

A IMPORTÂNCIA DA CAPACITAÇÃO DOS RECURSOS HUMANOS PARA SEGURANÇA DA INFORMAÇÃO

Fausto Batista da Cunha Filho¹
Aluizio Ferreira da Rocha Neto²

RESUMO

O presente trabalho tem por objetivo fazer conhecer as fragilidades existentes nos recursos humanos, no que diz respeito à segurança da informação. Para isso realizou-se um estudo de caso em uma empresa real, através de entrevista com os funcionários da mesma, bem como com a simulação de ataques de Engenharia Social aplicados sob a supervisão da diretoria. Com esses resultados em mãos, foi possível constatar os riscos existentes, bem como a necessidade de um treinamento e qualificação dos funcionários e colaboradores.

Palavras-chave: Segurança da Informação. Ataques Simulados. Engenharia Social.

THE IMPORTANCE OF HUMAN RESOURCES TRAINING FOR INFORMATION SECURITY

ABSTRACT

This work has for objective does know the existent fragilities in the human resources, with regard to information security. For this carried out a case study in a real company, through interview with the employees of the same, as well as with the simulation of attacks of Social Engineering applied under the supervision of the management. With those results in hands, it was determined risks, as well as the need of training and the qualification of the employees and collaborators.

Keywords: Information Security. Simulated Attacks. Social Engineering.

1 INTRODUÇÃO

Nos dias de hoje é comum ouvir-se falar em segurança da informação e ter o pensamento, facilmente, remetido a uma cena de filme, onde um “espião” invade uma

¹Discente do Curso de Especialização em Redes de Computadores pelo Centro Universitário do Rio Grande do Norte - UNI-RN. Bacharelado em Sistemas de Informação pelo Centro Universitário do Rio Grande do Norte - UNI-RN.

E-mail:faustofilho@gmail.com

²Docente do Curso de Especialização em Redes de Computadores do Centro Universitário do Rio Grande do Norte - UNI-RN. Mestrado em Ciência da Computação pela UNICAMP, Brasil.

E-mail: aluiziorocha@gmail.com

corporação, utilizando diversos recursos tecnológicos, para obter informações sigilosas. No entanto a realidade é bem diferente e é preciso rever esses conceitos.

A informação é um ativo que, como qualquer outro, importante para negócios, tem um valor para a organização. A segurança da informação protege a informação de diversos tipos de ameaças para garantir a continuidade dos negócios minimizar os danos ao negócio e maximizar o retorno dos investimentos e as oportunidades de negócios. (NBR ISO/IEC 17799:2001, p. 2).

As informações estão em todos os lugares, seja em casa, trabalho, e-mail, agendas pessoais, no computador e principalmente na cabeça das pessoas. É importante saber o devido valor dessas, para não compartilhá-las com pessoas indevidas.

Santos (2004, p. 21) diz que “toda informação está associada a um dado ou valor representando o suporte lógico para a mesma. É o uso que será feito deste dado e dos conceitos a ele relacionado, que o torna útil ou não.”

Toda a modernização da internet e a migração contínua dos mais diversos serviços para ela, assim como a sua integração com a rede de telefonia móvel, dada com a utilização de smartphones³, vêm contribuindo cada vez mais para sua popularização. E esta popularização, conseqüentemente, gera informações, pessoais e profissionais, que nem sempre são tratadas com a devida segurança. O que propicia a ação de estelionatários, ou pessoas que visam se aproveitar de certas informações, para benefício próprio, ou para prejudicar alguém.

Cientes disso, pessoas de má índole vêm se aproveitando da falha humana para se apossar dessas informações, utilizando métodos diversos para persuadir o seu “alvo” a lhe entregar subsídios, ou até mesmo cometer ações que lhe favoreçam. Os métodos de persuasão são conhecidos, na segurança da informação, como Engenharia Social.

Nas empresas, as informações são críticas, pois, em muitos casos, são fatores estratégicos para a manutenção desta. Para proteger suas informações, realiza-se investimentos em segurança, adquirindo equipamentos de alta tecnologia, portas com acesso biométrico, câmeras de segurança, entre outros equipamentos, que controlem e monitorem o acesso aos dados da empresa. Entretanto, é esquecido o investimento na capacitação e conscientização do recurso humano, deixando-o vulnerável para ataques de Engenharia Social.

Desta forma, as corporações, para suprirem esta nova demanda da área tecnológica, devem investir em programas de Treinamento do seu capital intelectual, ou seja, seus

³Telefone celular com funcionalidades avançadas que podem ser estendidas por meio de programas executados por seu sistema operacional.

funcionários. Para Goldstein (1991 apud LACERDA, 2003; ABBAD, 2003), o treinamento é uma aquisição sistemática de atitudes, conceitos, conhecimentos, regras ou habilidades que resultem na melhoria do desempenho no trabalho, obtidos por meio da análise de tarefas e princípios da tecnologia instrucional.

Aproveitando a inexistência de treinamentos específicos e utilizando os recursos atuais, os ataques são realizados, via telefone (voz), mensagem de texto, e-mail, sites e perfis falsos, ou até mesmo pessoalmente, com a abordagem do alvo. Para isto, a vítima é abordada na qual, usualmente é oferecido algo de seu interesse, alguma coisa que lhe seduza, algum ganho, que será obtido, desde que o abordado cumpra algum requisito.

Neste artigo analisaremos uma empresa real, que tenha informação como diferencial estratégico. Isso se dará através de entrevistas aos seus funcionários, bem como a simulação de ataques de Engenharia Social. Será realizada uma análise dos resultados obtidos, apontando intervenções para a empresa, tendo como objetivo principal constatar a importância da capacitação dos recursos humanos para a segurança da informação.

2 DESENVOLVIMENTO

2.1 Referencial Teórico

A Engenharia Social tem foco em segurança da informação e significa segundo Ulbrich e Della Valle (2011, p. 110.) “garimpagem de informações vitais sobre uma determinada pessoa, empresa, produto ou organização”, lembram ainda, que a prática de Engenharia Social é considerada crime e tem interpretação legal baseada nos crimes existentes como falsidade ideológica (art. 299⁴ do código penal), no caso de se passar por outra pessoa, ou ainda como estelionato (art. 171⁵ do código penal), quando as informações obtidas são utilizadas em fraudes financeiras. Esses crimes poderão ir de multas até a detenção do indivíduo.

Popper e Brignoli (2012) afirmam que antes de citar as diversas formas de ataque, o ideal é citar quem são os atacantes. Engana-se quem pensa que os ataques sempre são executados pelos hackers. O quadro a seguir mostra alguns tipos de intrusos e seus principais objetivos.

⁴Omitir, em documento público ou particular, declaração que dele devia constar, ou nele inserir ou fazer inserir declaração falsa ou diversa da que devia ser escrita, com o fim de prejudicar direito, criar obrigação ou alterar a verdade sobre fato juridicamente relevante.

⁵Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento.

Quadro 1 – Tipos de Intruso

Intrusos	Objetivos
Estudantes	Bisbilhotar mensagens de correio eletrônico de outras pessoas por diversão;
Hackers/Crackers	Testar sistemas de segurança, ou se apropriar de informações;
Representantes Comerciais	Descobrir planilhas de preços e cadastro de clientes;
Executivos	Descobrir plano estratégico dos concorrentes;
Ex-funcionários	Sabotagem por vingança;
Contadores	Desfalques financeiros;
Corretores de Valores	Distorcer informações para lucrar com o valor das ações;
Vigaristas	Roubar informações, como senhas e números de cartões de crédito;
Espiões	Descobrir planos militares;
Terroristas	Espalhar pânico pela rede e roubo de informações estratégicas.

Fonte: (POPPER; BRIGNOLI, 2012).

Basicamente, de acordo com Ulbrich e Della Valle (2011, p. 111), existem dois tipos principais de ataque, o direto e o indireto.

Já o ataque direto, trata-se da abordagem da vítima, que pode ser realizado via telefone, fax, ou em alguns casos pessoalmente e exigem um prévio planejamento para que se consiga obter o sucesso.

O ataque indireto está relacionado com o crime no meio digital, buscando informações com o auxílio direto da tecnologia, como instalação de “Cavalos de Tróia⁶”, e-mail e/ou sítios de internet com a utilização de códigos maliciosos, que passam a enviar ao seu executor, informações diversas coletadas no computador da vítima, como numa espécie de grampo digital.

Em geral, associamos a prevenção de um ataque à Segurança da Informação às correções de falhas computacionais, que podem levar ao sucesso destes ataques (BRAGA, 2012). No entanto, empresas e usuários domésticos precisam praticar a segurança diariamente, através de alguns procedimentos adotados, como por exemplo, evitar compartilhar informações pessoais. Outra atitude, que deve ser adotada, é tratar senhas como assinaturas, pois ao compartilhar essas informações, é preciso lembrar que qualquer ação, realizada com a utilização de uma

⁶São softwares, que em analogia com a história romana, de dentro da máquina infectada, permite acesso ao invasor externo.

senha específica, será remetida ao proprietário e não a quem utilizou indevidamente, até que se prove o contrário.

De acordo com Borges-Andrade (2002) uma das características essenciais do conceito de treinamento é a noção de que ele representa um esforço despendido pelas organizações para propiciar oportunidades de aprendizagem aos seus integrantes. Ele está tradicionalmente relacionado à identificação e superação de deficiências no desempenho de empregados, preparação de empregados para novas funções e adaptação da mão de obra à introdução de novas tecnologias no trabalho.

Nos dias atuais, todos nós nos deparamos com uma quantidade enorme de informações, vinda de todos os lugares, seja em ambiente corporativo, ou doméstico, em meio digital, ou físico. Dado isso, necessitamos armazenar e controlar essas informações de maneira organizada e segura. Para isso necessita saber o devido valor que informação possui e ter definido, claramente, com quais pessoas podemos compartilhar cada uma destas.

Seguindo esse raciocínio precisamos dificultar também a nossa assinatura digital, criando certo grau de complexidade para evitar que nossa senha seja facilmente quebrada por softwares ou simplesmente por dedução humana.

Uma senha forte deve ser formada de números, letras e sinais gráficos, sem apresentar relação direta com informações dos seus usuários, o que as torna difíceis de ser lembradas e, portanto, com grande probabilidade de ser anotadas por seus usuários em locais de fácil acesso, favorecendo os ataques de engenharia social (MITNICK; SIMON, 2006).

Ataques por e-mail são cada vez mais comuns. Através de e-mails com solicitações de atualização de cadastro bancário, ou do Cadastro de Pessoa Física (CPF), o atacante se passa por determinada instituição, induzindo o alvo a informar, em um site falso, similar ao verdadeiro, dados pessoais, que serão utilizados posteriormente em fraudes. Esse procedimento é conhecido como “*phishing*” ou “*phishing scan*”, é um termo que se origina do inglês, em sua tradução temos “pesca”. Esse nome se dá pelo fato do perpetrador tentar “pescar” informações de suas vítimas, jogando diversas iscas e esperar que alguém caia na armadilha.

Os principais tipos de dados, que são visados nesse tipo de ataque são: senhas, números de cartão de crédito e outros dados pessoais.

Derivado desse ataque, surgiu o “*phishing*” via celular.

As tentativas de ataques via celular, tem crescido assustadoramente. Assim como o envio por e-mail, esse ataque é realizado em massa, tentando alcançar o maior número de vítimas possíveis, para se obter um maior retorno.

Uma nova maneira desenvolvida pelos criminosos de capturar informações de pessoas despreparadas consiste na utilização de dispositivos celulares, com o envio de mensagens de texto, geralmente informando que o proprietário do celular foi contemplado em um sorteio de uma promoção, que geralmente está sendo noticiado pela mídia. Nomes de grandes marcas são utilizados como Nestlé, Coca-Cola, Bradesco, Itaú, Caixa Econômica, Volkswagen, Ford, dentre outras. Na continuação do texto da mensagem, é informado um número de telefone, geralmente de uma unidade federativa diferente do receptor da mensagem, solicitando que a vítima entre em contato “gratuitamente” por um telefone fixo. Essa solicitação não é por acaso, tudo já foi pensado. Em alguns casos até uma senha fictícia é fornecida no corpo da mensagem.

O ataque partindo de um Estado diferente do alvo é mais uma técnica de Engenharia Social, um passo a frente que o estelionatário está em relação ao restante da população. Pois as empresas de telefonia fixa permitem que seus usuários solicitem bloqueios para ligações que tenham como destino a rede de telefonia móvel. O que não se sabe, é que quando se liga para um aparelho celular em outro estado, a ligação deixa de ser tarifada como rede de telefonia móvel e passa a se enquadrar em ligação interurbana, caindo em outra faixa de tarifação e permitindo a ligação para rede de celular do outro estado. A vítima só perceberá que está pagando pela ligação quando receber a próxima fatura do telefone.

Outro ataque bastante comum a infecção da máquina por “cavalos de tróia”, que se dá através de e-mails. Incidem o envio de aplicações disfarçadas, que ao serem instaladas, infectam o computador e passam a monitorar o mesmo. Ou ainda, criam brechas de segurança na máquina infectada, para torná-la acessível via internet, ou rede, por quem enviou o programa.

2.2 METODOLOGIA

Buscando compreender a realidade de uma empresa real, realizou-se um estudo de caso em uma corporação, com atuação em mais de um estado e que utiliza a informação como fator estratégico em seu negócio.

Nesta firma constatamos que os dados, confidenciais e públicos, trafegam internamente de setor para setor e há necessidade de se priorizar a segurança da informação.

Elaborou-se um questionário, buscando identificar, a cerca do conhecimento e do comportamento dos funcionários, qual a situação da segurança da informação na referida empresa.

Realizou-se uma entrevista com 36 (trinta e seis) funcionários desta empresa, tendo como principal objetivo, conhecer o perfil dos profissionais que lidam com essas informações e seus conhecimentos a cerca da segurança da informação.

Antes de se realizar a pesquisa, foi elaborado um plano de ataque simulado, que consistiu em, passar-se por um consultor de tecnologia, para se obter a maior quantidade de informações possíveis.

Para a primeira ligação, foi utilizado o telefone do tele atendimento, juntamente com o nome do diretor, que constam na página de internet da empresa.

Ao entrar em contato com o setor de atendimento ao cliente, foi possível, em poucos minutos, levantar informações sobre cargos, telefones e nomes de funcionários. Nomes de diretores: financeiro, administrativo e marketing, bem como os nomes dos responsáveis pelos recursos humanos, pela gerência do site e o responsável pelo setor de informática da empresa foram cedidos, sem muito questionamento.

Ao ligar para o responsável pelo site, tentou-se identificar as tecnologias de desenvolvimento utilizadas na página da empresa e o local onde essa página é mantida.

Oportunamente, cabe salientar que todo o procedimento, foi devidamente acompanhado pelo diretor geral e pela diretora administrativa, que apesar de saber o que estava ocorrendo, não interferiram nos procedimentos, deixando os seus funcionários totalmente alheios à situação.

Esses e outros fatos mostram a necessidade de treinamento para os funcionários, buscando prepará-los para possíveis interações com demais funcionários, clientes e colaboradores.

Marras (2009, p. 145) traz uma definição do treinamento como o “processo de assimilação cultural a curto prazo, que objetiva repassar ou reciclar conhecimentos, habilidades ou atitudes relacionadas diretamente a execução de tarefas ou à sua otimização no trabalho”.

3 RESULTADOS

3.1 VERIFICANDO O CONHECIMENTO

Os resultados obtidos na entrevista realizada com os funcionários e nos ataques simulados são mostrados a seguir.

TABELA 1– Conhecimento Sobre Engenharia Social.

Você sabe o que é Engenharia Social?	Percentual (%)
Sim	11,11%
Não	88,89%

FONTE: Pesquisa realizada pelo autor.

A falta de conhecimento do assunto é a principal causa de fraudes tecnológicas, pois encurta o caminho até o alvo, uma vez que alguém que tem acesso a sistemas ou informações, poderá compartilhar esses dados com terceiros por pura ingenuidade e despreparo, tornando ineficazes as ferramentas de segurança existentes na empresa. Pode-se verificar que mais de 88% dos funcionários, segundo a Tabela 1, não sabem o que é Engenharia Social.

Tabela 2 – Conhecimento Sobre Segurança da Informação.

Você já participou de algum treinamento sobre segurança da informação?	Percentual (%)
Sim	11,11%
Não	88,89%

Fonte: Pesquisa realizada pelo autor.

De acordo com a Tabela 2, constatou-se que o a falta de treinamento é o principal motivo do desconhecimento do assunto tratado, onde a mesma quantidade, pouco mais de 88% dos entrevistados, não participaram de treinamento sobre Engenharia Social, o que facilita a execução de possíveis ataques contra os funcionários e a empresa.

3.2 PHISHING SCAN VIA E-MAILS, SITES E CELULARES

Tabela 3– Constatando recebimento de links via e-mail.

Você já recebeu algum e-mail com link para fotos ou vídeos?	Percentual (%)
Sim	85,74%
Não	14,29%

Fonte: Pesquisa realizada pelo autor.

Tabela 4– Conhecimento Sobre *Phishing Scan*.

Você já recebeu algum e-mail solicitando atualização de cadastro bancário ou da receita federal?	Percentual (%)
Sim	38,89%
Não	61,11%

Fonte: Pesquisa realizada pelo autor.

O ataque de captura de informação, ou “*phishing Scan*” se utiliza técnicas de Engenharia Social para despertar o interesse dos usuários de e-mail. Geralmente se envia um ataque em massa, com um conteúdo aparentemente direcionado, porém não muito específico. Pode ser sobre algum fato público, noticiado na mídia como escândalos de celebridades e fatos que as pessoas tenham interesse em ver, ou solicitação de atualização de informações como dados bancários e atualização de cadastro de CPF⁷. Geralmente com um link, esse ataque trará um programa, como o nome de “fotos”, “vídeos”, conforme mais de 85% dos entrevistados confirma ter recebido, conforma a Tabela 3, ou até mesmo o endereço de um site, que se assemelhe a algum site confiável, como o endereço de um banco ou da própria Receita Federal, que mais de 38% dos funcionários afirmam ter recebido, conforme mostra a Tabela 4.

Tabela 5 – Constatando *Phishing Scan* via telefone celular.

Você já recebeu mensagem de celular informando que você ganhou uma promoção e que precisa ligar para receber o prêmio?	Percentual (%)
Sim	94,44%
Não	5,56%

Fonte: Pesquisa realizada pelo autor.

De acordo com a Tabela 5, mais de 94% dos entrevistados já receberam um “*Phishing Scan*” via telefone celular.

Analizou-se uma mensagem de texto, recebida via celular, de um golpe por telefone, que continha a seguinte mensagem: "<REDE GLOBO>PeG E AVIAO DO FAUSTAO (6 EDICAO) INF SEU TIM FOI SORT COM 1 CASA + 35 MIL INF: LIG DO TIM. 0418597503456. senha (98765)⁸"

Realizou-se uma ligação para o número indicado. Ao atender o telefone, o criminoso já pronuncia o nome da promoção e solicita o número da “senha” para confirmação da sorteio. No entanto alguns erros grosseiros por parte do fraudador tornam a conversa bastante suspeita. Uma delas foi dizer: “o senhor é o nosso décimo sorteado neste anoletivo”, onde se sabe que “ano letivo” refere-se ao período onde se há atividades escolares ou acadêmicas, o que não tem ligação com o contexto da promoção. Algumas outras palavras e expressões são detectadas ao longo da conversa como “é por que tem muito gaiatinho, que fica ligando, passando trote”. A palavra “gaiatinho” é uma expressão regional, que não é utilizada por

⁷Cadastro Nacional de Pessoa Física.

⁸Mensagem recebida pelo autor.

funcionários de telemarketing treinados, que é o mínimo que se pode esperar de uma promoção, supostamente, realizada pela “REDE GLOBO”.

Tabela 6 – Verificando a Existência de Perfil Público

Você possui conta no facebook ⁹ ?	Percentual (%)
Sim	83,33%
Não	16,67%

Fonte: Pesquisa realizada pelo autor.

A popularização das mídias sociais é uma mina de ouro para os engenheiros sociais, em especial o facebook que por estar em maior evidência, contém informações mais atualizadas que os demais. Por meio de um cadastro, o usuário cede algumas informações pessoais, como lugar onde estudou no ensino médio, aonde faz/fez faculdade e o nome de seu empregador. O facebook utiliza inteligência artificial para sugerir aos seus usuários, perfis parecidos, que tenham em comum alguma informação, como ano de conclusão em mesma instituição de ensino, mesmo empregador e amigos ou grupos compartilhados. Desta forma é possível abordar um grupo determinado de uma mesma empresa, ou com um perfil similar.

Podemos observar na Tabela 6, que mais de 83% dos funcionários, possuem perfil público no facebook.

É possível omitir certas informações, pois o próprio facebook permite configurar o mode de exibição, através de filtros. São eles: público, amigos, somente eu, personalizado, melhores amigos, família, conforme é visto na figura 1.

Figura 1 – Filtros de visualização do conteúdo no Facebook



Fonte: Gerado pelo autor.

⁹Site e serviço de rede social, operado e de propriedade privada da Facebook Inc.

A utilização correta desses filtros pode evitar que informações pessoais privadas, cheguem a mão de pessoas mal intencionadas. Não é aconselhável informar telefones, endereço, empresa na qual trabalha e qualquer tipo de informação pessoal no perfil.

3.2 SENHAS

As senhas constituem um dos pontos mais vulneráveis encontrados nas empresas. É comum o compartilhamento dessas entre funcionários para acesso aos sistemas internos.

Tabela 7 – Verificação da Utilização de Senhas na Empresa.

Você utiliza senhas para acessar os sistemas da empresa?	Percentual (%)
Sim	100,00%
Não	0,00%

Fonte: Pesquisa realizada pelo autor.

De acordo com os dados da Tabela 7, todos os entrevistados utilizam senhas para acessar os sistemas da empresa.

Tabela 8 – Verificação da Utilização de Mesma Senha para Serviços Distintos.

Você utiliza uma mesma senha para diferentes serviços?	Percentual (%)
Sim	50,00%
Não	50,00%

Fonte: Pesquisa realizada pelo autor.

Um dado bastante preocupante é que 50% dos funcionários confessaram utilizar uma mesma senha para diferentes serviços, o que podemos verificar na Tabela 8, comprometendo a segurança, pois ao quebrar uma senha, se tem acesso a todos os sistemas em que o usuário tenha cadastro com a mesma senha, necessitando apenas verificar as páginas visitadas do navegador e testar o nome de usuário e senha.

O ideal é que se tenha uma senha de acesso para cada situação, nunca se deve utilizar a senha do banco, ou e-mail, para demais serviços.

Tabela 9 – Verificação de Compartilhamento de Senhas Entre Funcionários.

Você já utilizou a senha de algum colega de trabalho?	Percentual (%)
Sim	61,11%
Não	38,89%

Fonte: Pesquisa realizada pelo autor.

Outro fato que também merece preocupação é a utilização de logins compartilhados, no qual mais de 61% dos funcionários, utilizam, ou utilizaram a senha de outro(s), conforme nos mostra a Tabela 9. Essa utilização compromete a autenticidade das ações realizadas pelo funcionário, pois não se pode definir, em processo de auditoria, quem realmente executou a ação.

Tabela 10 – Verificação de Como se dá o Armazenamento de Senhas.

Como você armazena suas senhas?	Percentual (%)
Na memória	66,67%
Anota em agenda ou em papel	11,11%
Em lugar confidencial	22,22%

Fonte: Pesquisa realizada pelo autor.

Ainda associado às senhas, verificamos, na Tabela 10, que o armazenamento destas se dá, em sua maioria (66,67%), na memória do detentor, o que indica fortemente, que as senhas são formadas por dados que compõem o cotidiano do funcionário, isso pode incluir: datas, números de documentos, nomes de parentes (filho, cônjuge), endereços e demais. O que a torna frágil, pois em uma conversa informal, se pode extrair, facilmente, tais informações.

Uma senha pode ser criada a partir de qualquer coisa, por exemplo, o nome de filhos, cachorro, carros, pais, cônjuge, uma frase, ou qualquer coisa que venha a mente. No entanto é preciso saber que existem softwares que procuram por palavras existentes. Logo, se sua senha é composta por uma simples palavra que esteja disponível em um dicionário ou em algum outro comum, poderá ser quebrada de modo bastante simples, assim como deduzida por alguém que lhe conheça.

Sugere-se que a senha tenha de 10 a 12 caracteres; seja uma mescla de maiúsculas e minúsculas; contenham ao menos um dígito numérico; não repetir nenhum caractere mais de três vezes; e não utilize a mesma senha por mais de cinco vezes. Também pode ser sugerido que a senha não seja nome de pessoa, mesmo que em ordem reversa; não seja uma data, nem formada por uma, não esteja em nenhum dicionário, mesmo em ordem reversa.

Uma sugestão para elevar o nível de sua senha é usar letras maiúsculas, minúsculas e números na composição. Esse é o básico para um nível mínimo de segurança em sua senha.

Outra sugestão é uso de caracteres especiais substituindo algumas letras, como por exemplo: @, \$, #, entre outros, que elevarão ainda mais o nível de dificuldade. Ainda como

sugestão pode-se utilizar frases como senha. Para exemplificar pode-se utilizar uma frase bastante conhecida: “diga-me com quem andas e te direi quem és”. Depois, pega-se a primeira letra de cada palavra da frase, alternando as letras entre maiúsculas e minúsculos. Teremos: “DmCqAeTdQE”. Já seria uma senha, bastante diferente e segura. Mas ainda pode-se aumentar a complexidade inserindo números no lugar das vogais. Tem-se: “DmCq43TdQ3” (substituiu-se o A pelo 4 e o E pelo 3).

O principal problema em se utilizar senhas distintas é exatamente a dificuldade de memorizar e é neste momento, em que ocorre outro problema. Mais de 11% dos entrevistados alegaram guardar suas senhas em um pedaço de papel, ou em uma agenda pessoal. Isso é um grave problema de segurança, qualquer pessoa que tenha acesso à essa informação, poderá se utilizar o login do usuário e se passar por ele.

Uma recomendação que deve ser lembrada é de não permitir que o navegador de internet salve as senhas automaticamente. Isso gera uma quebra de segurança séria, pois quem estiver utilizando a máquina, onde haja esse registro gravado, terá acesso direto a contas e serviços, sem nem se dar ao trabalho de procurar senhas e nomes de usuário, pois o próprio navegador se encarregará de efetuar a identificação automática do utilizador.

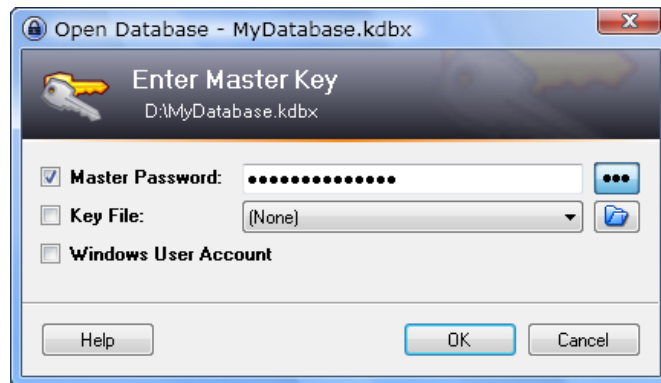
A maneira mais adequada de se armazenar senhas seria em memória, criando associações entre os diferentes serviços utilizados, porém existem formas seguras de se guardar essas senhas em um computador, ou em um celular, através de softwares¹⁰ de armazenamento de senhas, que utilizam criptografia¹¹ para não permitir acesso de demais pessoas. Seu funcionamento é bastante intuitivo, é solicitada, após a instalação, uma senha mestre, que servirá para ter acesso às informações. Essa senha deverá ser bem elaborada e jamais compartilhada com ninguém. Após acessar o sistema é possível inserir informações de login, senha, endereço do sítio de internet e alguma outra informação, que seja pertinente. Cada conta poderá ter informações distintas.

Existem diversos softwares, pagos e gratuitos, com a mesma finalidade: guardar e proteger senhas. Escolhemos como exemplo o “KeePass”, que é um projeto código aberto, totalmente gratuito.

¹⁰Programas de computadores.

¹¹É o estudo dos princípios e técnicas pelas quais a informação pode ser transformada da sua forma original para outra ilegível, de forma que possa ser conhecida apenas por seu emissor e destinatário.

Figura 2 – Tela de acesso às informações do KeePass

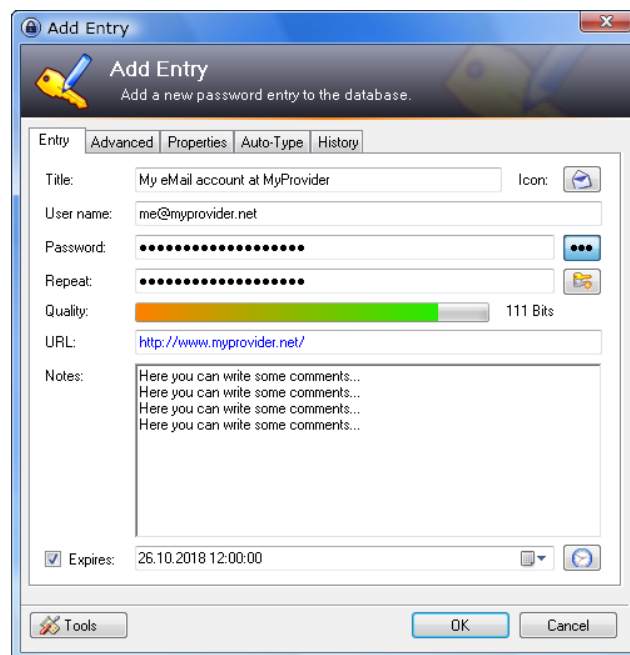


Fonte:Gerado pelo autor.

Na Figura 1, podemos verificar a solicitação da “senha mestre”, que dá acesso às informações do usuário. É oportuno lembrar que essa senha precisa ser mais difícil e mais bem protegida, pois ela dará acesso às informações contidas dentro do arquivo gerado pelo software, que são dados referentes a nomes de usuários e senhas de contas utilizadas.

Ainda é possível criar um arquivo senha (Key File), que servirá como credencial para acesso ao programa, ou ainda utilizar o login de usuário do windows como senha de entrada. A escolha do tipo de entrada, deve ser informado na instalação do programa.

Figura 3 – Tela para adição de uma nova entrada de dados no KeePass



Fonte: Gerado pelo autor.

Uma vez acessado o programa permite que seja criada entradas de dados, que terão um título (title), um nome de usuário (username), a senha (Password). O software exige que se repita a senha, como uma forma de conferência. Simultaneamente à inserção da senha, uma barra, indica através da cor, o nível de segurança da palavra-passe escolhida. Variando do vermelho, que tem uma conotação de alerta, até o verde, que assume a conotação de segurança. Ainda é possível definir algum comentário, algo que seja importante de lembrar em relação ao login gravado. Logo abaixo existe uma opção, onde é possível informar a data e hora de expiração da senha. Como também pode ser desabilitada a expiração, apenas desmarcando a opção “Expires”.

Após gravar todas as senhas é necessário, manter uma cópia do arquivo por segurança. Essa cópia poderá ser arquivada em uma mídia, como CD/DVD, disco de armazenamento (HD), ou em outra máquina que se tenha acesso.

3.3 Comportamento

TABELA 11 – Verificando a Utilização de Serviços Bancários Via Internet na Empresa.

Você utiliza serviços bancários via internet no local de trabalho?	Percentual (%)
Sim	22,22%
Não	77,78%

FONTE: Pesquisa realizada pelo autor.

Outra mudança deve ser com relação ao comportamento diante do computador. O usuário jamais deve revelar sua senha a ninguém. É importante lembrar que a responsabilidade por toda atividade realizada mediante o uso de uma identificação digital será atribuída ao proprietário. Se a senha for comprometida, é necessário mudá-la imediatamente, evitando a continuação de seu uso indevido. Em seguida deve-se informar ao gerenciador da conta, no caso de uma empresa o setor de informática, ou no caso de um banco a agência em que se tem conta.

Na Tabela 11, constata-se que pouco mais de 22% acessa sua conta bancária em ambiente de trabalho.

Vale ressaltar o quanto é importante que se altere as senhas regularmente, principalmente senhas bancárias. Ao adotar esse procedimento o usuário inutilizará a senha anterior.

Sempre que se afastar do computador efetue o logout¹², feche completamente todas as janelas do navegador ao terminar, a fim de impedir que outros acessem sua conta.

Tenha extremo cuidado ao acessar serviços por meio de um computador compartilhado ou público. O acesso público à Internet é agora oferecido em muitas bibliotecas, aeroportos, centros de copiadoras e cafés. Recursos inerentes aos navegadores da Web podem permitir ao usuário seguinte acessar a sua conta. Para evitar esta possibilidade, não deixe de fazer o logout e fechar todas as sessões do navegador.

Não deixe documentos impressos expostos a terceiros. Hoje em dia praticamente todo mundo tem em mãos um aparelho celular com câmera embutida e pode fotografar documentos e outras informações expostas.

Tabela 12 – Verificação de comportamento ao receber conteúdo duvidoso

O que você faz quando recebe e-mail com conteúdo duvidoso?	Percentual (%)
Exclui	50,00%
Submete ao setor de TI	7,14%
Clica sobre o link	14,29%
Passa o mouse sobre o link para verificar	28,57

Fonte: Pesquisa realizada pelo autor.

¹² Terminar o uso de um sistema computacional, removendo a senha do usuário.

Muitos ataques de Engenharia Social têm como origem os e-mails. Ao infectar uma máquina, um *malware*¹³ pode remeter à lista de contatos do usuário infectado. E-mails com anexos, visando infectar mais pessoas, agora se passando pelo usuário que infectou. Algo como “Segue as fotos que você me solicitou” ou ainda “Veja atriz famosa fazendo sexo” entre outras informações que despertem o interesse e a curiosidade das pessoas e faça com que um grande número de pessoas caia nessa armadilha.

Não se deve abrir, em hipótese alguma, conteúdo de e-mails, mesmo de conhecidos, que não tenham o costume de enviar anexos, principalmente falando de celebridades, ou de fotos que não tenham sido realmente solicitadas.

Nesses casos o ideal é seguir o que 50% dos entrevistados alegou fazer, segundo a Tabela 12, e excluir o e-mail.

No caso de se acreditar que o conteúdo do e-mail é algo seguro, pode-se verificar o conteúdo, passando o mouse sobre o link, isso mostrará, na barra inferior (barra de status), o endereço do link, segundo a pesquisa isso é realizada por mais de 14% dos funcionários.

Caso surja alguma desconfiança, pode-se, ainda, submeter ao setor de informática para análise, como poucos entrevistados afirmaram fazer.

Tabela 13 – Verificando Comportamento ao receber solicitações de informação

O que você faz ao receber uma solicitação de informação por e-mail ou por telefone?	Percentual (%)
Não fornece	50,00%
Fornece após identificar o solicitante	27,78%
Fornece após consultar o superior	22,22%
Fornece de imediato, pois não trata de informações sigilosas	0,00%

Fonte: Pesquisa realizada pelo autor.

O fornecimento de informações é um problema a ser priorizado, na entrevista realizada, de acordo com a Tabela 13, nenhum funcionário informou que fornece a informação de imediato. Isso pode gerar uma falsa sensação de segurança, uma vez que os entrevistados, em sua maioria (88.89%), conforme apresentado na Tabela 1, desconhece o que é Engenharia Social e, a mesma quantidade não participou de treinamento sobre segurança da informação. Isso pode indicar que os profissionais não têm a percepção do real valor de

¹³Software destinado a se infiltrar em um sistema de computador alheio de forma ilícita, com o intuito de causar algum dano ou roubo de informações (confidenciais ou não).

algumas informações que estão em sua posse, e que estas podem ser passadas de maneira sutil, sem que o funcionário se dê conta de que está fornecendo conteúdo estratégico.

É preciso definir os níveis de informação e as responsabilidades de cada setor, para que os funcionários possam saber exatamente quais são as informações públicas e quais são as informações sigilosas e o que fazer quando abordado, indiferente do meio, por qualquer pessoa.

É importante lembrar, que clientes também necessitam de informações para manter negócios, é preciso identificar o cliente, através de confirmações de segurança, para que não ocorram problemas de relacionamento e confiança entre empresa, fornecedores e principalmente clientes.

3.6 ATAQUES SIMULADOS

Ao realizar ligações para a empresa, foi possível apurar diversas informações. Saber qual a tecnologia aplicada à página web da empresa e que o conteúdo da página não fica hospedado na empresa, mas sim em um servidor de serviços web terceirizado.

Nome de diretor de setor e responsável por atividades na empresa, também foi informado.

A vontade de ajudar, somada ao uso do nome do diretor geral da empresa, influenciaram na rapidez para se obter tanta informação.

Em uma visita, ao escritório da empresa, percebeu-se um roteador sem fio, que se encontrava ligado diretamente a uma máquina do setor administrativo e iniciou-se mais um ataque.

Sem realizar qualquer tipo de identificação, acessou as dependências da empresa e perguntou-se pelo diretor geral (Nome consta na página da internet). Foi respondido prontamente, que o mesmo não havia chegado. Retirando um dispositivo móvel de dentro de uma pasta, fez-se o seguinte questionamento aos funcionários: “Vocês sabem a senha da wi-fi¹⁴? Eu preciso enviar um e-mail e minha internet 3G não está acessando”. Mais uma vez, um funcionário prestativo, cedeu a informação. Conectou-se a rede e fez-se uma varredura de

¹⁴ Rede sem fio disponibilizada por dispositivo de roteamento.

máquinas e serviços, utilizando o software “Fing – Network Scanner¹⁵”, que não serão citados, atendendo a um pedido da empresa, visando manter o anonimato e a segurança da mesma.

Figura 4– Imagens do escaneamento realizado pela ferramenta FING



Fonte:<http://itunes.apple.com/br/app/fing-network-scanner/id430921107?mt=8>.

Em posse da senha da rede sem foi possível acessar a rede interna e verificar a existência de 9 (nove) computadores, com pastas compartilhadas, na rede do setor administrativo, sem qualquer restrição de acesso.

¹⁵ Ferramenta para verificação de rede e análise. Encontra e identifica dispositivos ligados à rede em que ele está conectado, identificando serviços, endereços e portas que estão sendo utilizados.

Foi possível acessar as máquinas e verificar o conteúdo de pastas compartilhadas, onde foram encontradas diversas planilhas, documentos de textos, fotos, entre outros. Pode-se observar até 8 (oito) pastas compartilhadas em uma mesma máquina.

O compartilhamento de pastas pode ser realizado, por qualquer usuário, desde que esteja com permissões de administrador na máquina em que se deseja realizar o compartilhamento.

A ausência de um servidor de domínio dificulta ainda mais a proteção dos dados, pois não há verificação de credenciais e permissões na rede. Permitindo livre acesso, de quem estiver na rede, a qualquer recurso compartilhado.

Tabela 14 – Pergunta de Segurança Básico

Em qual banco você possui conta?	Banco do Brasil
Banco do Brasil	16,67%
Caixa Econômica	44,44%
Bradesco	5,56%
Itaú	5,56%
Outros	27,78%

Fonte: Pesquisa realizada pelo autor.

A última pergunta realizada, teve o intuito de constatar a fragilidade dos funcionários em fornecer informações pessoais. Com essa informação seria possível atacar a empresa e seus funcionários, com o envio de e-mails solicitando atualização de cadastro nos principais bancos utilizados de acordo com a Tabela 14, Banco do Brasil (16,67%) e Caixa Econômica (44,44%) e oferecendo um link direto para um site falso, com a mesma estrutura dos bancos citados, para iludir os usuários a fornecerem seus dados, como conta, agência e senha, permitindo, assim, uma fraude financeira.

4 CONSIDERAÇÕES FINAIS

Após a realização da entrevista e a tabulação das respostas, realizou-se uma reunião com a diretoria da empresa pesquisada, durante a qual foram apresentados os resultados da pesquisa e apontadas as seguintes ações:

- a) criar um processo de treinamento para a conscientização da segurança da informação;

- b) utilizar o ambiente de intranet e mural de recados, para que sejam afixados informativos atualizados sobre Engenharia Social;
- c) promover treinamento sobre a criação e manutenção de senhas dos usuários;
- d) implantar políticas de segurança de acesso aos serviços corporativos;
- e) incentivar a alteração das senhas e identificações existentes, criando novos hábitos que promovam uma maior segurança;
- f) seguir o que determina a NBR ISO/IEC 27002 para o gerenciamento da política de segurança da informação na empresa.

Essas ações sugeridas visam criar uma cultura dentro da empresa consultada, conscientizando cada funcionário de suas responsabilidades para com as informações da corporação. Essa consciência deve ser constantemente reforçada, para evitar incidentes de segurança, visto que o fator predominante nestes desastres tem a intervenção de funcionários.

É recomendável que haja uma política de segurança centralizada e bem divulgada, para que todos saibam como se defender e a quem recorrer em caso de dúvidas. Não é necessário fazer com que as pessoas se tornem paranoicas, mas que estejam sempre atentas às solicitações que a elas sejam feitas e que saibam o valor das informações pelas quais são responsáveis.

Percebemos através da análise realizada as facilidades em se obter informações a respeito da empresa e de seus funcionários através dos ataques simulados.

Também constatamos a fragilidade dos funcionários, segundo a pesquisa realizada, devido a falta de conhecimento sobre o assunto, o que tornou o ambiente propício para o estudo de caso.

Após a apresentação de todos os problemas detectados pela pesquisa, bem como com o acompanhamento dos ataques simulados, a diretoria da empresa mostrou-se bastante preocupada com a situação e iniciou uma busca por profissionais capacitados para, através do estudo realizado, elaborar um treinamento devido, para cada grupo de funcionário, uma vez que informações da empresa são alavancas de desenvolvimento econômico e estratégico e a perda dessas pode gerar prejuízo.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA BNT. **NBR 17799**: Código de Prática para Gestão da Segurança da Informação nas Empresas: item 2.1. Rio de Janeiro, 2001.

BORGES-ANDRADE, Jairo Eduardo. **Desenvolvimento de medidas em avaliação de treinamento**. Estud. psicol. Natal, v. 7, n. spe, 2002. Disponível em: <http://www.scielo.br/scielo.php?script=sci_arttext&pid=S1413-294X2002000300005&lng=en&nrm=iso>. Acesso em: 22 ago. 2012.

BRAGA, Pedro Henrique da Costa. **Técnicas de Engenharia Social**. Disponível em: <<http://www.gris.dcc.ufrj.br/documentos/artigos/engenharia-social>>. Acesso em: 21 ago. 2012.

LACERDA, Érika Rodrigues Magalhães; ABBAD, Gardênia. **Impacto do treinamento no trabalho**: investigando variáveis motivacionais e organizacionais como suas preditoras. Rev. adm. contemp, Curitiba, v. 7, n. 4, dez. 2003 . Disponível em: <http://www.scielo.br/scielo.php?script=sci_arttext&pid=S1415-65522003000400005&lng=en&nrm=iso>. Acesso em: 23 ago. 2011.

MARRAS, Jean Pierre. **Administração de recursos humanos**: do operacional ao estratégico, 13. ed. São Paulo: Saraiva, 2009.

MITNICK, Kevin D.; SIMON, William L. **A Arte de Invadir**. São Paulo: Pearson, 2006.

POPPER, Marcos Antonio; BRIGNOLI, Juliano Tonizetti. **Engenharia Social**: um perigo eminente. Disponível em: <<http://www.posuniassselvi.com.br/artigos/rev03-05.pdf>>. Acesso em: 21 ago. 2012.

SANTOS, Luciano Alves Lunguinho. **O impacto da engenharia social na segurança da informação**. 2004. 83 f. Monografia (Pós-Graduação em Redes de Computadores) - Universidade Tiradentes, Aracajú, 2004.

ULBRICH, Henrique; DELLA VALLE, James. **Universidade H4ck3r**. São Paulo: Digerati Books, 2011. v.1.