeando sites que tenham essas informações
4. Utilizando aplicativos maliciosos instalados em seu computador/navegador/redes sociais

O método 1 é banal. Você escolhe uma pessoa na internet e começa a tentar descobrir mais informações sobre ela. Pessoas com nome mais incomuns são até um alvo mais fácil por produzirem resultados mais concisos nas buscas em qualquer buscador de internet. É a velha pergunta: "Já procurou seu nome no Google?" Se você fizer isso, vai ver quantas informações tem de graça na Internet sobre você. Com um pouco de busca você vai ver que consegue achar até seus números de RG e CPF por exemplo.

O método 2 já precisa da ingenuidade de alguma pessoa do círculo de contatos da pessoa "forjada". Senhas fracas podem ser quebradas facilmente hoje em dia com alguns programas que ficam testando senhas. Roubar uma senha também é outro golpe, onde alguém recebe um e-mail que pede para a pessoa digitar a senha em algum lugar (ou até mesmo responder por e-mail) e aí a pessoa ganha acesso a várias informações. E você não precisa ter a sua senha roubada... se você mandou um e-mail para alguém que teve a senha roubada, os criminosos podem ter lido essa mensagem e a partir daí conseguem por exemplo saber já a sua assinatura e que você é conhecido daquela pessoa.

O método 3 é o seguinte: pense em quantos sites você já precisou se cadastrar para poder usar, às vezes por alguns poucos minutos e nunca mais... Se esse site um dia for hackeado seus dados ainda podem estar lá. E isso é mais fácil se o site for um site "esquecido" no tempo, que não recebe muitas atualizações de segurança. Uma coisa comum também é que pessoas usam a mesma senha para todos os sites. Isso acaba causando uma bola de neve: se a pessoa consegue seus dados em um site que ela hackeou, há grandes chances de que o criminoso utilize essas informações para entrar em outros sites relacionados, por exemplo e-mail e redes sociais.

O método 4 é polêmico. A parte banal é a pessoa reclamar: "Um vírus está no meu computador e não

sei como!". Pois então saiba agora: Nem todo aplicativo malicioso é necessariamente instalado sem conhecimento do usuário! Há uma grande gama de aplicativos que explicitamente informa ao usuário o que ele faz e o usuário se quer se importa com isso. E muitos desses aplicativos informa que ao instalar esse programa, ele tem acesso aos seus dados de usuário, sua lista de amigos, seus dados de e-mail... Veja por exemplo as permissões de um aplicativo para celular gratuito. Você imagina o que esse aplicativo exemplo-app.jpg faz para precisar de acesso à sua "Localização Aproximada", "Ler status e identidade do telefone", "Acesso total à rede", etc? Não digo aqui que este aplicativo é um aplicativo malicioso, mas muitos aplicativos maliciosos possuem as mesmas permissões e a pessoa deliberadamente instala no computador, no celular, no navegador de internet, na Rede Social e depois não sabe como tantas pessoas sabem as informações sobre ela... Eventualmente algum desses aplicativos pode ser feito apenas para conseguir de graça várias informações sobre você e depois utilizá-las para ganhar algum dinheiro de forma lícita ou ilícita. Antes que me esqueça, o aplicativo que utilizei de exemplo era apenas um metrônomo, mas podia ser um joguinho, um papel de parede, infinitas coisas.

Segue um e-mail repassado à comunidade USP sobre incidentes recentes, que envolvem criminosos se passando por professores da universidade que precisam de dinheiro para alguma emergência. Como os criminosos conseguiram esses dados? Muito provavelmente utilizando um dos métodos listados acima.

Para mais informações, recomendamos ler a cartilha do CERT.BR - http://cartilha.cert.br/

Email repassado pela STI-USP

Prezados,

Notamos nas últimas semanas um aumento no número de incidentes de segurança envolvendo roubo de identidade, e pedimos aos colegas que orientem seus usuários para que fiquem alertas para esse tipo de golpe. O golpista cria um perfil falso da vítima usando um sistema de e-mail gratuito (como o Gmail, por exemplo), em seguida manda mensagens para pessoas próximas a vítima. Essas mensagens variam, mas elas usam técnicas de engenharia social para aplicar o golpe, sendo composta pelos seguintes elementos:

- Cumprimento direcionado a pessoa recebendo o e-mail (Olá, <FULANO>), tentando criar uma conexão com a vítima;

- Em seguida, a mensagem informa algum tipo de fatalidade, como um acidente ou a morte de um parente próximo;

- Na mensagem, se passando pela vítima, é informado que tentou sacar uma quantia em dinheiro para resolver pendências com relação a fatalidade mencionada, mas que teve um problema com o cartão e precisa com urgência de uma quantia em dinheiro;

- O texto continua relatando dificuldade de comunicação (estou no interior, estou fora do país, estou na cidade X), sem acesso a internet ou telefone, pedindo para a pessoa responder o e-mail que em um determinado prazo de tempo (30 minutos, por exemplo), ele responderá a mensagem;

- É solicitado alguma ajuda financeira, a ser depositada na conta de um parente próximo a ser informada posteriormente (depois que a pessoa responder o e-mail informando se pode ajudar ou não, no caso);

- A mensagem tem uma assinatura com dados da vítima, para torna-la mais “crível”. O perfil da conta também pode usar uma imagem da vítima, o que pode dar uma falsa sensação de “veracidade”;

- O assunto da mensagem costuma ter carater imediatista (URGENTE !!!).

- O golpista usa uma conta de e-mail usando o nome da vítima, acrescido de outras informações para dar maior “veracidade” (vitima.usp@jmail.com ou vitima@quentemail.com , por exemplo).

O que fazer caso perceba alguém tentando se passar por um professor, funcionário ou aluno da USP?

(Continuando e-mail da STI-USP)

Nesse tipo de situação, antes de mais nada é preciso manter a calma. Se receber uma mensagem como esta, confirme com a pessoa se foi ela que enviou mesmo, usando outro meio de contato (telefone ou pessoalmente, de preferência). Confirmada a fraude, informe o recebimento da mesma a nossa equipe de atendimento (atendimentosti@usp.br) com cópia para nosso Grupo de Segurança em TI (security@usp.br). As vítimas do golpe serão orientadas quanto a procedimento a seguir nesse tipo de incidente.

Fim do e-mail da STI-USP