Como dar seus dados para possíveis golpistas ou tornar alguém rico na internet

Há muito tempo a internet sofre com pessoas tentando enriquecer de maneira fácil às custas dos outros. Diversos tipos de golpes e fraudes circulam a rede em vários locais: São páginas com conteúdo falso, e-mails fraudulentos, propagandas irritantes, softwares mal intencionados, links de redes sociais... Ah, as redes sociais, estão cheias desse lixo.

Mas o que aquele link de testes de “quem eu sou no filme X” ou “quando vou morrer”, ou “quem é seu par romântico” tem a ver com enriquecer pessoas por aí, com o roubo de dados e com e-mails fraudulentos que eu receberei no futuro? A resposta é: TUDO

A primeira coisa que você deve pensar: Nada na internet é gratuito. A segunda coisa é: propaganda é a alma do negócio. Manter uma página na internet gera custos. Se esse conteúdo vem até você sem te pedir dinheiro explicitamente, é porque alguém está pagando essa conta. E se ninguém está desembolsando esse dinheiro do próprio bolso, isso normalmente é pago por propagandas que vão aparecer para você no processo OU por dinheiro que eles vão fazer te enviando propagandas de um jeito ou de outro.

E pior que receber propagandas, é dar aos golpistas todas as informações de graça para que eles possam no futuro tentar te extorquir, aplicar golpes em você ou em outras pessoas utilizando o seu nome.

Veja por exemplo este caso: Sabe qual o significado do seu nome em Árabe? Pois é, com um clique você digita seu nome e este site te dá o suposto significado do seu nome em Árabe. Não estou dizendo que este site em específico é um site que dá golpes, apesar de ter toda a cara de um site de golpes, então serve como bom exemplo. Vamos ao funcionamento:

Você vê uma postagem de um amigo seu no Facebook dizendo qual o significado do nome dele em Árabe. Os nomes foram escondidos para preservar as pessoas.

Note que a postagem está em nome da pessoa. É o nome dela, dividido na metade, dizendo que o significado de cada metade do nome em “Árabe” é. Mas olhem que curioso: O link para quem clicar na imagem é um site que leva o nome da pessoa que digitou, seguido do sexo que a pessoa selecionou e um número, que chuto que deve ser a iteração daquele nome que apareceu no site. Ou seja, quando você clica no link, o site já pode saber exatamente quem foi a pessoa rendeu um click de sucesso.

Aí vem a segunda parte: O site pede o seu nome. Vamos testar com um nome que todo mundo sabe o que significa: digamos: Saxofone

Saxofone é um instrumento musical inventado pelo belga Adolphe Sax. Qual o significado oculto por trás desse nome? Sax é sobrenome do inventor, Phone vem do grego phonus, significa “voz”. Mas qual o significado árabe de Saxofone?

Mas será que é mesmo? Acho que o nome Saxofone é algo único, não?

Pois bem, agora é só compartilhar e o que acontece é que o link que você clica para compartilhar no Facebook é o próprio site que vai postar por você na sua página. Basicamente o que você está fazendo é dar total liberdade para que uma página sabe-se lá onde, sabe-se lá de quem utilize o seu nome para colocar conteúdo no Facebook.

E aí você me pergunta: Onde rola o dinheiro? Bem, o dinheiro vem das propagandas que eu ocultei utilizando software para bloquear propagandas. Mas veja aqui como é a página sem bloquear propagandas:

Basicamente são propagandas que rendem dinheiro para o site, quando elas são exibidas e quando elas são clicadas. Aqui está a descrição de como elas funcionam: Google Adsense

Mas, lembre-se... há também a obscura maneira de o site poder rastrear de onde vem os cliques criando uma URL baseada no nome que você testou, mais a possibilidade dele poder postar coisas em seu nome. Provavelmente isso em um primeiro momento não vai te causar nenhum problema de imediato, mas se um site do tipo for mal intencionado, eles podem facilmente identificar ligações entre pessoas e começar a descobrir o que você gosta, quem são seus amigos no Facebook, etc... E o que as pessoas podem fazer com isso?

Bom, digamos que eu verifiquei no site qual significado do meu nome em “Árabe” e compartilhei no meu Facebook. Aí meu amigo vai lá, clica no link que eu compartilhei e vê qual o significado do nome dele em “Árabe”. Assim já é possível ver por exemplo que essas duas contas podem ter alguma ligação de amizade. Essa ligação fica armazenada em algum lugar.

Eventualmente esse meu amigo vai viajar. Ele posta fotos da viagem dele com seu smartphone, com

a função GPS ligada. Essas postagens são públicas. Isso mostra facilmente que ele não está em sua casa. Eventualmente algum golpista descobrem qual o e-mail dele, qual o meu e-mail e consegue acesso à informação lá de trás, a informação que nos liga por “suposta amizade no facebook”. Aí pode-se facilmente gerar um golpe de engenharia social: Imagine que eu posso receber um e-mail de nomedomeuamigo@gmail.com (ou outro provedor conhecido) dizendo que ele teve problemas em sua viagem e está precisando de uma transferência bancária. Dependendo do nível de sites, aplicativos e tudo mais que o meu amigo utiliza, as informações sobre ele podem ser todas verídicas, que podem facilmente me fazer acreditar que é ele mesmo. A partir daí está jogada a isca, cair ou não é de cada um.

Por mais experiente que você seja na internet, sempre vai ter alguém querendo aplicar esse golpe com você. Na USP mesmo já tiveram casos de professores que estavam viajando e várias pessoas receberam esse tipo de golpe tentando ganhar algum dinheiro. Os e-mails eram contas verdadeiras criadas em provedores de e-mail gratuitos e os dados eram todos verídicos, exceto que aquele e-mail não era o do professor e o professor não estava precisando de dinheiro. Alguns chegaram a responder e receberam um número de conta para depósito, mas por sorte ninguém chegou a depositar.

Em casa já ligaram dizendo que o cartão de minha mãe havia sido clonado e que eles precisavam confirmar alguns dados do cartão. Ela já havia passado várias informações até que o estelionatário pediu que ela começasse a digitar algumas coisas no teclado do telefone e ela se recusou. O vizinho não teve a mesma inteligência: digitou as coisas e até foi um “motoboy do banco” pegar os cartões dele em casa.

Então nesta guerra digital que temos por aí, não seja você uma vítima. Não deixe suas informações livres para qualquer um na internet, tome muito cuidado com fraudes eletrônicas, desconfie de todos aplicativos de celular e extensões de navegadores e principalmente cuidado com sites “inofensivos”. Alguns podem até apenas ganhar dinheiro com a propaganda que eles exibem para você, que já é algo extremamente ofensivo pois a maioria das propagandas hoje em dia leva em conta os sites que você visitou para te oferecer o anúncio correto, mas muitos deles vão basicamente ter seus dados de redes sociais de graça para depois usá-los contra você.

Para maiores informações, recomendamos a Cartilha CERT