MINISTÉRIO DA DEFESA
COMANDO DA AERONÁUTICA

INTELIGÊNCIA

FCA 200 - 3

PREVENÇÃO À ENGENHARIA SOCIAL

2009

MINISTÉRIO DA DEFESA
COMANDO DA AERONÁUTICA
CENTRO DE INTELIGÊNICA DA AERONÁUTICA

INTELIGÊNCIA

FCA 200-3

PREVENÇÃO À ENGENHARIA SOCIAL

2009

MINISTÉRIO DA DEFESA
COMANDO DA AERONÁUTICA

PORTARIA Nº 02/CIAER , DE 8 DE OUTUBRO DE 2009.

Aprova a edição do Folheto que dispõe sobre Prevenção à Engenharia Social.

O CHEFE DO CENTRO DE INTELIGÊNCIA DA AERONÁUTICA, tendo em vista o disposto no Inciso II, do art. 4º do Regulamento do Centro de Inteligência da Aeronáutica, aprovado pela Portaria nº C-7/GC3, de 27 de setembro de 2005, resolve:

Art. 1º Aprovar a edição do FCA 200-3 "Prevenção à Engenharia Social", que com esta baixa.

Art. 2º Esta Portaria entra em vigor na data de sua publicação.

Brig Ar PAULO AFONSO PINHEIRO LARI
Chefe do CIAER

(Publicado no BCA nº 206, de 6 de novembro de 2009)

SUMÁRIO

PREFÁCIO

Todo sistema/rede deve ter sua confidencialidade, integridade e disponibilidade preservadas. Essas características podem ser comprometidas, direta ou indiretamente, pelos riscos da Engenharia Social.

Treinamentos acerca de consciência de segurança oferecem uma defesa primária contra a Engenharia Social. Pesquisas recentes, em psicologia social, demonstram, entretanto, que treinamentos de consciência de segurança, sozinhos, não capacitam o pessoal a resistir à persuasão da Engenharia Social.

A defesa contra engenharia social deve considerar o que se conhece acerca da psicologia da persuasão e desenvolver o conhecimento para entender o ataque persuasivo e a dinâmica da construção da resistência a isso.

A Engenharia Social é diversa e suficientemente complexa para necessitar de uma defesa multinível que complemente um sistema de defesa em profundidade.

1 DISPOSIÇÕES PRELIMINARES

1.1 FINALIDADE

O presente Folheto tem por finalidade recomendar aos Comandantes, Chefes e Diretores procedimentos referentes à prevenção de ações adversas, que utilizam métodos de Engenharia Social, no âmbito do Comando da Aeronáutica (COMAER).

1.2 ÂMBITO

O presente Folheto aplica-se a todas as OM do COMAER.

2 A ENGENHARIA SOCIAL

2.1 DEFINIÇÃO

Em geral, Engenharia Social é o processo de enganar (manipular) pessoas de forma que elas forneçam diretamente ou proporcionem acesso à informação privada, classificada ou privilegiada a alguém que não deveria tê-la.

2.2 CARACTERÍSTICAS DA ENGENHARIA SOCIAL

Há inúmeros métodos utilizados para conseguir informação, ou acesso a ela, por meio do pessoal da organização. Alguns dos mais comuns incluem: se passar por um membro da organização, troca de favores, convencimento do alvo de que o pedido é normal, assegurar à vítima de que ele não é responsável pelo que está fazendo e apelar para velhas amizades.

Ataques de engenharia social estão cada vez mais frequentes e podem ser técnicos ou não-técnicos; ambos manipulam o pessoal da organização para conseguir informação não autorizada que pode ser utilizada contra a própria organização ou para fins criminais.

A Engenharia Social concentra-se em explorar as fraquezas das pessoas, dos sistemas de TI (tecnologia da informação) e dos processos de segurança de TI.

Organizações e companhias estratégicas ao redor do mundo têm reportado tentativas de utilização de técnicas de engenharia social para obter informações internas por meio de telefones, e-mail e contatos pessoais.

O pessoal mais visado tem sido aqueles que desenvolvem tarefas como: atendimento ao público (especialmente em áreas de TI), *helpdesk*, recepcionistas, guardas, seguranças, pessoal de limpeza e serviços de alimentação.

2.3 PRINCÍPIOS DA ENGENHARIA SOCIAL

2.3.1 DESENVOLVIMENTO DA CONFIANÇA

O primeiro passo é estabelecer confiança com a pessoa de interesse (vítima). O agente (hacker) habilidoso obterá informações de forma muito lenta, pedindo pequenos favores ou obtendo informações por meio de conversas aparentemente inocentes. A engenharia social é, geralmente, bem sucedida, pois as pessoas são naturalmente prestativas.

2.3.2 ENGENHARIA SOCIAL REVERSA

Uma forma muito comum desse princípio é o agente (comumente um hacker) causar um problema num sistema ou rede de TI e, posteriormente, se oferecer para saná-lo, tornando-se assim um “herói” ou “salvador da pátria” e, com isso, ganhando a confiança e o crédito dos outros.

2.3.3 MÍDIAS E ACESSOS

Além do telefone, muito usual, acesso físico aos locais de trabalho é utilizado - serviços contratados, pessoal de limpeza, suporte técnico de software, hardware etc. Grande

quantidade de informação pode ser recolhida de mesas, lixo, diretórios telefônicos, edição ou reedição de programas, utilizados por sistemas de TI para se obter senhas e logins, entre outros.

2.4 GATILHOS PSICOLÓGICOS POR TRÁS DA ENGENHARIA SOCIAL

2.4.1 O ESTADO EMOCIONAL

Quanto mais acentuado está o estado emocional de uma pessoa – raiva, ansiedade, surpresa, medo, pânico, etc – maior a probabilidade de um agente lograr obter mais informações que normalmente seria possível. O agente provoca essa reação por meio de comentários inseridos na interação com a vítima (promessas de prêmios, dinheiro, ameaça de demissão ou prejuízo profissional, etc). O afloramento de um estado emocional extremo funciona como poderoso elemento de distração e diminui a capacidade da vítima de avaliar, pensar de forma lógica e de contra-argumentar.

Pensamento contrafactual é um fenômeno descrito quando a expectativa de, por exemplo, receber um grande prêmio, paralisa a capacidade de raciocínio lógico de uma pessoa. A pessoa passa a ignorar o fato de ser improvável e remota aquela possibilidade e arrisca valores e bens valiosos – informação ou acesso a ela – diante da possibilidade do prêmio.

2.4.2 SOBRECARGA

Falsas premissas são passadas despercebidas quando são ouvidas rapidamente e estão entremeadas por clichês. Esse é o gatilho psicológico da sobrecarga. Com muita informação para processar, as pessoas tornam-se mentalmente passivas – elas absorvem mais informação do que podem avaliar. Argumentar a partir de uma perspectiva inesperada pode, também, provocar a sobrecarga. A vítima necessita de tempo para processar a nova perspectiva, mas esse tempo não está disponível. A vítima fica, dessa forma, mais inclinada a aceitar argumentos que deveriam ser refutados.

2.4.3 RECIPROCIDADE

Trata-se de uma regra social na qual se alguém dá ou promete algo a outra pessoa essa última sente-se obrigada a retribuir-lhe o favor, mesmo quando aquilo que lhe foi dado não foi pedido ou quando o pedido em troca está muito além do recebido. Esse gatilho psicológico é muito útil, principalmente no mundo corporativo onde as pessoas tendem a não avaliar os pedidos de forma aprofundada, pois, "se alguém nos ajudou em algo aquela pessoa está do nosso lado e não nos oferece perigo". Esse princípio é muito utilizado em engenharia social reversa.

Outra maneira de reciprocidade é demonstrada por experiências onde duas pessoas discordam de algo; nessa situação quando uma delas cede em algum ponto – não importando quão pequeno seja – a outra irá sentir-se obrigada a ceder também. Novamente, no ambiente corporativo, isso é muito comum quando alguém ajuda outra pessoa em algo com a expectativa de, eventualmente, receber algum favor em troca. Esse sistema de intercâmbio não oficial é considerado inestimável se alguém quer ser bem sucedido. A engenharia social utiliza esse sistema porque suas motivações são desonestas e aquilo que se busca não poderia ser dado a custo zero.

2.4.4 RELACIONAMENTOS ENGANOSOS

Consiste na utilização de relacionamentos com intenção de manipular outras pessoas. Uma das maneiras de fazer isso é compartilhar informações e discutir a respeito de inimigos comuns. Uma vez estabelecido o relacionamento há numerosas maneiras de explorar isto. Por exemplo: um hacker, certa vez, após manter cerca de uma hora de conversa com um técnico da AOL (American On Line – provedor de Internet) deixou "escapar" que seu carro estava a venda. O técnico mostrou interesse e ele enviou-lhe um arquivo com a foto do carro. O arquivo continha um backdoor que conseguiu abrir uma conexão através do firewall da AOL.

Outra forma de o engenheiro social conseguir um rápido relacionamento é agir de forma a fazer a vítima acreditar que tem muito em comum com ele. Quando a vítima percebe que pensa de forma similar, demonstra interesses iguais e compartilha dos mesmos valores de vida sente-se fortemente motivada a tratar seu interlocutor de forma favorável, acreditando nele mesmo sem motivação legítima.

2.4.5 DISPERSÃO DA RESPONSABILIDADE E DO DEVER MORAL

É fazer a vítima acreditar que não será responsabilizada pelas suas ações. Ironicamente esse gatilho funciona bem quando o dever moral é usado como motivação para a persuasão, pois nesse caso a vítima é levada a crer que está fazendo algo para salvar alguma pessoa, ajudar a organização ou, pelo menos, evitar sentir-se culpado.

A vítima é levada a crer que está tomando decisões que farão a diferença entre o sucesso e o fracasso da sua organização ou de alguém em particular que esteja dependendo dessas decisões para manter seu emprego, sua carreira etc.

2.4.6 AUTORIDADE

Pessoas são condicionadas a atender à autoridade. Esse gatilho é mais poderoso quando é difícil verificar a legitimidade da autoridade. Essa falha de perspectiva faz com que se abra um amplo leque de oportunidades para alguém se fazendo passar por uma autoridade.

Por exemplo: certa vez, numa experiência, 22 diferentes enfermeiras em locais variados, foram orientadas, por telefone (contrariando as normas), a ministrar doses de remédios não autorizadas, por médicos que elas nunca viram e numa dosagem duas vezes mais alta que o máximo diário. Essas orientações deveriam ter sido questionadas, porém, em 95% dos casos, as enfermeiras estavam prosseguindo para efetuar o procedimento quando foram detidas pelos observadores.

2.4.7 INTEGRIDADE E CONSISTÊNCIA

As pessoas tendem a serem fieis aos seus compromissos no ambiente de trabalho, mesmo quando estes não parecem ser, inicialmente, muito adequados. Para alguns é uma questão de integridade fazer aquilo que disse que faria, mesmo quando há indícios de que a solicitação não é legítima. Essa tendência é tão forte que há quem faça aquilo que foi prometido por um companheiro de trabalho, na sua ausência. Nesse momento um engenheiro social aproveita-se das férias ou ausência temporária de pessoas para explorar esse gatilho.

3 DEFESA MULTINÍVEL CONTRA ENGENHARIA SOCIAL

Construir uma defesa contra a engenharia social é similar a construir qualquer defesa forte. A chave é determinar quais são as vulnerabilidades e ameaças e armar as defesas contra elas.

A defesa deve ter diversos níveis, pois se um engenheiro social conseguir penetrar num deles haverá outro para barrá-lo. Uma vez que a engenharia social tem se mostrado muito eficiente, uma estratégia multinível é crítica. Essa estratégia pode não se limitar a defesas, pois o predador de engenharia social achará ou, eventualmente, criará um ponto fraco. Dessa forma o sistema deve ser capaz de contra-atacar ou pelo menos reconhecer que está sob ataque.

O conceito de SELM (*Social Engineering Land Mines* – Minas Antiengenharia Social - MAES), plantadas nas estruturas das organizações, proporcionam a capacidade de contra-atacar, pois mais que prevenir ataques, funcionam para expor o engenheiro social.

3.1 NÍVEL FUNDAÇÃO: POLÍTICA DE SEGURANÇA VISANDO ENGENHARIA SOCIAL

O fundamento para a segurança das informações é a sua política de segurança. Esta é ainda mais crítica quando visa proteger a rede da organização contra a engenharia social, uma vez que essa última visa às pessoas que necessitam saber como responder aos questionamentos feitos e muitas vezes não estão em posição de fazer considerações se alguma informação deve ou não ser dada. Isso deve ser definido, antecipadamente, por pessoas que avaliaram meticulosamente o valor dessas informações.

Estudos em metacognição na teoria da persuasão demonstram que uma forma de aumentar a resistência à persuasão é desenvolver a confiança na consciência do pessoal. Isso pode ser feito esclarecendo e solidificando, de forma objetiva, as políticas adotadas pela organização, diminuindo assim as chances de um persuasor subjugar um membro da equipe.

A política de segurança tem que visar muitas áreas: controles de acesso à informação, configuração de contas em redes de TI, análise e aprovação de acessos, trocas de senhas, trancas (travas, fechaduras, bloqueios etc), identificações, destruição (trituração) de documentos, escolta de visitantes, etc. A política deve disciplinar e, acima de tudo, deve ser reforçada e fiscalizada a sua execução. Essa política reforçará a capacidade do pessoal resistir aos gatilhos psicológicos da "Autoridade" e da "Dispersão da responsabilidade e dever moral".

3.2 NÍVEL PARÂMETRO: TREINAMENTO DE CONSCIÊNCIA DE SEGURANÇA PARA TODOS

A política de segurança proverá as linhas mestras para o treinamento e para a motivação. A consciência de segurança é bem mais complicada que simplesmente dizer aos membros da organização para não fornecerem suas senhas a ninguém.

Os componentes da organização têm que conhecer o tipo de informação que um engenheiro social pode usar e quais tipos de conversas são suspeitos. Devem saber identificar a informação que possa ser confidencial e devem entender sua responsabilidade em

protegê-la. Eles têm que saber como dizer "não" quando necessário e ter a certeza de serem apoiados pelas suas respectivas chefias.

Todos devem saber identificar os sinais básicos que identificam um ataque de engenharia social, tais como: recusa de quem liga ou interpela em fornecer um contato, pressa, intimidação, blasonaria (referir-se a autoridades ou famosos, como se fosse amigo ou íntimo, com fins de impressionar), erros de soletração ou ortografia, perguntas estranhas, pedidos de informação classificada (proibida), etc.

Deve-se ter em mente que o engenheiro social irá, inicialmente, tentar estabelecer uma relação de confiança e posteriormente irá explorá-la para obter todo tipo de informação valiosa.

Há alguns pontos importantes no currículo de treinamento de consciência de segurança que devem ser destacados.

a) saber o que tem valor

A maioria das pessoas subestima os seus conhecimentos e acessos até sofrerem um ataque de hacker ou perderem seu disco rígido. Isso pode fazê-las compreender que aquilo em que elas vêm trabalhando há anos tem algum valor.

b) amigos não são sempre amigos

Amigos feitos por telefone, e-mail, sites de amizade, ou quem, por qualquer motivo, esteja fazendo perguntas concernentes a assuntos privilegiados, classificados ou privados podem não ser amigos de maneira nenhuma. Todos devem ter em mente que alguém que simplesmente pareça amigo não significa, de forma alguma, que seja confiável ou possa ter acesso a informações sensíveis. Dependendo do valor da informação a ser conseguida e do nível de segurança envolvido na rede da organização, o engenheiro social pode utilizar-se de medidas muito elaboradas para convencer a(s) vítima(s) que ele(a) é um amigo. Isso pode levar períodos de dias, meses ou até anos.

c) senhas são pessoais e intransferíveis

Apesar de que alguns hackers nunca pedirão a senha de alguém, outros poderão utilizar argumentos superconvincentes pelos quais a vítima deveria fornecer-lhes uma senha. Desafortunadamente, muitas pessoas sem treinamento adequado, tenderão a fornecer suas senhas sem refletir a respeito. Muitos sites oferecem prêmios a quem se associa a eles ou utiliza algum aplicativo. Não é incomum que as pessoas utilizem as mesmas senhas ou senhas muito parecidas, em diversos meios eletrônicos, com as que se utilizam em suas redes corporativas. Se o site solicita-lhe um e-mail o hacker pode, também, obter o domínio da vítima.

d) uniformes são baratos

Um engenheiro social pode apresentar-se num ambiente de trabalho fingindo ser alguém com uma razão legítima para estar ali. Em muitos locais, o simples trajar de um uniforme garantirá a entrada de alguém. É importante treinar o pessoal a não aceitar um uniforme como uma razão para alguém acessar qualquer lugar. Uniformes são baratos e estão disponíveis para compra, oficialmente ou não. Deve-se

ter em mente que quase toda informação valiosa justifica alguém penetrar num sistema de TI e com trinta segundos de acesso configurar uma sabotagem (vírus, armadilha, etc) de engenharia reversa.

3.3 NÍVEL FORTALEZA: TREINAMENTO DE RESISTÊNCIA PARA PESSOAL EM POSIÇÕES-CHAVE

Essas pessoas incluem, não somente os cargos mais elevados, mas também, pessoas que desempenham funções mais singelas, porém de grande proximidade com aqueles que detém o conhecimento mais valioso, tais como: secretárias(os), serventes, motoristas, telefonistas, atendentes de público externo, gerentes e administradores de sistemas, ajudantes-de-ordens, assessores, etc.

Estudos recentes demonstram que o treinamento de resistência pode ser efetivo no endurecimento das pessoas à persuasão. Muitas técnicas de resistência, do campo da psicologia social, podem ser aplicadas para ajudar adequadamente a preparar o pessoal para resistir às técnicas de persuasão do engenheiro social. Algumas delas são:

a) inoculação

Funciona como uma vacina, onde se expõe a vítima ao "vírus" enfraquecido para se construir resistência específica. É quando se acostuma o pessoal com os argumentos que o engenheiro social utilizaria, expondo-os a tais argumentos e treinando-os com contra-argumentos fortes para desmontar a argumentação de ataque. O delicado, nesse caso, é o treinador saber antecipar os argumentos que seriam utilizados pela engenharia social.

b) alerta antecipado

A aplicação prática do treinamento de resistência consiste em esclarecer aos componentes da organização que o engenheiro social não só tentará persuadi-los, mas, principalmente, que os seus argumentos serão manipuladores, enganosos e falsos. O pessoal tem que ser alertado que as ações do hacker são criminosas e tentarão roubar-lhes algo. Esses esclarecimentos, de forma muito objetiva, direta, "preto no branco", são essenciais para que o alerta antecipado seja efetivo.

c) cheque de realidade

Uma das razões pelas quais o treinamento de consciência de segurança falha é que o pessoal envolvido tende a ter um otimismo irreal a respeito da sua própria invulnerabilidade. Essa percepção leva muitos a ignorarem os riscos legítimos e falharem em tomar as medidas para apartá-los. Entretanto, uma vez eles sejam enganados, isso demonstra a eles que são verdadeiramente vulneráveis, o treinamento torna-se muito mais efetivo.

Há três estágios na percepção da susceptibilidade ao risco. A primeira é a consciência – saber que há o risco (é onde para a maior parte dos treinamentos em consciência de segurança). A segunda é a susceptibilidade geral – que é acreditar na probabilidade do risco dos outros. O terceiro estágio é o da susceptibilidade pessoal que é atingida quando se percebe a própria vulnerabilidade. Um programa de treinamento de

consciência e de resistência de segurança terá valor limitado se não for atingido o terceiro estágio – percepção das vulnerabilidades pessoais.

Apenas dizer a um membro da organização que ele pode ser iludido pela engenharia social não é suficiente para que ele deixe a sua atitude de invulnerabilidade.

Estudos revelam que o treinamento de resistência deve dar a oportunidade dos participantes serem iludidos e enganados antes de começarem as aulas.

Há inúmeras possibilidades de fazer isso, dependendo da imaginação de cada um, como: ligações feitas, por alguém com boa capacidade de persuasão, para tentar extrair diversos conhecimentos dos participantes do treinamento, explorando isso nas aulas; fazer um aplicativo que apareça na tela do usuário dizendo-lhe que sua senha deve ser digitada novamente, junto com seu nome de usuário, por perda de conexão, depois retornando uma mensagem dizendo-lhe que foi enganado. Ou seja, há maneiras de fazer com que o participante do treinamento sinta como é fácil ser enganado. Essa é a única forma de fazê-lo entender isso e sair de seu complexo de invulnerabilidade, passando assim a ficar atento para as táticas de engenharia social.

3.4 NÍVEL PERSISTÊNCIA: LEMBRETES CONTÍNUOS

Uma defesa multinível necessita incluir um sistema de lembretes contínuos para a necessidade da consciência de segurança. Lembretes regulares e criativos são necessários para manter o pessoal alerta para os perigos que podem estar espreitando do outro lado de uma ligação “amistosa”.

Um bom exemplo disso é o que ocorre em departamentos de polícia, onde se reportam os policiais mortos em ação. Isso faz com que o pessoal lembre-se, constantemente, dos riscos da profissão e esteja atento e preparado para eles. Da mesma forma, deve-se lembrar, aos componentes da organização, a respeito das possibilidades de ataques de hackers e de engenharia social, além de, especificamente, informar qualquer tentativa recente.

3.5 NÍVEL “PEGUEI VOCÊ”: MINAS ANTIENGENHARIA SOCIAL (MAES)

Minas antiengenharia social são armadilhas colocadas nos sistemas para realmente expor e parar um ataque. Exatamente como as minas terrestres num campo de batalha, essas armadilhas são colocadas para explodir o atacante. Ela destruirá o sigilo, talvez mutile o atacante e pare o ataque. As MAES irão alertar a vítima e o sistema de segurança da vítima que um ataque está em progresso e pode ser direcionado ou uma medida específica de segurança pode ser engajada. Algumas idéias podem ser aplicadas, dentre outras:

a) o conhecedor de todos

O conhecedor é uma pessoa que faz dessa ocupação o seu negócio, ou seja, conhecer todos que trabalham naquele setor, organização ou, ainda, que usualmente entrem ou trabalhem ali. Muitos setores já têm alguém que é, naturalmente, assim. Basta que essa pessoa seja treinada e alertada a respeito dos riscos de segurança

a respeito da presença de engenheiros sociais ou hackers e tenham o poder de fazer algo rápido de forma a direcionar um visitante sem acompanhamento. Essa MAES – mina antiengenharia social – pode ser útil mesmo na eventualidade do "invasor" estar usando credenciais ou crachás, pois hackers podem forjar essas identificações, e com isso não esperarem ser confrontados.

b) registro de segurança centralizado

Havendo um registro centralizado dos eventos de segurança, que esteja sendo monitorado por pessoal de segurança, pode ajudar a prevenir um ataque efetivo. Todas as vezes que alguém receba uma ligação suspeita, seja questionado acerca de informações sensíveis ou tenha que refazer um *login* ou uma senha, isto poderia ser registrado nesse controle centralizado. Se um hacker está obtendo informações de um membro da organização e utilizando-se delas para falar com outro membro, os padrões podem ser anotados nos registros. Tão logo o padrão seja observado, o pessoal da segurança pode tomar ações para parar o ataque e alertar os componentes da organização a respeito.

Atualizações nesse registro centralizado têm que ser monitoradas em tempo real, assim essa MAES teria que utilizar a melhor forma de comunicação disponível na organização. Notificações via e-mail para o gestor desse registro pode ser uma boa opção.

Para que esse registro centralizado seja uma MAES efetiva todos os eventos de segurança têm que ser reportados pelos membros da organização e a aderência deles a esse processo deve ser checada com frequência. O registro deve ser centralizado e monitorado de forma que o "atacante" não possa alternar para pessoas diferentes na estrutura organizacional.

c) política de retornar a ligação

Retornar a chamada para qualquer um que esteja requerendo uma troca de senha ou login. O retorno da chamada irá checar se o número de telefone corresponde ao local e função prevista no diretório telefônico para a pessoa que está requerendo o procedimento. Isso irá prevenir certos truques utilizando-se dos sistemas de PABX. As pessoas tendem a ajudar aqueles que pertencem à organização por receio de receberem reprimendas se não o fizerem.

d) perguntas-chave

Outra MAES é a utilização de perguntas padrão a serem feitas para identificar alguém que esteja buscando informações ou tentando descobrir uma senha.

- a regra das três perguntas: deve ser combinada com o pessoal (cada um dos integrantes), com antecedência. São perguntas para autenticação do interlocutor. Pode ser utilizada por pessoal de *helpdesk*, no atendimento a solicitações via meios de TI. Essas questões e suas respectivas respostas devem ser de acesso apenas do pessoal do *helpdesk*;

- pergunta falsa: é uma pergunta que possui uma falsa informação embutida. Ou o suspeito (atacante/hacker) responderá à questão de forma a corroborar a falsa informação, sendo assim descoberto, ou passará no teste e a "vítima" poderá desculpar-se

pelo engano. Exemplo: Oh, Sr José, como vai sua filha? Está se recuperando do acidente? Se o "atacante" responder que a sua filha não se acidentou ou que não possui nenhuma filha, o seu interlocutor (vítima) poderá desculpar-se pelo engano e prosseguir dizendo que se enganou, porém se o suspeito continuar falando do assunto ou corroborando a situação provavelmente terá sido identificado. Deve haver imediato reporte à segurança, nesse caso.

- política do "aguarde, por favor": a literatura de psicologia afirma com clareza que as pessoas são mais facilmente persuadidas a fazer algo questionável quando há pressa, pressão, surpresa ou sobrecarga. Uma MAES para prevenir isso é a política de colocar em espera qualquer ligação suspeita, pedido de informação privilegiada ou solicitação de troca de senhas. Isso irá parar a ação e dar a oportunidade para o operador pensar.

O ponto-chave aqui é tirar um minuto para avaliar a informação que está sendo pedida, se a solicitação é legítima, necessita de verificação ou autorização ou deve ser negada.

Essas são apenas algumas idéias. As MAES devem ser levadas a sério se uma postura defensiva tiver qualquer esperança de ser efetiva. Defesa estrita, sem qualquer ofensiva ou espionagem reversa, deixa o sistema aberto para todo e qualquer ataque contínuo.

Este tipo de rede herda as vulnerabilidades das redes de computadores, com a agravante de não necessitarem de cabos para conectá-los, tornando ainda mais fácil o trabalho do interceptador. Estão se tornando incontáveis os casos de redes sem-fio totalmente abertas e vulneráveis.

3.6 NÍVEL OFENSIVO: PRONTARRESPOSTA

O nível final de defesa é a prontarresposta. Isso é crítico a ponto de o sistema não poder esperar que o engenheiro social/hacker consiga atuar em alguém, de dentro da organização, que não se preocupe ou não conheça sobre segurança.

Deve haver algum processo, bem definido, que um membro da organização possa disparar, tão logo ele(a) suspeite de algo errado. Esse processo deve caçar, agressivamente, o "atacante/invasor" e, proativamente, alertar aos demais membros – vítimas potenciais.

Se não houver prontarresposta cada membro da organização estará lutando uma nova batalha. Nesse meio tempo o engenheiro social estará entendendo melhor as defesas da organização. Os procedimentos de prontarresposta param esse processo. Quanto mais cedo um engenheiro social for descoberto, em qualquer parte da organização, o ataque é caracterizado e os demais membros são alertados e saberão o que fazer.

4 **DISPOSIÇÕES FINAIS**

A Engenharia Social é uma ameaça muito real e que, atualmente, tem domínio de ação, geralmente, livre. Porém, isso não será sempre verdadeiro. Uma vez que se leve essa ameaça, verdadeiramente, a sério e se aplique um sistema multinível de

defesa, a Engenharia Social se tornará uma via muito mais difícil, se não impossível, de ser empregada por um engenheiro social.