Ameaças comuns de engenharia social

Muitas ameaças continuarão a trazer problemas para aqueles que usam a Internet, e a menos que você opte por parar de usar esse recurso, você deve conhecer estas ameaças. Veremos as ameaças direcionadas aos seres humanos e as fraquezas da natureza humana.

Que tipo de ameaças focam nos usuários e sobre a natureza humana? Vejamos alguns:

- **Malware** – Isso pode ser usado como um termo abrangente para vírus, spyware, keyloggers, worms, cavalos de Tróia e outras ameaças da Internet. No entanto, falando de engenharia social significa cavalos de Tróia.
- **Shoulder Surfing** (espiar sobre os ombros) – Este tipo de ataque ocorre quando uma das partes é capaz de olhar sobre o ombro de outro ou espionar a tela do outro. Isso é comum em ambientes de todo tipo, porque quando você vê outras pessoas assistindo o que você está fazendo, você terá a curiosidade humana normal sem perceber.
- **Eavesdropping –** Isso envolve em ouvir conversas, vídeos, telefonemas, e-mails e outras comunicações com a intenção de reunir informações que um atacante não seria autorizado teria.
- **Dumpster Diving –** O lixo de um homem é o tesouro de outro homem, e um atacante pode ser capaz de coletar informações sensíveis ou importantes de cestos de lixo e outros pontos de coleta e usá-lo para realizar um ataque. Na prática, essas informações devem ser trituradas, queimadas ou destruídas para evitar que sejam interceptadas por um atacante.
- **Phishing –** É o uso de um e-mail aparentemente legítimo que o convida a clicar em um link ou visitar um site onde suas informações serão coletadas. Este é um ataque

comum e é muito eficaz, embora esta técnica tenha sido combatida por mais de uma década e vários avisos foram publicados, dizendo aos usuários o que olhar antes de clicar.

Embora muitas empresas implementem tecnologia, políticas administrativas e medidas físicas para impedir ataques de engenharia social, a prevenção continua a ser atribuída aos seres humanos. Eles estão em muitos casos na linha da frente, assistindo a um ataque. As medidas que podem ajudar a derrotar ataques relacionados à tecnologia incluem o seguinte:

- **Instalando um Navegador Web Moderno –** Como porta principal para o mundo da Internet, seu navegador deve ser o mais seguro possível. Ser seguro significa pelo menos duas coisas: Use o navegador mais atual e mantenha o navegador atualizado. Além disso, evite plug-ins desnecessários e add-ons que desordenam o navegador e podem enfraquece-lo. A maioria dos navegadores modernos incluem recursos que protegem contra ataques de engenharia social como phishing e sites falsos.
- **Bloqueador de pop-ups** – Um navegador moderno reconhece pop-ups potencialmente perigosos, permitindo que você saiba quando ele bloqueia um pop-up e oferece a opção de bloquear seletivamente cada pop-up conforme necessário.
- **Advertência sobre site inseguro** – Se você acessar um site fraudulento, não confiável ou tiver problemas de segurança conhecidos, o navegador deve impedir o carregamento do site.
- **Integração com o software antivírus –** Seu navegador deve trabalhar com um programa antivírus residente para verificar arquivos baixados e validar se existem ameaças de segurança.
- **Atualizações Automáticas –** Os navegadores modernos geralmente se atualizam para incorporar correções de falhas no software e adicionar novos recursos de segurança.

- **Navegação privada –** Este recurso tornou-se comum nos navegadores mais recentes, incluindo todos os navegadores populares, como o Chrome, Internet Explorer, Firefox e outros. Este modo impede a gravação de tipos específicos de informações no navegador, como o histórico de pesquisa, bem como a prevenção de certos comportamentos a serem observados.
- **Mudando Hábitos Online –** Nenhum software pode compensar os maus hábitos de segurança da Internet. As ferramentas podem ajudar, mas não podem impedi-lo de agir imprudentemente ou descuidadamente on-line.

Alguns métodos comuns que você deve considerar para educar seus usuários ou clientes deve incluir no mínimo o seguinte.

- Tenha cuidado com as redes sem fio não seguras. O acesso Wi-Fi gratuito na loja de café na rua poderia custar-lhe muito se é inseguro e aberto para o mundo. Uma conexão não segura é uma rede aberta que permite que qualquer pessoa se conecte. As informações passadas de um laptop para o roteador sem fio e vice-versa podem ser interceptadas por pessoas com as ferramentas certas porque não são criptografadas. Além disso, os ataques de rede podem ser feitos a partir de outros computadores conectados à rede.
- Tenha cuidado ao acessar informações confidenciais em um local público. Mesmo em uma conexão segura ou uma VPN, as pessoas podem ver o que você digita em uma tela de laptop. Você pode revelar informações confidenciais a uma pessoa que anda perto com um telefone da câmera quando você fizer seus serviços bancários. O mesmo ocorre em um escritório, onde um colega de trabalho intrometido espiona por cima de uma parede de cubículo ou um administrador de rede sem escrúpulos espionando uma estação de trabalho poderá pegar uma senha.
- Não guarde informações pessoais em sites de compras. A maioria dos sites de compras oferecem para salvar um

cartão de crédito e informações de endereço para checkout mais fácil no futuro. Embora a informação seja supostamente segura, muitos roubos de tais informações ocorreram recentemente.

- Tenha cuidado com a publicação de informações pessoais. As pessoas adoram conversar e compartilhar ou postar os detalhes de suas vidas pessoais em sites de redes sociais como o Facebook. Eles dão ao público acesso à sua informação e, em seguida, reclamar sobre questões de privacidade.
- Cuide do seu computador pessoal. Navegadores de Internet como o Internet Explorer e o Mozilla Firefox facilitam o armazenamento de senhas e informações de formulários. Qualquer pessoa que abra um navegador da Web pode verificar o histórico de navegação, visitar sites seguros e entrar automaticamente como você, se você optar por ter o navegador salvar sua senha. Evite armazenar senhas – ou, melhor ainda, proteja com senha seu computador e bloqueie-o quando não estiver em uso. Crie uma segunda conta num computador para outras pessoas utilizarem para que as informações sejam mantidas separadas e certifique-se de que a conta está protegida por senha e não tem acesso de alto nível, como o que está disponível para um administrador.

Sugestões de livros: