Engenharia Social: mentiras cibernéticas

Muitas pessoas duvidam da segurança na internet e com isso criam uma série de questionamentos, nascendo assim os falsos mitos e as grandes lendas.

Existem poucas verdades e muitas mentiras, porém algo que posso afirmar, é que não existe uma rede 100% segura.

E um dos principais culpados desta vulnerabilidade existente nas redes domésticas e corporativas são os próprios usuários.

Os usuários muitas vezes se questionam como são feitas as invasões de computadores e aquele que tenta se proteger quase sempre comete diversos erros que facilitam esta invasão.

Você já ouviu falar de engenharia social?

É a prática utilizada pelos invasores para obter acesso as informações sigilosas, através da enganação, fazendo mau uso da confiança das pessoas.

Podemos dizer que a engenharia social é a “Arte de enganar”.

Acredite, na rede o seu melhor amigo pode ser o seu maior inimigo, pois ele é a pessoa que mais conhece suas virtudes e principalmente fraquezas. Então se pergunte, desde quando ele é seu grande amigo?

O “engenheiro social” tenta de alguma forma instalar programas maliciosos na máquina do usuário para abrir caminho para a invasão.

Porém, esse é um processo lento que deve contar com a boa vontade do nosso “amigo” usuário, que quase sempre cai nas armadilhas do invasor.

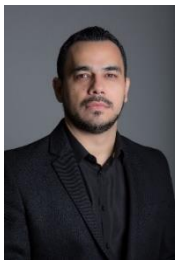
Uma das formas de invasão é através de e-mails, onde no corpo desta correspondência encontramos sempre um link. O invasor sabe que o usuário tem medos, necessidades e uma forte impulsão em realizar cliques com seu mouse

quando recebe recados com mensagens dizendo: “Clique aqui”, “Veja isso” ou “Baixe o arquivo”, no qual ao clicar será levado direitinho onde o invasor deseja. Estes e-mails possuem remetentes falsos com o nome de órgãos públicos, empresas de telefonia, nome no mercado, instituições financeiras ou muitas vezes com o nome de um amigo.

Bom, mesmo sabendo que não existe 100% de segurança, faça sua parte, desconfie do que vem muito fácil, mulheres e homens perfeitos existem, mas talvez não estarão toda sexta a noite na internet sem ter o que fazer. Links são feitos pra clicar, mas antes de apertar o botão esquerdo tenha atenção, não confie em todos e-mails que recebe, leia com cuidado

o nome dos destinatários e perceba também que o grande invasor é um assassino do seu idioma e um péssimo designer, tome cuidados com mensagens de amigos, ele talvez também seja uma vítima que sem saber está passando um software mal intencionado a você. Suas senhas devem ter certa complexidade e deve sofrer alterações periódicas, lembre-se que datas são senhas tão vulneráveis que até alguns sites rejeitam este tipo.

Por último, softwares de proteção não são feitos apenas para instalar, também são feitos para serem atualizados.



Jefferson Costa
Especialista em
Educação e Tecnologia
www.jeffersoncosta.com.br