



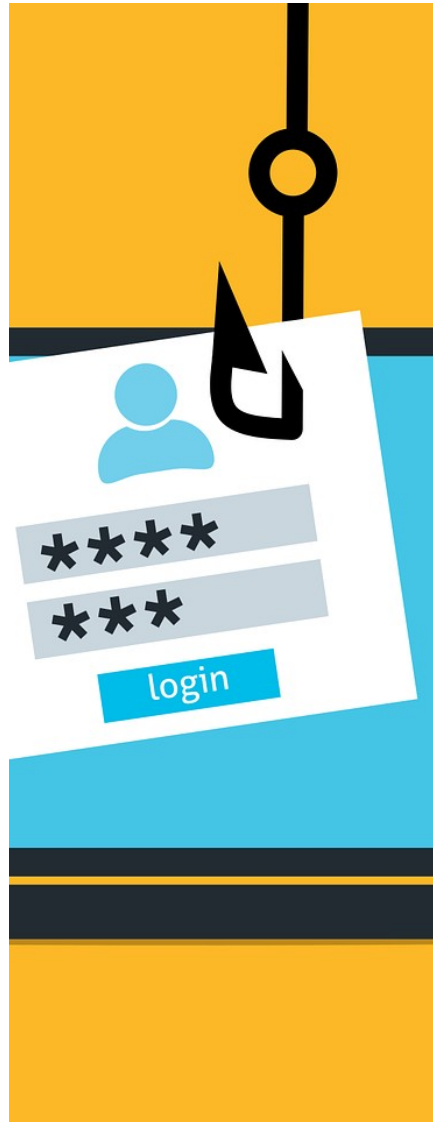
Autoria: Silvio Ferreira
Finalidade: educativa e comunitária
(Extensão UniCV)

Essencial saber



Este capítulo é uma continuação natural do capítulo 01, onde já estudamos as emoções básicas e secundárias do ser humano e fiz até um gancho com os setes pecados capitais.

Agora daremos sequência e entenderemos como que tudo isso que foi estudado se encaixa perfeitamente neste livro. Tudo que foi estudado lá é necessário para termos uma base sólida para o que vem agora: engenharia social. Tudo agora fará sentido.



A engenharia social

A engenharia social possui técnicas, e a maioria dessas técnicas se resumem em obter informações pessoais ou privilegiadas da vítima.

E para conseguir isso o fraudador irá enganar essas vítimas através, por exemplo, de identificações falsas, conseguindo a sua confiança, o seu carisma ou despertando sua curiosidade ou senso de urgência (só para citar como exemplo).

O primeiro ataque (que seria a isca propriamente dita) pode ser feito através de um telefone ou e-mail por exemplo. Mas, não se resumem a isso.

Um outro exemplo de isca pode ser um simples DVD ou pen drive deixado pelo próprio fraudador na empresa. O fraudador pode, inclusive, conversar pessoalmente com algum funcionário e depois deixar com ele a isca. No capítulo 02 eu já dei um exemplo dessa prática. Vamos recapitular:

“Imagine a seguinte situação: você trabalha em uma grande empresa, e em um determinado dia, quando se encaminhava até a sua sala de trabalho encontrou dentro de um elevador um CD ou um DVD escrito “demonstrativo de salários da empresa”, ou, “lista de demissão mês atual”. São frases fortes não?!

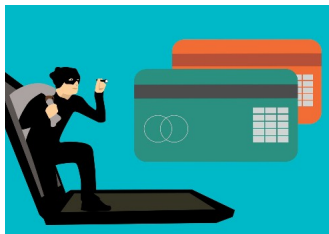
Você mais que curioso correu para seu computador para ver quanto as pessoas estão ganhando ou quem será demitido. Será que seu nome está na lista?

Ao abrir o suposto documento é exibida a mensagem: “versão do sistema incompatível”.

Ou você tentaria novamente em outro computador ou deixaria de lado.

Mas o que você não sabe é que este CD ou DVD foi deixado por... “

Por um fraudador. Um cibercriminoso. Um golpista. Você escolhe o nome. O fato é que foi usada a engenharia social



Se o exemplo anterior fosse real e tivesse acontecido com você, qual emoção você sentiria ao se deparar com o tal DVD ou pen drive? Medo? Curiosidade? Outra? Alguma emoção correto?

Esse é o ponto. A engenharia social trabalha, e muito, no âmbito da manipulação das emoções, no jogo psicológico. Quanto mais facilmente a pessoa for manipulável emocionalmente, maiores as chances dela executar uma determinada ação que culminará no roubo de suas informações pessoais, empresariais ou qualquer outro tipo de informação.

Um jovem que sonha muito em ter um videogame pode cair facilmente em golpes aplicados em sites conhecidos, como a OLX (ou outros sites), onde paga-se e não se recebe o produto.

Uma pessoa que quer muito viajar, ela está deprimida, pouco dinheiro, vendo seus amigos irem passear e “somente ela que não”, pode cair facilmente em golpes de vendas de pacotes de viagens ou passagens aéreas pela metade do preço convencional.

A engenharia social além de trabalhar na manipulação das emoções, depende fortemente de interação da vítima com o fraudador ou com as iscas deixadas pelo fraudador, ou ambos. Somente dessa forma é que se consegue levar a vítima a tomar decisões enganosas e envolvendo quebra de segurança.

Por que a engenharia social funciona?

Em um primeiro momento pode parecer ser algo “bobo”. Mas não é. Podemos até pensar: nunca cairei em um golpe desses. Isso nunca vai acontecer comigo. Concordo sim, principalmente porque você está estudando, está buscando informações. O caminho da segurança é esse.

Mas muitos são pegos nessas armadilhas traiçoeiras. Sabe os dois exemplos que dei anteriormente? Do garoto que queria comprar um videogame e da pessoa que queria viajar? São casos reais.

São pessoas próximas à mim. Um levou levou calote na OLX e a outra levou calote ao deslumbrar a possibilidade de comprar um pacote aéreo muito mais barato.

Nesse exato momento, milhares de tentativas de golpes estão sendo aplicados. Do mais variados tipos, de diversas maneiras, dos mais diversos lugares.

Nesse exato momento tem pessoas de dentro de penitenciárias ligando para possíveis vítimas e dizendo que elas ganharam um carro zero quilômetro de alguma promoção que ela sequer estava cadastrada. Muitas cairão nos golpes.

Por que muitas cairão nos golpes? A resposta para essa pergunta já está no capítulo 01:

“Tudo isso só é possível porque eles exploram, antes de qualquer coisa, a maior falha de todas: a falha humana. Cibercriminosos usam, exploram e abusam de nossas próprias vulnerabilidades. As nossas fraquezas, medos e ambições. “

A engenharia social não depende de plataforma de sistema operacional, softwares e não importa quantas camadas de segurança há em uma empresa ou sistema.

Isso porque ela vai atacar o elemento mais falho em qualquer plataforma ou sistema de segurança: o ser humano.

O ser humano possui traços comportamentais e psicológicos que podem tornar até o sistema mais protegido e seguro em um sistema falho. Dentre esses traços se pode destacar as emoções humanas.

As emoções têm o forte poder de dominar uma pessoa. Uma pessoa sob forte raiva, medo ou ciúmes (só para citar como exemplo) pode tomar decisões sem pensar, sem a devida atenção. Pode inclusive não se importar com o resultado de suas ações.

Jorge Bucay, médico e escritor argentino, é autor da frase que resume tudo isso:

“Não somos responsáveis pelas emoções, mas sim do que fazemos com as emoções.”

Vulnerabilidades emocionais

Muitas iscas digitais são criadas para explorar, e muito, diversas emoções. E não é somente iscas digitais. Você pode simplesmente receber uma ligação de alguém se passando por uma operadora de cartão, dizendo que uma compra suspeita de um valor muito alto foi feita em seu cartão (e para desbloquear eles irão pedir os dados do seu cartão. Obvio que isso é fraude, golpe).



Portanto, perceba que iscas digitais podem ser criadas sem o uso de muita tecnologia. O fraudador pode literalmente ligar para você, ou pior, pode abordar pessoalmente você. Inclusive, isso se chama no-tech hacking (que abordo no próximo tópico).

Portanto, vamos finalmente entender um pouco mais sobre como as emoções podem ser exploradas:

- **Medo:** é uma emoção muito explorada, muitas iscas são criadas para pegar vítimas exatamente pelo medo. Imagine o seguinte: e se você receber um e-mail dizendo que fotos íntimas suas vazaram na internet, ou que você está recebendo uma intimação da justiça, ou do tribunal regional do trabalho, ou que sua conta será bloqueada e por aí vai? Muitas iscas digitais são criadas dessa forma;
- **Curiosidade:** diversas iscas exploram a curiosidade. Você pode receber um e-mail dizendo que tem um vídeo íntimo seu vazado na internet, ou fotos sigilosos (veja como isso pode ser eficiente: uma mesma isca pode pegar pessoas pelo medo ou pela curiosidade), ou ainda que seguindo simples instruções você ganhará algum prêmio (que pode ser até em dinheiro), descobrir como comprar passagens aéreas quase de graça, etc;
- **Solidariedade:** quer um exemplo clássico? É o famoso golpe da campanha, ou vaquinha, para ajudar a criança que está muito doente, muitas vezes com câncer, só que o dinheiro nunca vai chegar na criança de fato. Os pais da criança sequer sabem que existia tal campanha. É preciso ter cuidado. Se quiseres ajudar, procure primeiro saber se a campanha é legítima. Ligue para a fundação que está por trás da campanha, vá até o local (se possível). Ajudar o próximo é um gesto de bondade e é algo importante, mas quando é real. Muito cuidado com campanhas de doações falsas, ganhar dinheiro, descontos imperdíveis, venda de produtos cujo dinheiro será revertido em prol de entidades beneficentes, etc.

Aprenda a questionar determinadas situações e não aja somente pela emoção;

- **Preguiça:** já dei um exemplo clássico que pode ser usado aqui. O famoso recurso de memorizar senha que abordei no capítulo 03. E lá afirmei que muitas vezes o uso desse sistema está ligado à própria preguiça. Afinal, para que digitar a senha toda vez que for acessar o sistema, se ele pode memorizá-la? O perigo mora aí. Qualquer um que conseguir chegar até esse computador acessará facilmente aquilo que a senha deveria proteger. Cuidado com isso. Essa prática, em empresas, deveria ser banida;
- **Vaidade:** que tal comprar agora um iphone 13 pela metade do preço? Clique no link oficial nos próximos 15 minutos e ganhe um carregador e um EarPods! “Uau”, até eu quase caí no meu próprio texto. Tentador não? Principalmente se for um e-mail supostamente enviado por uma empresa famosa e conhecida, e a página do link for exatamente igual à página oficial/original da tal empresa famosa e conhecida. Inclusive, iscas como essa exploram muito mais do que vaidade. Exploram gula, luxúria e soberba (isso mesmo, eis aqui alguns dos pecados capitais que citei no capítulo 01).
- **Ansiedade:** é fato que vivemos em uma sociedade de pessoas ansiosas. Tudo é muito rápido e voa na velocidade da urgência. As pessoas estão lendo cada vez menos, os vídeos agora são cada vez menores, ler o contrato do serviço para quê? Pergunte a um jovem o que é um documentário e ele terá dificuldade para explicar com exatidão, mas, pergunte o que é TikTok, Kwai, Reels ou Shorts e a resposta estará na ponta da língua. O resultado dessa ansiedade generalizada e de toda essa pressa e urgência, é que muitos clicam em links

(iscas) sem sequer pensar no que estava fazendo, são incapazes de criar suspeitas sobre a situação, por mais absurda que seja. É assim que milhares de vítimas são pegas. É comum recebermos em nossos e-mails avisos de cancelamentos e bloqueios de serviços que sequer usamos, de bancos que nunca fomos clientes. Mesmo assim milhares clicam nos links desses e-mails, mesmo quando não são clientes e/ou nunca usaram o tal serviço. Mas a pressa é tamanha, a desatenção é vergonhosamente deixada de lado, que muitos clicam no link, preocupados, para resolver a questão o mais rápido possível.

Esses são somente alguns exemplos. Poderia continuar aqui escrevendo exemplos e mais exemplos para cada emoção básica e secundária e para cada pecado capital. Mas por hora, o que expus aqui é suficiente.

No Tech Hacking

Quando um ataque não necessita de aparatos tecnológicos como computadores, muitas vezes nem telefone sequer, é chamado de no-tech hacking.

Esse termo pode ser explicado de diversas formas. Uma delas seria algo tipo hackear sem tecnologia.

O no-tech hacking é uma técnica que pode, inclusive, ser usada para testar a segurança de uma empresa ou organização.

E quais seriam os tipos de ataques no-tech hacking? Vou citar alguns só para exemplificar:

- **Dumpster diving:** é vasculhar o lixo da empresa e/ou pessoal alvo. Através do lixo muitas informações podem ser conseguidas, tais como nomes que estão em contas e as próprias contas, extratos bancários, números de telefones e até listas de números de telefones, memorandos, manuais, calendários de reuniões e tudo mais que for possível. Quanto mais informações, melhor serão os ataques. E todas as informações conseguidas podem ser usadas de muitas formas. Ligações podem ser realizadas para a empresa, onde a pessoa pode simplesmente fingir ser o gerente de algum banco, ou, o gerente da sede da empresa que precisa acessar urgentemente o banco de dados, etc. Muito cuidado com o que é jogado no lixo. O ideal é que na empresa tenha uma máquina picotadora de papel, e todos os papéis devem ser destruídos nela antes de irem para o lixo;
- **Shoulder surfing:** é um tipo de técnica usada para obter informações pessoais (como senhas) no estilo “olhando por cima dos ombros” da vítima. O observador ficará atento a cada tecla pressionada, ou, ouvirá com muita atenção ao que está sendo falado. Por isso, cuidado ao digitar senhas em qualquer lugar, se perceber que tem alguém observando o seu teclado, muito perto, o ideal é pedir, se possível e com delicadeza, licença à pessoa. Afinal você precisa acessar um sistema que possui acesso restrito, não se trata de uma senha pública;
- **Lock picking:** é a arte, ou o estudo, de como funciona as fechaduras de portas e cadeados e tudo mais. Aqui envolve o estudo do funcionamento desses dispositivos e ferramentas que podem ser usadas para abri-los;

- **Tailgating:** basicamente, é quando alguém se infiltra (consegue entrar) em algum lugar usando outras pessoas. Vou citar um exemplo clássico, que é usado em filmes, séries e livros: o invasor segue, observa ou fica aguardando uma pessoa que tem acesso ao local que ela deseja entrar. Pode ser, por exemplo, em um prédio. Imagine que ele não tem acesso ao prédio, há uma porta ou portão que somente os moradores conseguem destravar (pelo lado de dentro e através do interfone por exemplo). O invasor aguarda paciente alguém sair, e quando finalmente alguém abre ela se encaminha naturalmente e tentar entrar como se fosse um morador do local. É a famosa frase “Ei! Segure a porta, por favor!”