**UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ**

**DEPARTAMENTO ACADÊMICO DE ELETRÔNICA – DAELN**

**ESPECIALIZAÇÃO EM GESTÃO DA TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO**

**LUIZ FERNANDO MIZAEL MEIER**

# ENGENHARIA SOCIAL: ESTUDO DE CASO SOBRE OS RISCOS DE UM ATAQUE EFETUADO POR UM EX-FUNCIONÁRIO

**MONOGRAFIA**

**CURITIBA**

**2018**

**LUIZ FERNANDO MIZAEL MEIER**

# ENGENHARIA SOCIAL: UM CASO DE ESTUDO DOS RISCOS DE UM ATAQUE EFETUADO POR UM EX-FUNCIONÁRIO

Monografia apresentada como requisito parcial à obtenção do título Especialista em Gestão da Tecnologia da Informação e Comunicação, do Departamento, da Universidade Tecnológica Federal do Paraná.

Orientador: Prof. Christian C. S. Mendes

**CURITIBA**

**2018**

Ministério da Educação
**Universidade Tecnológica Federal do Paraná**
**Câmpus Curitiba**
Diretoria de Pesquisa e Pós-Graduação
IV CURSO DE ESPECIALIZAÇÃO EM GESTÃO DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

# TERMO DE APROVAÇÃO

ENGENHARIA SOCIAL: ESTUDO DE CASO SOBRE OS RISCOS DE UM ATAQUE EFETUADO POR UM EX-FUNCIONÁRIO

Por

**LUIZ FERNANDO MIZAEL MEIER**

Esta monografia foi apresentada às **17:30 h** do dia **14/11/2018** como requisito parcial para a obtenção do título de Especialista no CURSO DE ESPECIALIZAÇÃO EM GESTÃO DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO, da Universidade Tecnológica Federal do Paraná, **Campus Curitiba**. O candidato foi arguido pela Banca Examinadora composta pelos professores abaixo assinados. Após deliberação, a Banca Examinadora considerou o trabalho:

| | | |
|---|---|---|
| **1** | | Aprovado |
| **2** | | Aprovado condicionado às correções Pós-banca, postagem da tarefa e liberação do Orientador. |
| **3** | | Reprovado |

_____

**Prof. Msc. Alexandre Jorge Miziara**
UTFPR - Examinador

_____

**Prof. Msc. Christian C.S. Mendes**
UTFPR – Orientador

_____

**Prof. Msc. Alexandre Jorge Miziara**
UTFPR – Coordenador do Curso

- O Termo de Aprovação assinado encontra-se na Coordenação do Curso -

Dedico este trabalho à minha família, pelos momentos de ausência.

## AGRADECIMENTOS

Agradeço primeiramente à minha esposa, cujo apoio e paciência foram primordiais para vencer este desafio.

Agradeço ao meu orientador, Prof. Christian Mendes, sem o qual este trabalho não teria existido.

Agradeço ao meu antigo gestor e ainda amigo, por me autorizar e apoiar a efetuar os testes necessários para a conclusão desta monografia.

Aos meus colegas de sala, pelos bons momentos.

À Secretaria do Curso, pela cooperação.

Enfim, a todos os que por algum motivo contribuíram para a realização desta pesquisa.

## RESUMO

MIZAEL MEIER, Luiz Fernando. **Engenharia Social:** como se proteger de ataques de um ex-funcionário. 2018. Total de páginas: 35. Monografia (Especialização em Gestão de Tecnologia da Informação e Comunicação) - Universidade Tecnológica Federal do Paraná. Curitiba - 2018.

Este estudo de caso visa explanar e demonstrar os riscos da Engenharia Social, assunto tão pouco valorizado e abordado dentro das corporações. Muito se fala sobre segurança da informação e da importância em possuir ferramentas de proteção a ataques e vazamento de informações. No entanto, o elemento humano continua sendo o elo mais fraco no processo de vazamento de informações e na exploração de vulnerabilidades. O comportamento despreocupado e a inocência das pessoas no relacionamento interpessoal fazem com que o costume do questionamento, principal ferramenta de defesa na Engenharia Social, seja deixado de lado. O presente trabalho demonstra como técnicas comuns de abordagem fazem possível o ganho da confiança e o convencimento da vítima a prestar informações ou executar ações conforme a vontade do atacante.



**Palavras-chave:** Engenharia Social. Ameaça. Vulnerabilidade. Segurança da Informação. Tecnologia.

## ABSTRACT

MIZAEL MEIER, Luiz Fernando. **Social Engineering: how to protect your company from an ex-employe attack**. 2018. Total pages: 35. Monography (Specialization in Information Technology and Communication Management) - Federal Technological University of Paraná. Curitiba - 2018.

This case of study attempts to explain and show the risks of Social Engineering, a subject so undervalued and low approached in companies. A lot is spoken about information security and the importance of having protection tools against hacking and leaking information. However, the human element continues to be the weakest link in the process of leaking information and in the vulnerabilities exploitation. The unconcerned behaviour and the innocence of people dealing with each other make the habit of questioning, principal tool in defense against Social Engineering, to be left aside. The present work shows how common techniques of approach make possible the gain of trust and the convincing of the victim to give information or execute actions as the attacker wants to.



**Keywords**: Social Engineering. Questioning. Security. Technology.

## SUMÁRIO

# 1. INTRODUÇÃO

A Engenharia Social, segundo Ian Mann, um dos mais famosos engenheiros sociais, “é a arte de manipular pessoas, enganando-as, para que forneçam informações ou executem uma ação.” Desde os tempos mais primórdios existe o ato de enganar pessoas e/ou se aproveitar delas.

Em tempos como hoje, é inegável o uso das tecnologias para a execução das mais variadas atividades. Este ambiente digital, além de trazer benefícios, traz também muitos riscos para as corporações (MARCIANO, 2006). Com a tecnologia tão avançada e a segurança da informação tão valorizada, preocupa-se mais com os aspectos técnicos para proteção da informação e, por consequência, acaba-se esquecendo da principal e mais antiga vulnerabilidade, o fator humano. O mundo corporativo está tão preocupado com ameaças digitais, que direciona todo seu esforço em investimentos e em ferramentas de controle de acessos, proteção de dados e backups. Kevin Mitnick defende, em seu livro, A Arte de Enganar (2003), que concluiu ser mais fácil descobrir a senha de um usuário simplesmente perguntando, ao invés de utilizar-se de artifícios tecnológicos elaborados.

É neste contexto paradoxal entre tecnologias avançadas *versus* o elemento humano que se debruça o estudo de caso apresentado neste trabalho. São utilizadas abordagens personalizadas, a despeito dos artifícios técnicos de proteção da atualidade, para conseguir o máximo de informações e acessos sigilosos de uma companhia a partir de falhas humanas, seja por procedimentos não executados, mal executados ou indevidos. Além disso, são abordados também ataques direcionados a usuários com a intenção de enganá-los e conseguir informações sigilosas. Por último, informações sigilosas, acessos restritos e demais indícios necessários para aplicação de golpes semelhantes costumam ser obtidos com facilidade por ex-funcionários mal-intencionados, nessa presente análise como exemplo.

Paralelamente, demonstram-se os processos que podem ser adotados pelas companhias a fim de aumentar sua proteção contra os ataques de Engenharia Social que, em sua maioria, parecem inofensivos ao olhar da vítima.

# 2. OBJETIVOS

## 2.1 OBJETIVOS GERAIS

O objetivo geral deste trabalho de conclusão de curso é demonstrar a importância que as empresas devem despender em relação a engenharia social dentro dos seus ambientes, com a finalidade de evitar invasões e ou fraudes causadas pela imprudência ou auxilio não intencional de colaboradores como brechas para o trabalho de um hacker.

## 2.2 OBJETIVOS ESPECÍFICOS

i) Ilustrar a forma como um engenheiro social atua em um ambiente.

ii) Demonstrar os principais métodos utilizados para aproveitar-se das falhas humanas com objetivo de obter informações.

iii) Demonstrar empiricamente o real risco de invasão e vazamento de dados sigilosos a que as empresas ainda estão sujeitas e, assim, convencer seus administradores da necessidade de investimento em capacitação de pessoal a fim de evitar prejuízos causados por ataques possibilitados pela engenharia social.

iv) Propor formas de prevenção a ataques externos a fim de evitá-los.

## 3. A ENGENHARIA SOCIAL

Conforme exposto na introdução, a Engenharia Social é o ato de manipular ou enganar pessoas. Dentro do contexto de segurança da informação, a Engenharia Social é vista como a porta de entrada para grande parte dos ataques a empresas. Sem uma pessoa para entregar um acesso válido para o atacante, a chance de quebrar o grande muro de defesas técnicas adotados hoje por empresas é bastante menor.

Diferentemente dos sistemas de uma empresa, os seres humanos não são tão facilmente controláveis. Cada pessoa foi “programada de maneiras infinitamente complexas e, portanto, agem de maneiras diferentes às abordagens dos agressores.” Sendo assim, cada indivíduo possui características que podem vir a ser exploradas visando sua manipulação, como por exemplo a pré-disposição a ajudar um terceiro e a resistência a entrar em conflitos pessoais.

O departamento de TI ou a respectiva área responsável pela gestão da Segurança da Informação de uma empresa pode ter os mais aprimorados sistemas, como firewalls, ferramentas de vazamento de informações e criptografia de dados. De nada estas proteções valerão se os funcionários não forem capacitados a respeito da criticidade de informações e a respeito de quais dados podem tratar com outros funcionários, clientes e pessoas alheias à corporação. De nada adiantam várias tecnologias com objetivo de realizar a proteção dos dados corporativos se um atacante conseguir obter informações sigilosas através de uma simples ligação telefônica.

E como chega-se, de fato, às informações e ações através das pessoas? Kevin Mitnick, em seu livro A Arte de Enganar, obra em que explana os artifícios da engenharia social e ilustra os métodos que utilizou enquanto hacker, dá um amplo panorama de como conseguir informações e quebrar protocolos utilizados em empresas de maneira simples, principalmente utilizando-se de contatos telefônicos. O próprio Mitnick iniciou a carreira de hacker efetuando ataques simples em estações de ônibus.

Ian Mann informa em “Engenharia Social”, livro em que ilustra o resultado de vários anos prestando consultoria na área de engenharia social, baseado em estudos empíricos e consultorias, quais os processos para leitura de uma pessoa e como fazer para ganhar sua confiança e enganá-la. Toda a seção 2 ilustra os elementos do

comportamento humano e como fazer para driblar suas proteções naturais e explorar possíveis falhas através de mecanismos como confiança, empatia e intimidação.

Para uma pessoa mal-intencionada e que já conhece os colaboradores e processos da empresa, o risco potencial de dano é muito maior. É por este motivo que se abordam também, neste trabalho, quais os riscos e possibilidades de ataques que uma pessoa de dentro da empresa pode causar à corporação. Nesse último caso, o dano seria muito maior, uma vez que se não forem adotados certos procedimentos preventivos, um ex-funcionário continuará com acessos às instalações da empresa, contatos com pessoas e fornecedores, como no exemplo explorado na presente análise. Com somente uma dessas informações já é possível conseguir dados e manipular ações de funcionários e, assim, prejudicar a empresa ou simplesmente coletar dados sigilosos.

Um gestor de uma empresa, hoje, deve estar atento ao setor de TI e ao de desenvolvimento humano, se quiser se proteger devidamente dos riscos da segurança da informação, incluindo a engenharia social. Somente delegar todas estas tarefas aos profissionais de TI não será suficiente, pois nem todos os membros desta equipe possuem o trato adequado para lidar com questões relacionadas ao comportamento humano. Talvez seja o caso de envolver, inclusive, o departamento de Recursos Humanos. O trecho abaixo, de Ian Mann (2011), aborda este tema:

> Muita gente acaba em um cargo de TI porque gosta de tecnologia. Se quisesse trabalhar com pessoal, estaria trabalhado com Recursos Humanos. Assim, se você é executivo, com responsabilidades que incluem segurança da informação, pense nas diferentes pessoas dentro das suas equipes. Elas estão oferecendo a você o equilíbrio correto entre segurança física, de TI e humana? Você pode precisar pensar em recrutar um psicólogo!

Baseado na citação de Mann, pode-se afirmar que a segurança da informação é um processo que conta com a participação de todos os indivíduos da corporação, pois qualquer pessoa envolvida nos assuntos de uma companhia está sujeita a ser alvo de ataques. Sendo assim, é de suma importância a preparação dos profissionais no que tange à possíveis abordagens sociais.

Segundo Santos (2016), um engenheiro social precisará, primeiramente, coletar o maior número de informações necessárias para a efetivação do ataque. Em posse destas informações, os ataques se dividirão em duas abordagens: social e técnica. Na primeira, o atacante tenta conseguir seus objetivos somente manipulando as pessoas por telefone ou pessoalmente, visitando as dependências da empresa. Na

segunda abordagem, o cracker se utilizará de ferramentas técnicas para conseguir o que deseja, como mídias sociais, mensagens de celular e sites falsificados.

## 3.1 A COLETA DE INFORMAÇÕES

A coleta de informações é o primeiro estágio que um atacante realiza. É neste momento em que ele mapeia todas as fraquezas da vítima para ter as informações necessárias para conceber o ataque, seja ele qual for.

Nesta etapa o objetivo é agregar a maior quantidade possível de dados para que, quando do ataque efetivamente dito, não haja surpresas que possam vir a prejudicar o andamento da operação.

Independentemente do objetivo do ataque ser somente a coleta de informações ou a invasão dos sistemas da empresa tecnicamente, este momento é importante, pois é através dele que pode se conhecer tanto as tecnologias da empresa, a fim de encontrar um caminho de entrada, quanto informações estratégicas. Os seguintes processos podem ser utilizados neste momento:

a) Pesquisa pública: qualquer pessoa consegue pesquisar sobre uma empresa através de seu website e já a partir daí ter os contatos iniciais (daqueles colaboradores necessários para aplicação ou sucesso do golpe). Algumas corporações, inclusive, listam seus representantes no site da empresa, visando demonstrar mais transparência aos possíveis clientes. O que não se leva em conta é que este tipo de informação, por exemplo, pode ser usado para captura de dados manipuláveis ou restritos. A partir disso pode-se pesquisar mais sobre a pessoa em si na internet e em suas redes sociais, sabendo assim seus costumes, personalidade e, dependendo do nível de cuidado do alvo, até mesmo sua localização, o que poderia acarretar, em casos extremos, em sequestro.
b) Ligações telefônicas: conforme dito na introdução, algumas informações consideradas críticas podem ser conseguidas simplesmente perguntando às pessoas. Segundo Fonseca (2011), o telefone é um dos meios mais utilizados pelos engenheiros sociais na busca por informações. Ainda Segundo Fonseca (2011), “o Engenheiro costuma utilizar chamadas em cadeia, quando o objetivo é conseguir informações mais profundas de uma companhia. Faz-se uma primeira chamada, onde serão fornecidas informações sobre nomes de pessoas ou dados técnicos. Para conseguir essas

informações, basta se passar por cliente ou possível patrocinador da empresa atacada. Na segunda chamada o atacante utiliza as informações obtidas na primeira chamada para que outra pessoa diferente da primeira chamada, passe informações ainda mais valiosas.” Seguindo este processo, o engenheiro consegue ir articulando informações e pessoas e, assim, conseguir os dados de que necessita.

c) Testes de acesso: neste momento o atacante utiliza-se de procedimentos técnicos para conseguir informações sobre as tecnologias empregadas pela empresa. Para isto, simula acessos a servidores web e servidores de e-mail, por exemplo, a fim de saber as versões de software utilizados e descobrir, assim, suas vulnerabilidades.
d) Visita física: uma das etapas que apresenta maior risco ao atacante é quando se dirige diretamente à empresa, se fazendo passar por cliente, por exemplo, a fim de descobrir os métodos de segurança da empresa e as dependências físicas, com o objetivo de saber, assim, seus defeitos e formas de agir futuramente.

## 3.2 TIPOS DE ATAQUES

### 3.2.1 Phishing

A técnica de phishing consiste em enviar mensagens falsas a usuários (via SMS, e-mail ou mídias sociais) se fazendo passar por uma empresa, com um conteúdo que seja atrativo. O objetivo é que a vítima clique em um link malicioso que a levará a um site, também falso, para a captura das informações digitadas pela vítima. Tal ataque também pode visar a infecção imediata através do download de um aplicativo malicioso (FONSECA, 2017).

### 3.2.2 Telefone

Nesta abordagem, o engenheiro social faz ligações telefônicas às vítimas a fim de, através da habilidade de persuadir, melindrar ou conseguir a empatia do atacado levando-o a executar ações ou passar dados sigilosos. SILVA, ARAUJO e AZEVEDO (2013).

### 3.2.3 Visitas Presenciais

Trata-se de visitas ao local do ataque para conseguir pessoalmente as informações desejadas ou execução de processos. O atacante pode se fazer passar por um fornecedor ou um cliente. Um hacker experiente pode utilizar-se de diversas formas para conseguir lograr seu objetivo. Tais formas podem ser o uso da autoridade, empatia, curiosidade ou qualquer outro aspecto que o permita enganar pessoas (OLIVEIRA, 2017).

### 3.2.4 Spam

Envio de vários e-mails a fim de conseguir que o usuário clique em um link malicioso ou execute um arquivo infectado.

### 3.2.5 Varredura de Lixo

Esta técnica de ataque consiste em revirar, literalmente, o lixo das instituições que são o alvo dos ataques, a fim de conseguir informações sigilosas (FONSECA, 2017).

### 3.2.6 Smishing

Nome dado à abordagem iniciada via mensagens SMS. Pode ser tanto um tipo de *spam* (item 3.2.4) ou levar a um phishing (item 3.2.1).

### 3.2.7 Baiting

Esta técnica consiste em deixar dispositivos infectados, como pen drives ou cd-roms, à disposição de vítimas. Boa parte das pessoas não hesita em, ao encontrar um desses dispositivos, conectá-los em seus computadores para checar o conteúdo (OLIVEIRA, 2017).

## 4. METODOLOGIA

Segundo PATTON (2002), o estudo de caso é o ato de reunir informações acerca de um fenômeno. É uma análise de um fenômeno atual ou passado, baseado em provas coletadas de inúmeras fontes e que pode ser baseado em entrevistas ou em pesquisa científica (Freitas e Jabbour, 2011).

Os resultados deste estudo de caso foram obtidos de forma empírica, ou seja, através da experiência (FERREIRA, 1985). Foram utilizadas várias das técnicas anteriormente citadas.

O ambiente utilizado para o estudo de caso de uma empresa trata-se de uma situação hipotética de um ex-funcionário mal-intencionado e que deseja informações da companhia para prejudicá-la. Leve-se em conta o fato de que todos os testes aqui aplicados foram antes autorizados pelo gestor da empresa a qual serviu de vítima.

Abaixo segue o plano de ataques previsto:

i) *Footprint*: Análise e mapeamento das vulnerabilidades e de informações do alvo. Tal processo constitui-se através de pesquisas e ligações simples ao alvo com o objetivo de manipulá-lo e conseguir informações a respeito da empresa;

ii) Ataques telefônicos: Ligações objetivando vários tipos de informações, desde dados sigilosos até manipulação de agentes para obtenção de ações técnicas e administrativas;

iii) Roubo de informações de lixo e impressoras: Tal método visa coletar dados geralmente descartados por funcionários e que podem vir a se tornar úteis.

iv) Ataque pessoal ao estabelecimento: Este método visa ter acesso pessoal e direto ao setor de TI da empresa e conseguir ter a liberdade de agir diretamente nos equipamentos confinados.

# 5. ESTUDO DE CASO

O presente estudo visou efetuar, diretamente, ataques de engenharia social. A empresa atacada atua no seguimento comercial, no ramo automotivo, com aproximadamente 2000 funcionários, no estado do Paraná e Santa Catarina. O setor atacado foi o de tecnologia da informação, em virtude do conhecimento que o hacker tinha, por ser um ex-colaborador, e assim ter maior facilidade para se fazer parecer convincente.

Abaixo seguem listados os ataques efetuados, informando os objetivos de cada um e o procedimento adotado. A escolha dos ataques foi definida baseada no ambiente de estudo, visando um caso real, de forma que não foram executados todos os ataques descritos no capítulo 3.

## 5.1 ATAQUES

Abaixo seguem os tipos de ataques efetivados:

### 5.1.1 A Ligação de Footprint

Neste estudo de caso, o *footprint* iniciou-se com várias visitas às páginas web do grupo em questão, a fim de entender qual a dinâmica da empresa, seus negócios e, principalmente suas marcas (considere, pois, que o atacante hipotético direcionou as buscas aos dados que desconhecia, uma vez que tratava-se de um ex-funcionário já munido de informações internas e específicas sobre seu alvo).

Iniciado o *footprint*, foram feitas ligações para uma das lojas da rede a fim de descobrir os nomes de gestores e pessoas que poderiam vir a ter acesso privilegiado dentro da organização. Para tanto, o atacante fez-se passar, via telefone, por um cliente que havia tido problemas jurídicos com a empresa. Para resolver o assunto, a empresa teria ligado para o cliente e solicitado a este que conversasse com o gerente da loja em questão, haja vista que seria a pessoa com maior autonomia para responder por tal situação. Nesta ligação conseguiu-se facilmente, em conversa com o setor de atendimento, o nome do gestor, a localidade onde trabalhava e o telefone de seu escritório.

Após este telefonema foram efetuadas tentativas de contato com o gestor nos canais informados para checagem das informações coletadas.

### 5.1.2 Reset de Senha

Neste teste a intenção original era checar o quanto de informação seria possível conseguir via contato telefônico. Como os dados de acesso são uma das informações mais secretas que um usuário deve manter, tentou-se conseguir as credenciais de acesso do usuário. Tal procedimento só seria possível de duas formas: solicitando ao usuário, o que inviabilizaria o teste, ou entrando em contato com outra pessoa que tivesse acesso a estas credenciais. O que foi feito foi entrar em contato com o setor de TI, fazendo-se passar pelo próprio funcionário, a fim de conseguir que o setor citado informasse quais os dados de acesso do usuário.

Para tal, entrou-se em contato primeiramente com uma das filiais do grupo, fazendo-se passar pelo gestor cujos dados foram obtidos no item 5.1.1, querendo informações sobre o setor de TI. Iniciou-se a ligação e ela caiu em uma pessoa do departamento de TI, mas que não era responsável pelo atendimento esperado. Pediu-se a esta pessoa informações de contato para falar com o suporte a usuários, alegando um simples problema sistêmico urgente. Tal informação foi passada de forma prestativa sem nenhum questionamento.

Após a última ligação, entrou-se em contato com o departamento de suporte fazendo-se passar pelo usuário cujos dados conseguiu-se já na primeira tentativa. Neste contato, informou-se ao técnico que o usuário estava sem acesso aos seus sistemas e que sua senha não funcionava. Inicialmente houve uma resistência por parte do técnico em efetuar o reset da senha e passá-la por telefone, pois existe uma diretiva do setor em não passar este tipo de dado via telefone. Com um pouco de persuasão, utilizando o argumento de que dados para a diretoria dependiam deste acesso, por fim o técnico efetuou o reset de senha e informou a nova senha por telefone. Mais do que isso, foi possível convencê-lo a configurar um acesso VPN (tecnologia para acesso remoto ao ambiente da empresa) para que o hipotético usuário pudesse trabalhar de fora do escritório.

Com os dados obtidos, praticamente qualquer ação pode ser tomada em nome do gestor cujos dados foram vazados. Desde troca de e-mails, pelos quais qualquer

coisa pode ser autorizada formalmente até acesso a sistemas da empresa, autorizando ações, vendas indevidas e etc.

### 5.1.3 Recuperação de Senha de Fornecedor

A intenção deste ataque era se fazer passar por fornecedor de serviços de informática, a fim de conseguir credenciais de acesso a sistemas. Para este ataque, o hacker aproveitou-se de informações que já possuía por ser ex-funcionário da empresa que seria a vítima do ataque. Entrou-se em contato com a empresa identificando-se como funcionário de uma empresa que presta serviços de consultoria a um ERP, informando que havia um problema na conexão com o sistema. A desculpa era que o hacker era um analista que não conseguia acesso ao referido sistema porque estava trabalhando de sua casa naquele dia, sendo que os dados de acesso haviam ficado na empresa. Aqui tentou-se criar empatia com a vítima, apelando para acidentes e esquecimentos rotineiros. A única dificuldade foi que a vítima questionou qual era a senha que este estava utilizando. Como o hacker não tinha ideia de qual era a senha antiga, simplesmente inventou uma nova combinação que contivesse o nome da empresa entre os caracteres, simulando uma prática bastante comum entre as empresas, que é a de gerar senhas temporárias com fáceis combinações e que acabam, por fim, nunca sendo alteradas. Com esta informação a vítima não teve dúvidas e repassou a senha de acesso ao sistema requerida pelo pseudo-analista.

### 5.1.4 Acesso Físico ao Setor de TI

O objetivo deste ataque foi conseguir acesso físico a uma das salas de TI de uma das lojas do grupo em questão. Para este ataque, o hacker decidiu se dirigir a uma localidade onde nunca havia ido, para se assegurar de que não seria uma pessoa já conhecida por alguém do local e teria sua entrada facilitada.

O ataque iniciou-se pela preocupação com a aparência. O hacker chegou à localidade com uma roupa básica, normalmente utilizada por técnicos de informática, e uma mochila de notebook para simular que estava na localidade a trabalho. Entrou na loja pelo estacionamento de funcionários, para dar a impressão de que sabia o que estava fazendo e então entrou na companhia se apresentando à recepção. Ali, informou ser do departamento de TI e que estava no local para fazer uma manutenção,

e como não sabia onde era a sala de TI do local, precisava que alguém o acompanhasse. Sem questionamentos a recepcionista o levou ao encontro de uma das gestoras da localidade, que não tinha o cartão de acesso ao CPD. O hacker, que sabia que sua digital ainda provavelmente estaria válida, não quis se utilizar deste subterfúgio e manipulou a gerente a conseguir o cartão de entrada se desculpando pelo esquecimento do próprio cartão de acesso. Enquanto isto, utilizou o dedo incorreto no acesso biométrico para provar que não conseguiria entrar. Esta não pestanejou e procurou o gestor da loja que teria o cartão para acesso ao datacenter. Como o gestor não estava presente, o hacker utilizou a digital correta para acesso e entrou no local desejado, e em nenhum momento foi questionado sobre sua identidade.

### 5.1.5 Coleta de Dados Via Mídia Sociais

Para este ataque foi criado um site falso de promoções visando conseguir coletar dados cadastrais de usuários. A proposta tratava-se de contactar as vítimas via mensagens pessoais por WhatsApp ou SMS, divulgando um site de promoções que necessitaria de um pré-cadastro para ativar o usuário dentro da plataforma.

Para acesso, criou-se um site público com características comuns para abordagens de clientes: um site moderno, chamativo e focado em fazer o usuário fazer seu cadastro sem ter muitos questionamentos.

### 5.1.6 Obtenção de Lixo

Neste ataque visou-se aproveitar um momento em que o hacker estivesse na empresa para conseguir dados que haviam sido descartados pela vítima. Para este teste, aproveitou-se de dois momentos de distração das vítimas para conseguir papéis que haviam sido jogados no lixo e documentos que haviam sido deixados na caixa descartável ao lado da impressora do departamento. Deixar uma caixa ao lado da impressora é um procedimento comum à maioria das empresas, uma vez que é comum que páginas desnecessárias sejam impressas por engano.

Para conseguir dados impressos, o atacante hacker aproveitou o momento de chegada, quando não foi questionado a respeito do seu motivo de estar dentro das instalações da empresa e em nenhum momento foi interrompido. Os dados do lixo

foram conseguidos entrando-se em um setor onde não havia ninguém no momento, pois era hora de pausa para o almoço e não havia nenhum outro funcionário em horário de trabalho.

## 5.2 RESULTADOS DOS ATAQUES

### 5.2.1 Footprint

Analisando o processo de *footprint*, pode-se, já de imediato, encontrar vários erros processuais durante as ligações telefônicas. Destes, merecem atenção:

i) De início, percebe-se que a funcionária da empresa não se preocupa em coletar dados da pessoa que está ligando, a fim de checar se a informação acerca do processo supostamente informado pelo atacante é real. Assim, o atacante se sente confortável em dirigir a conversa para o local onde quiser. Um pouco de autoridade e suposta má-vontade ou mau-humor por parte do atacante ajuda neste momento, pois faria com que a vítima se sentisse melindrada por conta de ser um problema judicial.

ii) A vítima, após conversar com um colega de trabalho, decide dar ao atacante o nome do gestor em questão, que é a informação que o atacante realmente quer, além do telefone de contato pessoal deste, fazendo assim com que seja possível encontrá-lo a qualquer momento e saber sem problemas o seu paradeiro.

iii) Em outra ligação a outra loja, informada pela usuária do primeiro contato, fala-se com outro funcionário que não vê problemas em dizer que não sabe do paradeiro do gestor, além de pedir que se entre em contato em outro horário para nova tentativa.

### 5.2.2 Reset de Senha

Neste ataque, claramente percebe-se a falta de treinamento do técnico que efetuou o atendimento, uma vez que facilmente o atacante conseguiu as informações que queria, no caso conseguir efetuar o reset da senha do gestor em questão. Uma vez com esta informação, qualquer atacante conseguiria acesso aos sistemas corporativos através da senha da vítima de modo que qualquer privilégio poderia ter

sido assumido, desde procedimentos financeiros até contratuais, uma vez que o e-mail estaria liberado para o atacante.

Analisando com calma o ataque, percebe-se que o técnico se melindrou facilmente com o atendimento já de início, quando o atacante informou se passar por uma pessoa de importância dentro da corporação. A pressão por parte do atacante se tornou maior ainda a partir do momento em que, ao perceber uma certa resistência por parte da vítima, o engenheiro social perguntou se o técnico desejaria que o seu diretor entrasse em contato para solicitar o desbloqueio do acesso. Isso desarmou de uma vez por todas a atitude do técnico que, ao se ver pressionado por um cargo de alta posição, preferiu atender à demanda do que enfrentar a situação e seguir seu procedimento.

No capítulo 8 de A Arte de Enganar, Kevin Mitnick diz que a intimidação é uma das ferramentas bastante utilizadas por um engenheiro social, pois a maioria das pessoas prefere não entrar em conflitos, principalmente no ambiente de trabalho. Se a pressão vier de alguém com alto cargo dentro da organização, a chance de o atacante conseguir as informações que deseja se torna maior ainda, uma vez que a maioria das pessoas preza muito pelo emprego e acaba achando que é melhor não entrar em conflito com um diretor, por exemplo.

### 5.2.3 Recuperação de Senha de Fornecedor

De todos os casos, este é um dos mais perigosos em termos de potencial destrutivo. Uma pessoa mal-intencionada com dados de acesso de bancos de dados tem a possibilidade de parar a operação de uma empresa inteira.

Os colaboradores que possuem acesso a informações privilegiadas devem estar treinados a fim de evitar que atacantes consigam acesso a estes dados. A forma de abordagem do atacante, neste caso, foi simples e direta. Tratando-se de um ex-funcionário, já tinha conhecimento das empresas que prestavam serviços e simplesmente fez-se passar por um funcionário de uma destas empresas. Tal informação também poderia ter sido conseguida de outras formas. Uma delas é entrar em contato com a empresa vítima se fazendo passar por um prestador de serviços, a fim de conseguir informações sobre as empresas que hoje são fornecedoras. Com

estes dados, torna-se simples um contato na empresa fornecedora para conseguir informações das pessoas que de fato trabalham para o cliente em questão.

Informar senhas de acesso via telefone deve ser explicitamente proibido em qualquer situação. Inicialmente a vítima ainda quis fazer alguma validação perguntando ao atacante qual era a senha que este estava utilizando para acesso. O atacante simplesmente inventou uma senha que contivesse o nome da empresa, uma vez que este é um procedimento bastante comum no processo de geração de senhas: fazer um algoritmo com o nome da corporação.

Dos processos que poderiam ter sido adotados para evitar este ataque, um deles é o mesmo do item anterior: validação de dados do interlocutor. O mínimo a se fazer seria confirmar os dados da pessoa ao telefone, bem como da empresa de onde falava. Uma validação simples seria solicitar que a senha fosse requisitada por e-mail ou então informar que o contato seria retornado para a sede da empresa prestadora de serviços a fim de confirmar que se tratava mesmo de uma requisição genuína.

### 5.2.4 Acesso Físico ao Setor de TI

Este, de todos os ataques, é potencialmente o mais perigoso. Tanto a vítima quanto o engenheiro social estão em potencial risco. Da parte do atacante, o risco, no caso de ter sua identidade descoberta, pode se mostrar bastante alto a ponto de haver denúncias até mesmo policiais. A vítima, ao perceber que o ambiente da empresa está sendo invadido, pode reagir da maneira mais agressiva e ou imprudente possível.

Da parte da vítima, o risco é bastante alto no caso de o atacante conseguir acessar as dependências da empresa. Uma vez dentro das dependências da companhia o hacker já conseguiria acesso à rede da empresa através de uma mesa vazia ou de uma sala de reunião em desuso. Uma vez dentro do Datacenter o hacker conseguiria ter acesso a praticamente qualquer equipamento que queira atacar. Por ataque, entenda-se tanto golpes virtuais quanto físicos, como furto de equipamentos ou simples sabotagem.

Dentre os principais erros que levaram ao sucesso deste ataque, estão entre os principais:

i) Controle de acessos: a falta de ação do setor de TI no controle de acessos fez com que fosse possível o acesso ao datacenter através da impressão digital do atacante. Se os acessos do ex-funcionário fossem

totalmente desativados no momento de seu desligamento, não seria possível a este ter sucesso no ataque. Mesmo sem ajuda de outro funcionário, o ataque teria tido sucesso, uma vez que o colaborador não teria nenhuma resistência para chegar ao CPD.

ii) Treinamento dos colaboradores: em nenhum momento percebeu-se resistência ou desconfiança dos colaboradores da filial visitada. Mesmo sem conhecer nenhum dos funcionários o atacante não foi alvo de questionamentos de qualquer tipo. Faltou aos colaboradores da empresa o treinamento para questionar estranhos e /ou funcionários desconhecidos. O ataque poderia ter sido evitado com simples validações como questionamentos acerca das pessoas que trabalham no setor de TI. Além disso, também é uma boa prática que as informações de desconhecidos sejam validadas diretamente com os gestores da área. Uma ligação para o responsável do departamento de TI resolveria o problema e desarmaria a tentativa de intrusão. Este é o tipo de ataque que se vale da boa vontade e educação das pessoas. Além disso, departamentos técnicos tendem a ser ignorados por pessoas de outra área de atuação. Como o conhecimento é técnico, as pessoas tendem a assumir como verdade qualquer informação proveniente destes setores.

### 5.2.5 Coleta de Dados via Mídias Sociais

Este ataque foi o que se utilizou de maiores procedimentos técnicos para conseguir os dados dos usuários. Através de mídia social, como WhatsApp, um site foi divulgado, informando um portal onde os usuários poderiam se cadastrar e conseguir promoções na cidade de Curitiba, cidade onde está localizada a sede da empresa e a maioria de suas filiais. O site em questão foi montado com foco em passar credibilidade ao usuário, utilizando-se de alguns pontos importantes:

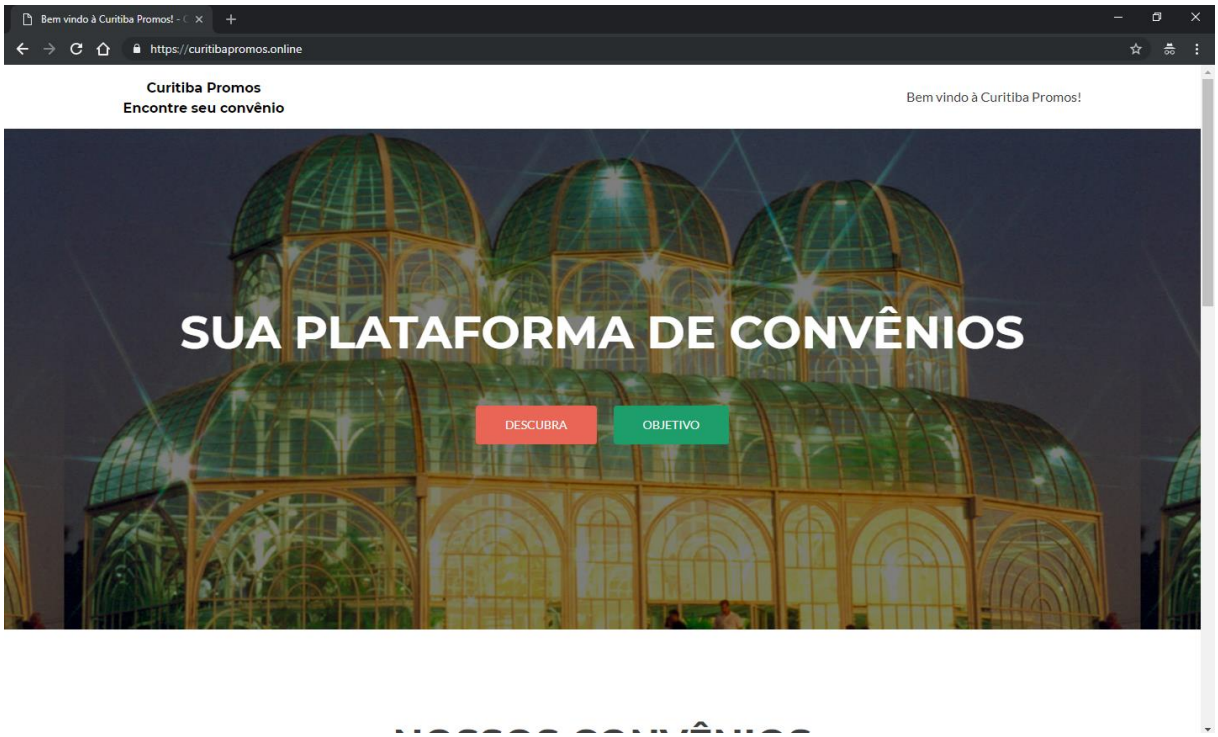
i) Simples e de fácil navegação;

ii) Acesso garantido via HTTPS (protocolo utilizado para navegação, mas com uma camada extra de segurança). Boa parte dos usuários com um pouco mais de cuidado levam este item em consideração na hora de confiar em um site;

iii) Site com domínio próprio, visando agregar confiança à marca;

iv) Presença em motores de busca como Google.

**Figura 1 - Site falso apresentado a vítimas**




Fonte: print screen de site falso.

Todos os itens listados anteriormente visavam conseguir a confiança do usuário a fim de que se cadastrasse com seu nome e e-mail no site. Um atacante de verdade utilizaria estes dados da forma que lhe melhor parecesse. Poderia ele se fazer passar pela vítima, utilizar seu e-mail para envio de spam e até solicitar cartões de crédito, caso os dados solicitados no site fossem de documentos e endereço de moradia.

### 5.2.6 Obtenção de Lixo

Verificar e coletar dados descartados pode ser uma boa prática tanto na etapa de *footprint* quanto no ataque em si, dependendo do foco. Neste ataque acadêmico foram checadas as lixeiras e bandejas de impressoras. É comum existir, ao lado das bandejas de impressoras, um outro local para o descarte e reaproveitamento de páginas impressas incorreta ou desnecessariamente. As lixeiras verificadas não tinham nenhum dado que pudesse ser aproveitado, diferente das bandejas de reaproveitamento de papel. Nestas, foram encontrados dois documentos: uma nota

fiscal, cujos dados empresariais poderiam ser reaproveitados, e um comprovante de residência de cliente, com vários dados pessoais de uma pessoa física.

Com os dados da empresa, uma pessoa mal-intencionada poderia muito bem fazer-se passar por funcionário para obter vários tipos de informação quanto para fazer vários tipos de cadastros em nome da empresa, e essa só teria conhecimento quando da ocasião de um problema ou incidente.

Com os dados do cliente, o atacante poderia facilmente procurar por mais dados deste na internet e se fazer passar pela pessoa em questão. Além disso, com somente dados de endereço e alguns dados pessoais, um atacante pode facilmente, por exemplo, criar um cartão de crédito em nome da vítima e essa só saberia do ocorrido quando recebesse algum tipo de cobrança ou visse que seu nome estava incluso no cadastro de proteção ao crédito. Isto somente para citar algumas das situações em que a vítima poderia se ver envolvida.

## 6. TENTATIVAS FRUSTRADAS

Todos os ataques descritos e analisados até agora neste estudo obtiveram sucesso, mesmo que parcialmente, em conseguir angariar informações ou ações potencialmente perigosas das vítimas. No entanto, algumas tentativas deste estudo de caso não foram bem-sucedidas. Há de se considerar que, por conta de ser um trabalho acadêmico, optou-se por coletar o mínimo de informações pessoais possíveis, de modo a não haver a possibilidade de comprometer os indivíduos. Dessa forma, e não havendo tempo hábil para análise do comitê de ética da UTFPR para o teste descrito em 5.1.5, não foram utilizadas todas as formas de abordagens que um ataque deste tipo apresentaria. Em um ataque real, o cracker tentaria, além do nome e e-mail, empregados neste trabalho, conseguir dados pessoais como senhas e dados de documentos pessoais.

Descreve-se abaixo as tentativas em que não se teve sucesso, mas que da mesma forma servem como aprendizado no estudo da Engenharia Social:

i) Tentativa de ataque telefônico para coleta de informações sobre configuração externa de e-mails: Neste ataque foi feita uma tentativa, após a demonstrada no item 5.2, de conseguir informações técnicas acerca de qual seria o procedimento correto a ser adotado para a configuração de e-mails em um dispositivo pessoal. Durante a tentativa de convencimento do técnico, este foi interrompido pelo líder de time, que ao ouvir a conversa, questionou o motivo de o técnico estar passando informações do tipo de forma tão despretensiosa.

   O líder, então, solicitou que a ligação fosse transferida para ser tratada pessoalmente por ele. Acontece que a pessoa por quem o hacker estava tentando se passar era um funcionário bastante conhecido do líder de time, que em outras situações já tivera oportunidades de ter contato pessoal com aquele. Ao desconfiar do timbre de voz diferente e do tipo de ligação, questionou o hacker que, encurralado, foi obrigado a encerrar a ligação alegando que iria escalar o assunto.

ii) Pesquisa comportamental: Disparou-se uma pesquisa de comportamento para tentar mapear o quanto as pessoas se

preocupam com os dados que publicam na internet. O resultado foi bastante além do que se esperava em termos de cuidado. Os entrevistados, em sua maioria, demonstraram um comportamento que, se real, faria com que tivéssemos muito poucos ataques bem-sucedidos. Entende-se que, pelo fato de as pessoas estarem cientes de que estavam sendo analisadas, responderam levando em conta que tomam mais cuidado do que realmente fazem na realidade, como, por exemplo, check-ins em restaurantes e fotos de viagem, o que relataram não compartilhar, por exemplo.

# 7. BOAS PRÁTICAS

Abaixo seguem as boas práticas que podem ser adotadas para evitar a ocorrência dos ataques executados neste estudo de caso.

## 7.1 LIGAÇÃO DE FOOTPRINT

Nos três casos listados no item 5.1.1.1 percebe-se claramente a falta do que tanto Mitnick quanto Mann chamam de classificação das informações das empresas. Classificar as informações refere-se a tratar determinados tipos de informação de acordo com o público ao qual se referem. Um procedimento padrão simples e que poderia frustrar uma tentativa de coleta de informações é o de classificação em 3 estágios: Público, Privado e Confidencial, a saber:

i) Público: Informações que são possíveis de serem dadas a qualquer pessoa, como contatos comerciais e específicos da empresa, referentes ao contato entre clientes e o negócio da empresa.

ii) Privado: informações não passíveis de serem dadas a qualquer pessoa e que só dizem respeito ao ambiente corporativo. Estão contempladas nesta categoria as informações referentes a procedimentos internos, dados corporativos administrativos e estratégicos da empresa.

iii) Confidencial: dados que não devem ser divulgados nem internamente dentro da corporação, como dados cadastrais de funcionários, remuneração, resultados de setores e ações estratégicas que só dizem respeito à direção ou presidência.

## 7.2 RESET DE SENHA

Ter procedimentos internos bem definidos é essencial para se proteger de ataques de engenharia social. Os atendentes devem estar bem treinados a respeito dos processos que devem seguir e das ações que devem tomar em situações em que se sintam atacados, como transferir a ligação para uma pessoa treinada para lidar com este tipo de situação.

Ações simples fariam com que o ataque descrito no item 5.1.2 não fosse bem-sucedido. De imediato pode-se dizer que um checklist inicial para confirmar os dados do solicitante já dificultaria o acesso do engenheiro social. Adicionalmente, levando

em conta que dados pessoais não são algo muito difícil de se conseguir, os técnicos poderiam adotar um processo de retornar o contato para o telefone cadastrado do funcionário, a fim de confirmar que de fato se trata do colaborador em questão.

## 7.3 RECUPERAÇÃO DE SENHA DE FORNECEDOR

O ataque do item 5.1.3 é bem típico e o que Mitnick descreveu como o mais fácil[3]: simplesmente pedir pelo dado desejado. Neste caso, uma senha sistêmica.

A boa prática, aqui, é treinar os usuários a se atentarem para os tipos de informação que costumam passar para terceiros, principalmente se forem dados críticos. Nunca, em hipótese alguma, um funcionário deve repassar informações críticas, como senhas, via telefone. Estas devem ser fornecidas aos interessados via métodos seguros, como cartas registradas ou através do gestor responsável.

## 7.4 ACESSO FÍSICO AO SETOR DE TI

O ataque descrito no item 5.1.4 é um dos que podem ser mais perigosos em termos de risco, pois o atacante terá tanto acesso lógico ao ambiente quanto físico. Poder-se-ia tanto prejudicar a empresa através de *hacking* via elementos de rede quanto fisicamente, como roubar um equipamento ou danificá-lo.

A melhor forma de prevenção, neste caso, é uma boa checagem dos dados de desconhecidos. Uma simples solicitação de dados cadastrais, como crachá, por exemplo, frustraria o ataque. Além disso, como o atacante não tinha, aparentemente, o acesso à sala de TI, o acompanhante da filial já deveria tê-lo acompanhado até a saída e contatado a pessoa responsável, como o gestor de TI.

## 7.5 COLETA DE DADOS VIA MÍDIAS SOCIAIS

Para o ataque descrito no item 5.1.5, a conscientização é de extrema importância, pois afeta também a vida pessoal do funcionário. Um bom treinamento é a forma sugerida para conscientizar os funcionários a terem cuidado com as informações que compartilham na internet. O treinamento deve focar nos riscos que as informações compartilhadas podem trazer também à vida pessoal, como sequestros, detalhes da vida e segurança pessoal.

## 7.6 OBTENÇÃO DE LIXO

O descarte correto do lixo, no sentido de risco de informações, é um assunto pouco abordado no espaço corporativo, por conta do crescimento da vida digital. Porém, em alguns casos, ainda pode ser possível conseguir muitas informações através de papéis jogados no lixo ou descartados para reciclagem.

Para evitar que o hacker conseguisse informações através de um dos itens acima, os funcionários devem ser avisados quanto aos riscos de considerarem dados no lixo como descartados. Ao menos os dados críticos e internos devem antes ser picotados ou descartados de uma forma que não possam mais ser recuperados. Dessa forma, um atacante não conseguirá informações através do descarte inadequado.

## 8. CONCLUSÃO

Após extenso trabalho de pesquisa e atuação em campo, conforme o presente trabalho demonstrou, percebe-se a necessidade de se atuar mais na capacitação e conscientização de pessoas/colaboradores no que tange aos riscos da engenharia social em ambientes corporativos.

Os testes aplicados demonstram que ainda é fácil aproveitar-se do elemento humano para o ganho de informações e vantagens. As ligações telefônicas demonstraram que é preciso pouco conhecimento da empresa para que seja possível conseguir o convencimento da outra pessoa e, assim, fazer com que esta proceda da forma como o atacante deseja ou conceda a este as informações pretendidas.

Através de ligações e ações simples, provou-se como é possível a uma pessoa mal-intencionada, até mesmo sem um conhecimento prévio do ambiente corporativo, conseguir coletar informações, ter acesso digital e físico a sistemas e locais restritos e fazer com que pessoas obedeçam a ordens ou atendam a pedidos de indivíduos a quem não conhecem, baseado simplesmente na segurança do conteúdo da conversação, como proposto por Mitnick.

Além da demonstração dos ataques, também provou-se que as boas práticas que poderiam ser adotadas a fim de evitar que se obtivesse sucesso no ganho de informações e manipulação de pessoas são fundamentais para a segurança completa dos dados disponíveis em uma empresa. A adoção de políticas internas à corporação voltadas ao desenvolvimento de protocolos de ação para casos como o analisado, visando maior proteção de seus dados, espaços e colaboradores é fundamental para evitar e prevenir possíveis danos.

Sendo assim, espera-se que este estudo de caso consiga chamar a atenção das empresas para o risco envolvido no trato de informações internas e a capacidade de dano possível em um tipo de situação como a aqui exemplificada. É completamente tangível o vazamento de informações sigilosas e, consequentemente, bastante alta a chance de que um ataque consiga gerar prejuízo financeiro à empresa demostrando que possíveis gastos com segurança e treinamento de pessoal seriam, na verdade, investimento.

O elemento humano mostra-se, ainda, mesmo em tempos de alta conectividade e interação digital, uma das maiores armas passíveis de serem aplicadas contra pessoas ou empresas. Cada vez mais, torna-se necessária a

preparação de funcionários para a defesa a ataques. Se os departamentos técnicos devem sim continuar a agir digitalmente através das ferramentas de proteção já conhecidas, os usuários devem aprender a se resguardar de possíveis situações de risco, seja através do questionamento ou da atenção a procedimentos de ataques de engenharia social.

Cabe, assim, às corporações disponibilizar condições técnicas e físicas para a aplicação de boas práticas de segurança, mas, acima de tudo, valorizar e incentivar a adoção de boas práticas e de protocolos mais rígidos de segurança por parte de seus colaboradores, sejam elas em ambiente corporativo e ou pessoal a fim de controlar, da melhor forma possível, o fator mais fraco da segurança da informação: o humano.

## REFERÊNCIAS

FERREIRA, Aurélio Buarque de Holanda Ferreira. **MINIDICIONÁRIO AURÉLIO**. 1985. 1ª ed. Editora Nova Fronteira.

FONSECA, Marcelo. **Engenharia Social, o Elo Mais Fraco da Segurança da Informação.** 2011. Monografia (Especialização em Gestão de Segurança Pública). Disponível em https://riuni.unisul.br/bitstream/handle/12345/2402/TCC_versao_final_1.pdf?sequence=1&isAllowed=y

FREITAS, Danilo Arantes de. **ENGENHARIA SOCIAL APLICADA NAS REDES SOCIAIS**. 2017. Trabalho de Conclusão de Curso. Disponível em https://www.passeidireto.com/arquivo/37524509/engenharia-social-nas-redes-sociais---phishing-na-pratica

FREITAS, Wesley R S. e JABBOUR, Charbel J. C. **UTILIZANDO ESTUDO DE CASO(S) COMO ESTRATÉGIA DE PESQUISA QUALITATIVA: BOAS PRÁTICAS E SUGESTÕES**. 2011. Artigo. Disponível em https://www3.ufpe.br/moinhojuridico/images/ppgd/8.12a%20estudo%20de%20caso.pdf.

MANN, Ian. **Engenharia Social**. São Paulo: Blucher, 2011. p. 10

MARCIANO, João Luiz Pereira. **Segurança da Informação – uma abordagem social**. 2006. Monografia. Disponível em http://repositorio.unb.br/bitstream/10482/1943/1/Jo%C3%A3o%20Luiz%20Pereira%20Marciano.pdf

MITNICK, Kevin D; Simon, William L. **A Arte de Enganar**. São Paulo: Blucher, 2003. p. 25

OLIVEIRA, Guilherme Legal de. **O Impacto da Engenharia Social em Uma Coporação**. 2017. Artigo. Disponível em https://www.riuni.unisul.br/bitstream/handle/12345/3037/GUILHERME_LEGAL_DE_OLIVEIRA.pdf?sequence=1&isAllowed=y

PATTON, M. G. **Qualitative Research and Evaluation Methods**, 3 ed. Thousand Oaks, CA: Sage, 2002

SANTOS, Daniel Pitanga dos. **A Engenharia Social no Brasil e Seus Riscos**. 2016. Monografia (Especialização).