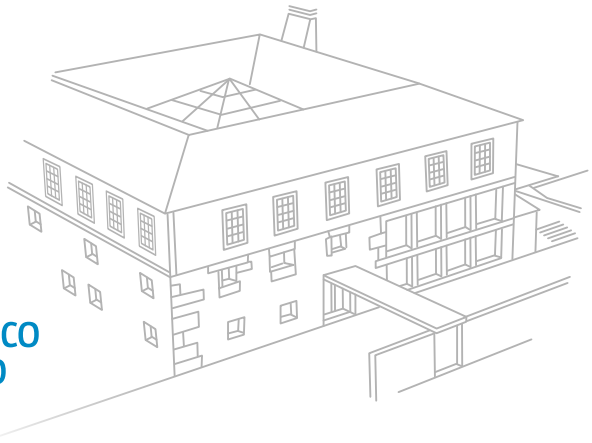


ESTGF | POLITÉCNICO DO PORTO

ESCOLA SUPERIOR DE TECNOLOGIA E GESTÃO

Análise comportamental sobre ataques de engenharia social

DESIGNAÇÃO DO MESTRADO Mestrado em Engenharia Informática

AUTOR Jana Eça Hohlenwerger Muniz Gaspar

ORIENTADOR(ES) Professor Doutor João Paulo Magalhães

ANO 2015

“The social engineer anticipates suspicion and resistance, and he’s always prepared to turn distrust into trust.”

Kevin Mitnick

Agradecimentos

A realização deste trabalho contou com importantes apoios e incentivos sem os quais não se teria tornado uma realidade e aos quais estarei sempre grata.

Ao Professor João Paulo Magalhães, pela sua orientação, pelos ensinamentos, pela pertinência das suas críticas e sugestões, e compromisso ao longo deste projeto.

A Professora Doutora Dorabela Gamboa pela atenção e disponibilidade.

Ao meu marido Jorge Gaspar pelo apoio incondicional, pela paciência, incentivo e por ter acreditado em mim.

Resumo

A engenharia social é utilizada para obter informações confidenciais ou acessos não autorizados a sistemas através de métodos que se baseiam nas relações humanas. É uma forma de ataque que tem vindo a ganhar expressão e a capturar a atenção entre as comunidades académica e empresarial.

Este trabalho aborda a engenharia social, tendo como foco, o lado humano da segurança informática. Em concreto este trabalho analisa o comportamento dos seres humanos perante dois cenários que estão de certa forma interligados entre si. O primeiro cenário envolve a utilização de perfis de redes sociais, aos quais as pessoas podem associar-se voluntariamente. O segundo envolve o registo voluntário das pessoas para a subscrição de notícias relacionadas com a área da saúde e bem-estar. O primeiro cenário tem por objetivo analisar a forma como as pessoas se relacionam e partilham dados com desconhecidos. Este cenário é utilizado para criar uma identidade virtual para a execução do segundo cenário. O segundo cenário analisa a predisposição das pessoas para divulgarem dados pessoais num sistema, ainda que, alertados sobre os termos e condições da sua subscrição no *site*. Os resultados obtidos pelo estudo são pertinentes na medida em que permitem compreender comportamentos humanos em função da idade e gênero, e possibilitam o planeamento de estratégias para colmatar falhas nos humanos, contribuindo para o aumento da proteção da informação.

Palavras-chave: Engenharia Social, Segurança da Informação, Ataques informáticos, Consciencialização.

Abstract

Social Engineering is used to gather classified information or unauthorized access to systems through methods based on human relations. It is a form of attack that has achieved growing relevance and captures the attention on the academic and business communities.

This work addresses the Social Engineering by considering the human side of the computer security. It provides an evaluation of the human behavior considering two different scenarios, which are somehow interconnected. The first scenario involves the usage of social network profiles that people can join voluntarily. The second scenario involves the analysis about how available is people reveal sensitive information through a simple subscription form related with to health and welfare news. The first scenario aims to analyze the way which people get related to and share information with strangers. This scenario is helpful to build a digital curriculum and engage people for the second scenario. The second scenario allows the analysis of people's predisposition in sharing personal data in a system, although being warned about the terms and conditions of their subscription in the site. The results achieved are very valuable, since it allows understanding the human behavior considering the age and gendering and also allowing the developing of strategies to mitigate the human vulnerabilities towards the data protection.

Key-words: Social Engineering, Information Security, Cyber-Attacks, Security Awareness.

Índice

Agradecimentos ii

Resumo iii

Abstract iv

Índice de Figuras vii

Índice de Tabelas x

Índice de Acrónimos xi

1. Introdução 1

1.1. Organização do Trabalho 5

2. A segurança informática e a engenharia social 6

2.1. A informação e a importância da sua segurança 6

2.1.1. Tipos de vulnerabilidades 7

2.2. A engenharia social 8

2.2.1. O engenheiro social 9

2.3. Ataques de engenharia social 12

2.3.1. Estrutura do ataque de engenharia social 13

2.4. Impacto dos ataques de engenharia social 20

2.4.1. O que é feito para mitigar estes ataques 22

3. Preparação e estratégia do processo de “engenharia social” 27

3.1. Metodologia de análise 28

3.1.1. Cenário 1 – Utilização de perfis em redes sociais 29

3.1.2. Cenário 2 – Site de notícias relacionadas com a saúde e o bem-estar 34

3.2. Conclusão do capítulo 41

4. Análise comportamental sobre ataques de engenharia social – Análise de resultados 43

4.1. Resultados do cenário 1: Construção de um perfil social para aproximação aos potenciais alvos de um engenheiro social 43

4.1.1. Número de pessoas que aderiram aos perfis 43

4.1.2. A evolução da construção do perfil social 51

4.2. Resultados do cenário 2: Recolha de dados pessoais por parte do engenheiro social 53
4.2.1. Adesão ao Blogue Pura Saúde 53
4.2.2. Dados obtidos a partir do cenário 2 57
4.3. Valor referencial dos dados recolhidos no *site* 63
4.4. Análise sobre os resultados obtidos 67
5. Conclusão 71
5.1. Trabalho futuro 73
6. Bibliografia 74

Índice de Figuras

Figura 1 - Número de utilizadores de Internet (número do ano são referentes a 1 de julho).. 1

Figura 2 - Mapa de clientes do site Ashley Madison [4] 2

Figura 3 - Pilares da segurança da informação 7

Figura 4 - Estrutura do modelo de ataque de engenharia social 14

Figura 5 - Ameaças mais comuns - Check Point 21

Figura 6 - Perfil de Luana Sampaio 29

Figura 7 - Publicações do perfil de Luana Sampaio.....30

Figura 8 - Perfil de Daniel Coelho.....30

Figura 9 - Publicações do perfil de Daniel Coelho 31

Figura 10 - Perfil de Nuno Ferreira 32

Figura 11 - Publicações do perfil de Nuno Ferreira.....32

Figura 12 - Perfil de Sandra Moniz 33

Figura 13 - Publicações do perfil de Sandra Moniz.....33

Figura 14 - Cabeçalho do Blog Pura Saúde 34

Figura 15 - Dica da semana e botão de subscrição do blogue 35

Figura 16 - Carrossel de notícias do Blog Pura Saúde 35

Figura 17 - Rodapé do Blog Pura Saúde.....35

Figura 18 - Página principal do Blog Pura Saúde 36

Figura 19 - Formulário de registo para a subscrição de notícias.....38

Figura 20 - Login da conta Google 39

Figura 21 - Login conta Facebook 40

Figura 22 - Página 1 dos Termos e condições de utilização da subscrição da newsletter 40

Figura 23 - Página 2 dos Termos e condições de utilização da newsletter 41

Figura 24 - Página 3 dos Termos e condições de utilização da subscrição da newsletter 41

Figura 25 - Número de pessoas que aderiram aos perfis na rede social 44

Figura 26 - Total de adesões e percentagem de cada perfil 45

Figura 27 - Pedidos enviados e recebidos.....46

Figura 28 - Evolução da adesão por semana 47

Figura 29 - Percentual de adesões por género de perfil 48

Figura 30 - Divisão por perfil e género.....49

Figura 31 - Adesão por faixa etária e género.....50

Figura 32 - Adesão por faixa etária 50

Figura 33 - Interação com os perfis da rede social 52

Figura 34 - Divulgação do Blogue através do perfil de Daniel Coelho 53

Figura 35 - Número total de adesões e de cada género 54

Figura 36 - Subscritores por distrito.....55

Figura 37 - Subscrição por faixa etária 56

Figura 38 - Subscrição por faixa etária e género 57

Figura 39 - Número de preenchimento dos campos no formulário de subscrição.....58

Figura 40 - Percentagem do preenchimento dos campos email e password na subscrição .59

Figura 41 - Percentual por género do preenchimento das credenciais 60

Figura 42 - Percentual por faixa etária e género do preenchimento das credenciais na subscrição.....61

Figura 43 - Percentual de credenciais válidas 62

Figura 44 - Percentagem de credenciais válidas por género 62

Figura 45 - Credenciais válidas por faixa etária e género 63

Figura 46 - Calculadora de dados 64

Figura 47 - Valor da informação no mercado negro por país 66

Figura 48 - Comparação entre o relatório do FBI e IC3 e os resultados obtidos no âmbito do estudo 68

Figura 49 - Comparação entre o estudo e o Report do IC3/FBI por faixa etária 69

Figura 50 - Percentagem dos campos email e password preenchidos e validados 70

Índice de Tabelas

Tabela 1 - Cálculo do valor dos dados recolhidos 65

Índice de Acrónimos

PNL – Programação Neurolinguística

FBI – Federal Bureau of Investigation

IC3 - Internet Crime Complaint Center

1. Introdução

Ao longo dos últimos anos temos assistido a um crescimento no número de utilizadores com acesso à Internet, na quantidade de informação acedida e partilhada e ainda na duração de tempo que permanecem ligados. De acordo com os números do internet live stats reports[1] e tal como nos mostra a Figura 1, atualmente existem 3.2 biliões de pessoas ligadas à Internet, o que representa aproximadamente 45% da população mundial. Em 1995 havia apenas 1% de pessoas ligadas à internet. Em 2005 foi atingido o 1º bilião de pessoas e em 2010 o segundo bilião. O 3º bilião foi atingido em 2014.

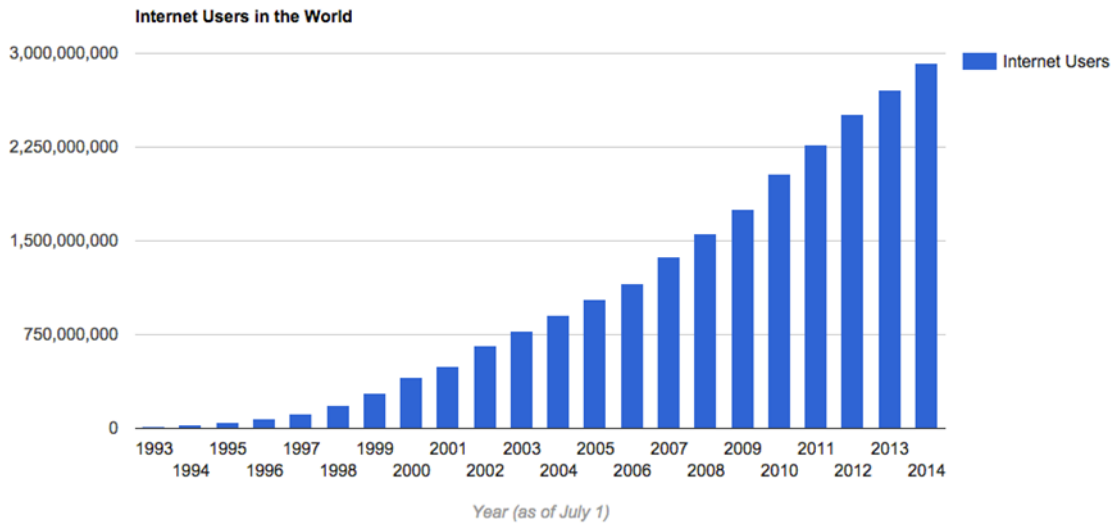


Figura 1 - Número de utilizadores de Internet (número do ano são referentes a 1 de julho)

Um fenómeno que ultimamente tem contribuído para o crescimento da utilização da Internet é a mobilidade. A evolução do número e tipos de dispositivos móveis (*laptops*, *tablets*, *smartphones*) com capacidade de ligação à Internet aumentou significativamente. É ainda esperado que este número cresça à medida que o número de "coisas" ligadas à Internet aumente (IoT – Internet-of-Things).

Não é nada de novo referir que com a evolução da Internet todos ganham. As empresas encontram novas formas de fazer negócios e aproximar-se dos seus clientes. Surgem novos negócios baseados no *online*. As pessoas consomem bens e serviços de forma mais facilitada, contribuem com conhecimento e ainda socializam com outros independentemente das distâncias físicas que possam existir. O que não é tão desejável é que, neste mundo *online* em que todos ganham, também existem movimentos *underground* nos quais circula muito dinheiro e informação relevante. Estes movimentos têm infelizmente evoluído em

números, eficácia e impacto das suas atividades. Aos movimentos *underground* referimo-nos em concreto a atos de ciberataque tais como:

- roubos monetários normalmente designados por cibercrime;
- roubo de informação sensível normalmente designado por ciberespionagem;
- roubo de segredos militares ou ataques a infraestruturas críticas designando-se normalmente por atos de ciberguerra;
- *hacktivismo*, isto é, a execução de causas ativistas através de ataques informáticos.

Ao longo dos últimos meses assistimos a um acréscimo de notícias relacionadas com ciberataques. Um caso recente tem a ver com o roubo dos guiões de filmes afetando a Sony Pictures. Este caso, reportado na comunicação social [2], levou o governo norte-americano a afirmar em público que tais ataques são intoleráveis, atribuindo os mesmos à Coreia do Norte, e levantando sanções em virtude de tais ocorrências. Outro exemplo também recente, foi o ataque ao *site* Ashley Madison, que pertence à empresa canadiana Avid Life Media [3]. Trata-se de um *site* de encontros amorosos com enfoque em encontros extraconjugais que sofreu um ataque que expôs os dados dos seus clientes. Esta empresa após ter sofrido o ataque, veio a público pedir desculpas aos mais de 37 milhões de clientes espalhados pelo mundo, como nos mostra a Figura **2**, alertando que estes podem vir a ter os seus dados pessoais, como por exemplo, nome, morada e número do cartão de crédito divulgados publicamente. De acordo com o responsável da empresa poderá tratar-se de um ataque interno por parte de alguém que conhecia bem a empresa e que, pelo menos uma vez, teve acesso à base de dados.

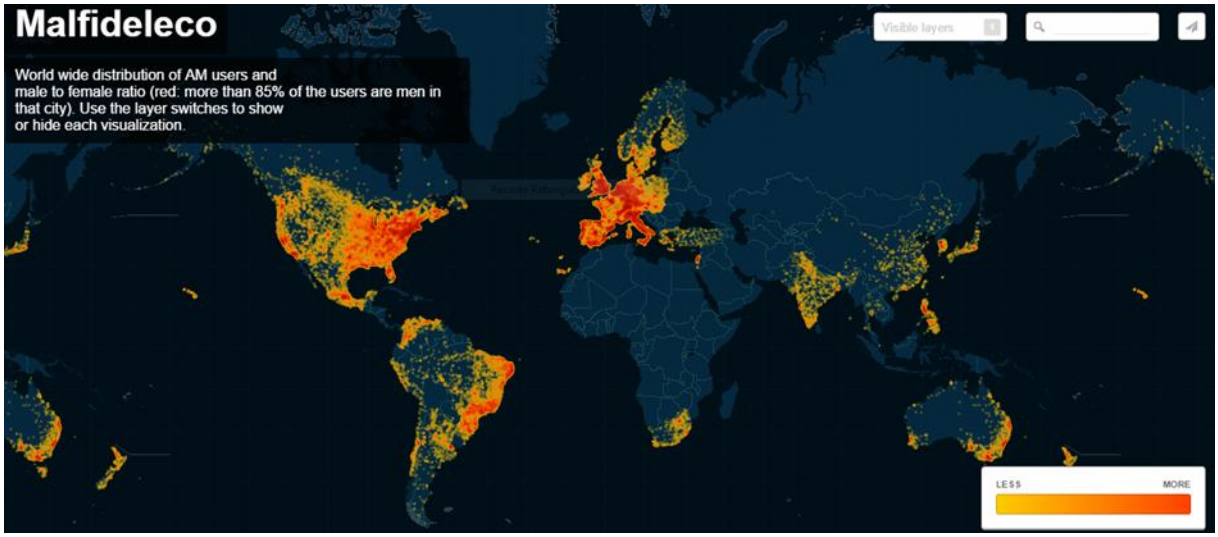


Figura 2 - Mapa de clientes do site Ashley Madison [4]

Outro ciberataque muito emblemático foi o Carbanak. O Carbanak [5] é considerado o maior ataque cibercriminoso da história, tendo resultado num roubo de 1 bilião de dólares a 100 bancos mundiais. Este ataque começou pela descoberta de endereços de correio eletrónico de funcionários dos bancos, seguindo-se o envio de *emails* aos mesmos que eram à primeira vista emails autênticos. Estes *emails* continham ligações para software malicioso que uma vez descarregado e instalado permitiu aos criminosos aceder aos computadores internos do banco. Bastou um dos funcionários do banco abrir o *email* para comprometer toda a instituição.

Nós assistimos ao longo do tempo ao reforço tecnológico das empresas com tecnologias de proteção contra ataques: *firewalls*, sistemas de deteção de intrusão, sistemas de autenticação, entre outros. No entanto, estes exemplos mostram que apesar das melhorias nos dispositivos tecnológicos para deteção e combate às ameaças de segurança, a sua adoção não é suficiente para conter ciberataques avançados. Um atacante conhece bem os sistemas atuais e explora meios alternativos que lhe permitem executar as ações por si planeadas. Um dos meios alternativos com maior sucesso está relacionado com o comportamento humano, sendo amplamente explorado por meio de um processo designado por engenharia social.

A engenharia social tira partido das vulnerabilidades humanas para executar um ciberataque. É uma forma de ataque que tem vindo a ganhar expressão e a capturar a atenção entre as comunidades académica e empresarial. Tal como referido em [6] a engenharia social é muito utilizada pelos atacantes para obter informações confidenciais ou acessos não autorizados a sistemas, através de métodos que se baseiam nas relações humanas.

Um facto particularmente interessante no ataque de engenharia social é que este depende da colaboração dos utilizadores e a possibilidade do seu sucesso depende do nível da capacidade da vítima em conseguir identificar a ameaça. Daqui se retira que quão mais conscientes estiverem as pessoas para a ciber segurança, mais difícil será um atacante tirar partido das pessoas para levar a cabo os seus ataques. Por parte das organizações este problema é reconhecido, sendo o lado humano referido como o “elo mais fraco”, no entanto verifica-se que a parte técnica da segurança de sistemas continua a ser o foco principal, havendo ainda muito por fazer no que diz respeito à componente humana.

O trabalho aqui apresentado aborda o lado humano da segurança informática. Em concreto, foca a questão da engenharia social, propondo uma análise do comportamento das pessoas perante dois cenários de teste e dos impactos que estes cenários podem ter para si próprias ou para as organizações que representam.

O primeiro cenário em estudo envolve a utilização de perfis de redes sociais, aos quais as pessoas podem associar-se voluntariamente. As redes sociais são um ambiente perfeito para que os engenheiros sociais identifiquem pessoas, as analisem por forma a perceber os seus comportamentos, podendo identificar em muitos casos, os locais que frequentam, incluindo o local de residência e o local de trabalho. Permite ainda perceber quem são as suas amizades, potenciando a personificação para obtenção de dados ou informações relevantes para um ataque que se esteja a desenhar. No âmbito deste trabalho, através deste cenário pretende-se avaliar como as pessoas se relacionam com terceiros. Serão consideradas, diferentes faixas etárias e o género para analisar quais os grupos mais predispostos a contatar com desconhecidos. O cenário é desenvolvido ao longo de algum tempo, permitindo auferir a confiança e aceitação de opiniões de um desconhecido. De forma mais específica este cenário permitirá medir o comportamento das pessoas em redes sociais, nomeadamente:

- a percentagem e rapidez com que as pessoas de diferentes classes etárias e organizados por sexo se relacionam e trocam dados com desconhecidos;
- a evolução da confiança criada para com o novo amigo, medida ao longo do tempo.

O segundo cenário tira partido do trabalho realizado ao longo do primeiro cenário, podendo no entanto alargar-se a um público mais vasto e diferente. Este cenário visa auferir o tipo de informações que as pessoas fornecem de forma voluntária a terceiros, incluindo dados sensíveis que põe em causa a possibilidade de acesso a informações relevantes. De forma específica este cenário analisará:

- a quantidade de pessoas que fornecem voluntariamente dados pessoais organizadas por classe etária e por sexo;
- a quantidade de pessoas que fornecem credenciais de acesso, sendo estas organizadas por classe etária e por sexo.

É de referir que o estudo não pretende tirar qualquer vantagem dos dados fornecidos pelas pessoas. Os dados recolhidos são imediatamente analisados, não sendo feito qualquer tipo de armazenamento dos dados pessoais em bases de dados. São armazenados apenas resultados que permitem uma análise estatística e comparativa dos dados fornecidos. Sobre os dados solicitados está subjacente uma lista de termos e condições que diz de forma clara que os dados pessoais recolhidos não serão cedidos a terceiros, podendo no entanto ser utilizados para fins de estudos sobre a utilização segura da Internet.

Os resultados deste estudo podem ser utilizados em diferentes contextos. O estudo, considerando os dois cenários em análise:

- ajudará a perceber de uma perspetiva prática as facilidades/dificuldades encontradas por um engenheiro social na identificação de alvos;
- ajudará a conhecer o nível de consciencialização das pessoas sobre os perigos da internet;
- permitirá a identificação de contra medidas adequadas para mitigar os riscos e manter o controlo das informações;
- facilitará a definição de programas de educação e treino específicos, tendo em consideração as vulnerabilidades dos públicos-alvo.

O nível de consciencialização das pessoas é fundamental para travar os ataques informáticos por via de engenharia social. Este trabalho ao estudar comportamentos de pessoas organizadas por faixas etárias e sexo e deduzir padrões de comportamento permitirá conhecer melhor a situação atual e a partir desta planear ações dirigidas que permitam mitigar os problemas encontrados.

1.1. Organização do Trabalho

Este trabalho está organizado da seguinte forma:

- No capítulo dois é apresentada a fundamentação teórica deste trabalho, realçando-se a importância da segurança da informação e os desafios que a engenharia social impõe para a proteção efetiva da informação.
- O capítulo três descreve os objetivos do presente trabalho considerando a análise comportamental sobre ataques de engenharia social, e apresenta também as metodologias utilizadas para este estudo.
- O capítulo quatro apresenta os resultados obtidos com o estudo.
- No quinto capítulo é feita a conclusão do trabalho.

2. A segurança informática e a engenharia social

Este capítulo apresenta uma revisão da bibliografia existente sobre a Engenharia Social, demonstrando como ela está presente no nosso dia-a-dia. Ao longo do capítulo é referida a importância da segurança de informação, os tipos de vulnerabilidades, destacando as vulnerabilidades associadas ao fator humano. As táticas e fatores psicológicos, bem como os motivos que levam o engenheiro social a realizar este tipo de ataque, são apresentados neste capítulo. São ainda apresentados exemplos conhecidos de ataques de engenharia social, a sua estrutura, os seus impactos e o que tem sido feito para os mitigar.

2.1. A informação e a importância da sua segurança

Segundo Peixoto em [7], o desenvolvimento económico das organizações depende de sistemas e infraestruturas de tecnologia da informação que devem ter alta disponibilidade, ser tolerante a falhas e proporcionar acesso a dados de forma integra. De acordo com o autor "*a informação representa a inteligência competitiva dos negócios e é reconhecida como ativo crítico para a continuidade operacional da empresa*".

Com a disseminação da utilização dos sistemas de informação e a sua conectividade a outras redes, incluindo a Internet, os sistemas encontram-se mais expostos do que nunca a ameaças de segurança. Os ataques estão a acontecer com mais frequência e têm-se tornado mais efetivos, mais criativos e mais complexos de detetar e atenuar, prejudicando diretamente o negócio das empresas. Tal leva a constatar que a segurança da informação deve ser considerada como um requisito essencial para a continuidade de qualquer organização no mercado. Esta ideia é reforçada pela Unisys em [8], ao afirmar-se a importância da segurança da informação e a sua prioridade, especialmente no ambiente de ameaças constantes, por forma a mitigar o impacto que uma pequena falha na segurança pode trazer para uma organização.

Ainda segundo Peixoto [7], "*O termo segurança da informação pode ser designado como uma área do conhecimento que salvaguarda os ativos da informação, contra acessos indevidos, modificações não autorizadas ou até mesmo sua não disponibilidade*".

A Segurança da Informação, numa definição mais abrangente, consiste na preservação da informação durante o seu ciclo de vida: origem, armazenamento, uso e transporte. Em cada uma destas fases, e tal como ilustrado na Figura 3, devem ser garantidos três princípios base [9]:

- **Confidencialidade:** garantia de que a informação é acedida apenas pelas pessoas que têm autorização para tal;
- **Integridade:** salvaguarda a exatidão da informação ao longo do seu ciclo de vida;
- **Disponibilidade:** garantia de que os utilizadores autorizados tenham acesso à informação de forma confiável e integra sempre que necessário.

Figura 3 - Pilares da segurança da informação

A falha de qualquer um dos três princípios base terá diferentes impactos consoante o valor da informação para a organização. A perda de confiança nos serviços e/ou até mesmo prejuízos financeiros e de reputação são exemplos de impactos gerais.

2.1.1. Tipos de vulnerabilidades

Do ponto de vista da segurança da informação, uma vulnerabilidade pode ser definida como um ponto passível de falha, ou seja, um elemento que pode ser explorado a qualquer momento por alguma ameaça, permitindo a um atacante obter acesso não autorizado. Este elemento pode ser um equipamento, uma instalação física, um software ou, ainda, um humano.

De acordo com Alves [10], as vulnerabilidades podem ser:

- **Físicas:** local (prédio, sala) onde se encontra a infra-estrutura dos sistemas. Deve-se escolher locais de forma a prevenir acidentes naturais, e a sua estrutura deve respeitar os padrões exigidos para a correta proteção do espaço;
- **Naturais:** tempestades, terremotos, inundações, incêndios são alguns exemplos de vulnerabilidades naturais. A prevenção contra estas vulnerabilidades é extremamente importante, principalmente em países onde estes acontecimentos são mais propensos. A falta de energia, poeiras, a humidade e a temperatura também podem provocar danos no sistema;
- **Hardware:** desgaste do equipamento, obsolescência, má utilização e avarias;
- **Software:** má instalação ou configuração, falhas ao nível da implementação, incompatibilidade entre hardware e software são causas comuns de vulnerabilidade que ao ser exploradas podem provocar o extravio de dados ou levar à indisponibilidade dos sistemas;
- **Mídias:** podem ser perdidos ou danificados. Como são tipicamente pequenos e fáceis de transportar podem ser roubados;
- **Comunicação:** perda de comunicação, acessos não autorizados à rede ou mesmo a máquinas. Deve-se ter o controlo de todas as máquinas que estão na rede e das suas comunicações para se evitar o roubo de dados;
- **Humana:** técnicas de engenharia social que se aproveitam das vulnerabilidades referentes ao fator humano.

O trabalho apresentado nesta tese foca as vulnerabilidades humanas, nomeadamente o nível de consciência por parte das pessoas no que diz respeito ao relacionamento com desconhecidos e na predisposição para partilhar informação genérica e informação sensível. Na próxima seção aborda-se a engenharia social no contexto da exploração de vulnerabilidades encontradas nos humanos e que podem comprometer toda uma estratégia de segurança de informação.

2.2. A engenharia social

As ameaças à segurança de informação levaram as empresas a adotarem medidas para reforçar a segurança dos seus sistemas, tornando-os mais eficazes no bloqueio de ameaças externas, dificultando assim, o acesso indevido. Atualmente, em geral, as organizações estão conscientes dos ataques informáticos e dispõem de tecnologias para tornar as suas infraestruturas mais protegidas. Sistemas de *firewall*, sistemas de deteção e controlo de

intrusão, auditorias de segurança regulares aos sistemas, rede e aplicações são bons exemplos deste reforço. No entanto, essa barreira tecnológica adotada pelas organizações levou a uma mudança de estratégia por parte dos atacantes, que agora, passaram a explorar as fragilidades do lado humano da segurança informática. Estas fragilidades exploram a utilização de variados elementos sociais e humanos para intrusão nos sistemas, roubo de informação relevante ou para afetar a sua reputação ou produtividade das empresas. Estes ataques acabam por ser feitos por pessoas de dentro, podendo ainda ser divididos em ataques voluntários ou involuntários. São voluntários quando a pessoa tem plena consciência do ataque e involuntários quando sem se aperceber estão a lesar a empresa/organização onde estão inseridos.

No "Global Security Index Report" [11], a IBM identifica uma tendência crescente para ataques mais focados em detrimento de ataques em massa tais como vírus ou SPAM. Num outro no relatório de 2006 designado de "Stopping Insider Attacks" [12], a IBM sugere que a prioridade dada aos ataques externos em detrimento dos ataques internos está errada e que esse facto está a permitir aos *hackers* explorar as fragilidades na estratégia de segurança das organizações. A Engenharia Social, pela sua simplicidade e engenho, é a forma mais fácil e eficaz de tornear os obstáculos que os sistemas de segurança impõem.

De acordo com Berti e Rogers [13], a engenharia social engloba "as tentativas bem-sucedidas ou fracassadas para influenciar uma pessoa a revelar qualquer informação ou agir de uma forma que possa resultar em acesso não autorizado, uso não autorizado de, ou divulgação não autorizada de um sistema de informação, de uma rede ou de dados".

O atacante, também denominado de *hacker*[1], ou engenheiro social, analisa o perfil da sua vítima, identifica e utiliza as mais diversas estratégias para seduzi-la e manipulá-la, para que esta disponibilize informações ou realize as ações que deseje.

Este tipo de ataque tem vindo a crescer. O aumento do uso das redes sociais e a falta de consciência dos utilizadores potenciam estes ataques. Neste sentido, as organizações precisam se preocupar mais com a conscientização e controlo dos funcionários.

2.2.1. O engenheiro social

Kevin Mitnick é conhecido por muitos como o maior *hacker* da história. A sua maior arma foi a engenharia social.

[1] O Hacker utiliza o computador para obter dados não autorizados. [14] O. Dictionaries. "Hacker". Internet: http://www.oxforddictionaries.com/definition/english/hacker. [Fev, 2015].

Segundo Kevin Mitnick [15], um Engenheiro Social é uma pessoa que manipula a confiança de outra para ter acessos a informações consideradas privadas. Ele também pode, por meio das poucas informações a que tem acesso, montar um cenário mais aprofundado sobre um alvo. Sem que o indivíduo saiba, as informações que ele considera irrelevantes dão ao engenheiro social a possibilidade de prejudicá-lo empresarialmente, socialmente, financeiramente ou psicologicamente. [16]

Segundo Eduardo Araújo [17], "*geralmente o engenheiro social é um tipo de pessoa agradável. Ou seja, uma pessoa educada, simpática, carismática. Mas, sobretudo criativa, flexível e dinâmica. Possuindo uma conversa bastante envolvente*".

Um exemplo da criatividade utilizada pelos engenheiros sociais é a utilização de programação neurolinguística (PNL). Neste âmbito foi inclusive criado um *framework* com o objetivo de estudar a maneira de como os seres humanos pensam e experimentam o mundo. Tal como apresentado por Hadnagy [18], os engenheiros sociais fazem uso deste *framework* para descobrir como devem usar a voz, que tipo de linguagem devem utilizar e ainda quais palavras deve escolher com o intuito de orientar as pessoas a fazerem o que desejam.

Zager [19] identifica quatro tipos de engenheiros sociais. Esta identificação é feita com base nos motivos do engenheiro social:

- **Engenheiro social Casual:** formam o maior grupo e são motivados pela curiosidade e pelo desafio de entrar no sistema
- **Engenheiro social Político:** agem por uma causa e também são chamados ativistas cibernéticos. Fazem uso de suas habilidades para divulgarem a sua causa ou atacarem organizações que representam interesses contra a sua causa;
- **(Organizado) criminoso:** composto por criminosos profissionais;
- **Agente Interno:** incluem funcionários de uma organização, bem como terceiros de confiança, como consultores externos e fornecedores. Podem causar grandes danos por causa do seu lugar na organização.

Na maioria das vezes, a vítima nem imagina que foi usada e muito menos que acabou de abrir caminho para um invasor. O sucesso de um ataque de engenharia social requer bastante paciência e persistência e essa é uma das grandes características dos engenheiros sociais.

2.2.1.1. A vítima e as suas vulnerabilidades

Como referido anteriormente, o fator humano é um dos maiores problemas na segurança da informação, sendo por isso, uma das principais causas de invasão e ataque. O Engenheiro

Social aproveita-se de algumas características inerentes à maioria dos seres humanos. Em [20] são apontadas características como solidariedade, ambição, curiosidade para aproximar-se do seu alvo, procurando conquistar a sua confiança, e com isso alcançar os seus objetivos.

De acordo com Corrêa [21] destacam-se ainda características do ser humano que o tornam vulnerável e suscetível a ataques de engenharia social:

- **Sentir-se útil para outras pessoas**: ser cortês ou ajudar quando necessário;
- **Encontrar novas amizades**: as pessoas sentem-se bem quando elogiadas, tornando-se mais abertas e vulneráveis a fornecer informações;
- **Obter lucro fácil**: quando existe a promessa de ganho fácil, as pessoas aceitam correr riscos e ficam mais suscetíveis a ceder informações;
- **Ser admirada e respeitada**;
- **Ser considerada com uma pessoa culta em determinados assuntos**;

Conhecendo essas fragilidades da natureza humana, os engenheiros sociais utilizam várias táticas que exploram não apenas, os aspetos físicos como também, os aspetos psicológicos do seu alvo. Essas táticas serão abordadas posteriormente.

2.2.1.2. Objetivos do engenheiro social

Considerando que os ataques de engenharia social são cada vez mais comuns, devido principalmente, a propagação da Internet e das redes sociais, o ato de manipular vítimas, é para os engenheiros sociais, uma atividade comum. Os principais motivos dos seus ataques, segundo Lafrance [22], são:

- **O ganho financeiro:** o foco do engenheiro social é o lucro. Este é considerado um dos principais motivos e o alvo será sempre prejudicado;
- **O interesse pessoal:** basicamente fazem o ataque por diversão ou curiosidade. Focam-se no acesso, alteração e remoção de informações. Apesar de não agirem com intenções maliciosas podem provocar grandes danos;
- **Desafio intelectual:** o objetivo do atacante é provar que algo é possível. Nem sempre o engenheiro social tem más intenções neste tipo de ataque, na maioria das vezes, trata-se de um desafio pessoal;
- **Vantagem competitiva:** espionar informações confidenciais que lhe tragam vantagem competitiva;
- **Pressão externa:** o engenheiro social sente a necessidade de demonstrar as suas habilidades com o objetivo de ser aceite num grupo, ou ainda para manter um certo

status. Essa pressão pode vir da família, amigos ou do grupo e é conseguida através da chantagem ou do retorno de um favor. As intenções variam de acordo com a pessoa ou grupo que impinge a pressão.

- **Contenção de danos**: o atacante deseja minimizar os danos causados por um ataque anterior, ou tentar ajudar pessoas ou organizações a corrigirem vulnerabilidades nos seus sistemas.
- **Político:** as causas deste tipo de ataque podem ser religiosas, políticas, ambientais e podem levar, ao terrorismo. O atacante deseja obter publicidade para sua causa.

Em resumo, independente do motivo que leva um engenheiro social a desempenhar um ataque, estes podem sempre provocar danos. Estes danos por menor que sejam, não devem ser desvalorizados. Pelo contrário, devem-se tomar medidas preventivas para evitá-los.

2.3. Ataques de engenharia social

Atualmente a engenharia social é muito utilizada para a obtenção de informações confidenciais e importantes. Os ataques de engenharia social não visam apenas as organizações, mas qualquer pessoa que seja do interesse do atacante. Estes ataques são também bastante difíceis de controlar, pois dependem do comportamento humano e do aproveitamento de funcionários vulneráveis.

De acordo com Alves [10], os ataques de engenharia social podem ser divididos em dois grupos: os diretos e os indiretos.

Os ataques diretos caracterizam-se pelo contacto pessoal entre o engenheiro social e a vítima, geralmente, através dos meios de comunicação, como por exemplo, o telefone, o fax, e também pessoalmente. Este tipo de ataque é o mais arriscado. Possui um alvo e requer do engenheiro social um planeamento detalhado e também experiência, pois precisa ser bastante claro no momento de interação com a vítima para que o seu plano não seja descoberto.

Para a realização de um ataque direto, o engenheiro social primeiro escolhe e aproxima-se do alvo, podendo ser uma pessoa do seu meio ou não, depois procura estudar a vítima, frequentando os mesmos lugares, observando-a, recolhendo o máximo de informações a seu respeito. Inicia o contacto de forma despretensiosa e subtil procurando ganhar aos poucos confiança e cumplicidade. Com o cenário criado, o ataque está pronto para ser executado. Um exemplo desse tipo de ataque é: um engenheiro social que telefona para uma organização fazendo-se passar por um técnico da área de segurança. Este diz ao funcionário que fará uma

atualização no sistema e que lhe passe as credenciais de acesso. O funcionário não quer atrapalhar o serviço de outro colega e cede-lhe as informações.

Os ataques indiretos caracterizam-se pela utilização de *softwares* ou ferramentas, como por exemplo, vírus, cavalos de tróia, ou através de sites e emails falsos para assim obter as informações desejadas. Na maioria das vezes, neste tipo de ataque, o alvo do engenheiro social não é o utilizador que recebeu o ataque, ele utilizará as informações extraídas da vítima para atingir uma entidade maior, que pode ser uma organização ou o governo.

O facto dos ataques indiretos serem, na maior parte das vezes, feitos através da Internet, são considerados menos arriscados que os diretos, pois, o engenheiro social não entra em contato com a vítima diretamente e também não possui um alvo definido. Um exemplo deste tipo de ataque são os *sites* falsos que oferecem algum tipo de prémio para os utilizadores. As pessoas para terem a possibilidade de ganhar um prémio deve preencher o formulário com seus dados pessoais. Este método é bastante utilizado pelos engenheiros sociais, primeiro criam os *sites* e depois utilizam as redes sociais para fazerem a divulgação dos mesmos.

2.3.1. Estrutura do ataque de engenharia social

Tal como referido, os ataques de engenharia social podem ocorrer de forma direta ou indireta. Entretanto, é preciso conhecer como funciona a elaboração de um ataque, em particular quais as etapas que o engenheiro social utiliza para o planeamento do seu ataque. Para isso, será abordado o modelo da estrutura do ataque de engenharia social, definido por Oosterloo [22]. A figura 4 ilustra o modelo distribuído em quatro fases: Preparação, Manipulação, Exploração e Execução.

Figura 4 - Estrutura do modelo de ataque de engenharia social

Cada ataque é único e o engenheiro social pode executar uma determinada fase mais que uma vez, se achar necessário, antes de seguir para a fase seguinte. Trata-se de um processo iterativo, ou seja, cada fase funciona como um ciclo que pode ser repetido sempre que for necessário e a passagem para a fase seguinte depende da obtenção do resultado esperado na fase atual. Em termos de fases temos:

- **Preparação:** a primeira fase consiste em toda a preparação antes do envolvimento do alvo, conhecido como *footprinting* Esta fase inclui a recolha de informações, e de outros atributos (físicos) necessários à próxima fase, por exemplo: a estrutura da organização, nomes de funcionários, funções dos funcionários, agenda, números de telefone internos, *email*, políticas e processos organizacionais, linguagem da organização, logótipos organizacionais, senhas, entre outras.
- **Manipulação:** Consiste em utilizar todos os meios para influenciar o alvo, para criar um ambiente credível e conquistar a confiança. A manipulação pode ser realizada fisicamente, com interação direta entre o engenheiro social e o alvo, ou através dos meios de comunicação, por exemplo, telefone, fax, *email*. Esta fase é utilizada para reunir informações.

- **Exploração:** é nesta fase que o engenheiro social faz uso da influência que possui sobre o alvo para obter mais informações. Ou seja, a confiança e influência conquistadas através da manipulação na fase anterior, são agora utilizadas para conseguir recolher informações mais específicas, por exemplo, nome dos servidores, nome de aplicações, endereços IP, manuais, entre outras.
- **Execução:** a fase de execução, como o nome diz, é a realização do ataque com a utilização de todas as informações e recursos obtidos nas fases anteriores. Consiste na sequência de ações para se chegar ao objetivo final. As táticas utilizadas pelo engenheiro social nesta fase têm um carácter técnico, mas são importantes porque demonstram a perícia do engenheiro social.

A duração de um ataque depende do seu nível de preparação, dificuldade e dimensão. O tempo gasto na fase de preparação é, na maioria das vezes, o maior, tornando-se a fase mais longa do ataque. Por outro lado, se esta fase for bem preparada e executada, encurtará o tempo gasto nas outras.

Em cada fase, são usadas táticas específicas para obter informações ou para manipular as pessoas a revelarem informações, para posteriormente, se chegar ao objetivo final do ataque. De acordo com Lafrance [23], a escolha da tática a ser utilizada durante um ataque ou durante apenas um ciclo, depende das habilidades e motivações do engenheiro social. Na próxima subsecção são apresentadas algumas das táticas utilizadas.

2.3.1.1. Táticas de ataque

As técnicas de ataque evoluem à medida que a engenharia social e os mecanismos de defesa evoluem. Contudo, e de forma geral um engenheiro social utiliza táticas como:

- **Reconhecimento/Estudo:** Esta tática é utilizada na fase de preparação, onde o engenheiro social estuda o alvo que pode ser um indivíduo ou uma organização. Ele observa, frequenta os mesmos locais, ouve conversas, e pode até seguir a vítima. A sua intenção é recolher informação útil e identificar as rotinas para utilizar posteriormente. Em [24], [25] e [26] é apresentada esta tática de forma mais exaustiva;
- **Pesquisa Web:** o engenheiro social utiliza os motores de pesquisa, grupos de notícias, *sites* de emprego, redes sociais, fóruns, entre outros, para recolher informações sobre o alvo;
- **Vasculhar o lixo:** Consiste na análise do lixo de uma organização para procurar informação potencialmente útil, que deveria ter sido descartada de forma segura. Como exemplo temos manuais, organograma, nome de funcionários, calendário com

anotações de reuniões, papel timbrado, formulários preenchidos, entre outros. Esta tática é descrita em [24] e [27]. Um aspeto importante desta tática tem a ver com o enquadramento legal. Como referido em [28], vasculhar o lixo é em determinados países uma ato ilegal. Em Portugal a proibição de remexer ou retirar qualquer objeto do lixo está prevista nos diversos regulamentos municipais ou de empresas quando são estas as entidades gestoras da recolha de resíduos sólidos urbanos. A lei fala apenas na proibição de danificar os equipamentos e recipientes, mas os regulamentos vão mais longe e em regra proíbem que se remexa no lixo.

- **Análise forense:** Semelhante à tática de vasculhar o lixo, só que nesta, o engenheiro social faz a busca em equipamentos de informática descartados ou avariados como discos rígidos e com o objetivo de reunir informações que deveriam ter sido removidas de forma permanente. Mais detalhes sobre esta técnica podem ser consultados em [24];
- **Phreaking**[2]**:** consiste na invasão do sistema de telefonia. Por exemplo, mudar o número de telefone mostrado no identificador de chamadas da vítima fazendo-se passar por outra pessoa ou fazer o reencaminhamento de chamadas para os engenheiros sociais. Esta tática é descrita em [29];
- **Phishing**[3]**:** Pode ser descrito como a tentativa de aceder, de forma ilegal, às informações pessoais. Normalmente é iniciada por correio eletrónico, chamadas telefónicas ou mensagens instantâneas, onde o atacante se faz passar por um colaborador legítimo ou uma pessoa/instituição credível. Por exemplo, a vítima recebe um *email* contendo um *link* que será redirecionado para um *site* falso;
- **Mail-outs:** similar ao *phishing*. Um exemplo é o envio de *emails* sob a forma de inquéritos. Estes são usados para recolher informações organizacionais e/ou pessoais e identificar as pessoas mais vulneráveis ao *phishing* e posteriormente fazer o envio de *software* malicioso. Esta tática é analisada em [26];
- **Profiling:** consiste na agregação de toda informação útil recolhida através de outras táticas para a personificação da vítima. Ou seja, a criação de um perfil do alvo escolhido utilizando por exemplo, linguagem própria ou rotinas pessoais. Este perfil será usado para revelar fraquezas ou criar guiões para manipular os diferentes alvos,

[2] Phreaking é o nome dado aos *crackers* de telefonia. Os Phreakers invadem sistemas de telefone para diversos fins, por exemplo, fazer chamadas telefónicas às custas de outro, roubar números de cartões de telefone. [22] B. Oosterloo, "Managing Social Engineering Risk," Master Industrial Engineering and Management, University of Twente, Enschede, Netherlands, 2008.

[3] Phishing é uma forma de fraude eletrónica caracterizada por tentativas de adquirir dados pessoais, através de email, SMS, entre outros. [30] Microsoft. "O que é o phishing?". Internet: https://www.microsoft.com/pt-pt/security/resources/phishing-whatis.aspx. [Fev, 2015].

utilizando os conhecimentos adquiridos. Em [31] e [32] são apresentadas táticas de *profiling*;

- **Physical impersonation**: esta tática é utilizada quando o engenheiro social precisa de entrar na organização ou qualquer outro local e nesse caso, tem que interagir com o alvo pessoalmente. Essa é uma tática bastante arriscada e, devido ao risco de ser exposto, apenas os engenheiros sociais experientes farão uso deste recurso;
- **Virtual impersonation**: ao contrário da *physical impersonation*, o engenheiro social prefere não correr riscos, e mantém uma certa distância do alvo, recorrendo a um meio de comunicação para a interação entre eles. Este meio pode ser um telefone, fax, *email*, entre outros. Apesar do risco de exposição ser menor, pode não ser tão eficaz como a interação pessoal na obtenção de informações. Em [27] é descrita esta tática.
- **Engenharia Social Inversa:** é quando o alvo vai ao encontro do engenheiro social e não o contrário. O engenheiro social cria um personagem, uma pessoa que parece estar ali para ajudar, ou seja, provocará uma situação em que o alvo pedirá a sua ajuda. Esta tática consiste em três etapas: a primeira é a sabotagem, onde o engenheiro social cria um problema no computador ou na rede do alvo. A segunda etapa é o marketing, onde oferece os seus serviços, evidenciando que é a pessoa indicada para resolver o problema. Por fim, a terceira etapa, assistência ou apoio. É nesta etapa que o engenheiro social informa que para conseguir resolver o problema, necessita de obter acesso ao sistema ou de algumas informações confidenciais. O alvo não desconfia de que se tratou de violação da segurança, pois o problema foi resolvido. Esta tática, quando bem planeada e executada permite obter mais facilmente informação importante sobre os alvos;
- **Roubo de identidade:** consiste na utilização de informações armazenadas através de outras táticas descritas anteriormente. Tem como finalidade a de se fazer passar por outra pessoa, física ou virtualmente. Esta tática é muito utilizada para adquirir credenciais de acessos e dados de cartão de crédito. O roubo de identidade é apresentado em [15] e [33] com maior detalhe;
- **Software malicioso**: são aplicações informáticas que recolhem informação sobre o comportamento do utilizador. Pode ser enviado de várias formas, por exemplo anexado a um *email* ou através de uma *pendrive*. Também pode ter vários formatos, como, um vírus, trojan[4], *keylogger*[5]. Estes *softwares* são normalmente instalados sem

[4] Os Trojans são programas maliciosos que executam ações não autorizadas pelo utilizador.[34] Kaspersky. "O que é um Trojan?". Internet: http://www.kaspersky.com/pt/internet-security-center/threats/trojans. [Oct, 2015].

[5] Keylogger é um termo usado para se referir a um dispositivo capaz de capturar as teclas digitadas no computador. [35] A. Rohr. "G1 Explica: o que é um keylogger?". Internet: http://g1.globo.com/tecnologia/blog/seguranca-digital/post/g1-explica-o-que-e-um-keylogger.html. [Oct, 2015].

o conhecimento do utilizador e atuam de forma silenciosa, isto é, sem sintomas de atividades que impeçam a sua fácil deteção e eliminação.

Além das táticas os engenheiros sociais tiram partido de fatores psicológicos para se aproximar dos alvos. Estes fatores são apresentados na próxima subsecção.

2.3.1.2. Fatores psicológicos ou táticas sociais

O sucesso do ataque de engenharia social depende da criação de um ambiente psicológico perfeito para o seu ataque. Para tal, o engenheiro social na sua aproximação ao alvo, explora fatores como a tranquilidade da vítima ou situações de urgência/emergência. Por exemplo, o engenheiro social faz-se passar por alguém do mesmo nível hierárquico ou superior, ou por cliente ou fornecedor, de modo a convencer o alvo a fornecer informações, executar algum programa ou até mesmo fornecer as credenciais de acesso.

Tal como referido em [6], quando se refere a um ataque de engenharia social, refere-se sobretudo as habilidades psicológicas requeridas por parte do engenheiro social, ganhando estas maior destaque do que as habilidades tecnológicas. Em Mitnick [15] esta situação é referida várias vezes.

De acordo com Gragg [36], alguns dos fatores psicológicos explorados pelos engenheiros sociais são:

- **Impacto emocional:** o engenheiro social provoca um estado emocional forte na vítima, pode ser um sentimento de espanto, antecipação, raiva, pânico, excitação, que funciona como uma distração, interferindo na sua capacidade de avaliação, pensamento lógico ou até mesmo no desenvolvimento de um contra-argumento, de modo a levá-la a fazer o que deseja. Um exemplo disso pode ser a promessa de um prémio valorizado pelo alvo. A pessoa fica a pensar no prémio, esquecendo-se que a possibilidade de ganhar é realmente remota e acaba por facilitar informações sem pensar nas consequências indiretas;
- **Sobrecarga:** lidar com várias informações de forma rápida afeta o funcionamento lógico e pode produzir sobrecarga sensorial. Tal como referido em [36], "*com muita informação para processar, as pessoas tornam-se mentalmente passivas*". Elas absorvem a informação ao invés de avaliá-la ficando mais vulneráveis;
- **Reciprocidade:** prestar um favor em troca de vantagens no futuro é algo muito útil para o engenheiro social. Segundo Kevin Mitnick [15], num ambiente empresarial é pouco provável que as pessoas avaliem o pedido como um todo, por isso, procuram

um atalho mental. Por exemplo, uma pessoa pensa que se alguém lhe liga e oferece ajuda para resolver um problema, essa pessoa não constitui à partida nenhum risco;

- **Relações dissimuladas:** consiste na construção de um relacionamento com a vítima com o único propósito de explorá-la. Um bom método para desenvolver uma relação é a troca de informações sobre assuntos com interesses em comum, *hobbies* ou falar de alguém que não apreciam. Um exemplo desse tipo de estratégia é o ataque à AOL referenciado em [37]. Neste ataque o engenheiro social ligou para o apoio técnico da empresa e durante a conversa de quase uma hora, referiu que seu carro estava à venda. O técnico disse que estava interessado, então, o atacante enviou-lhe um *email* com uma imagem do carro em anexo. Contudo, no anexo estava um *backdoor* que permitiu estabelecer uma ligação remota pelo atacante à empresa;
- **Propagação de responsabilidade e dever moral:** o objetivo do engenheiro social é fazer com que seu alvo sinta que ele não será responsabilizado por suas ações. Esta estratégia funciona bem em conjunto com o princípio do dever moral servindo como motivação para a persuasão. Ou seja, a vítima fica a pensar que está a fazer algo pelo bem da organização ou em prol de um colega, diminuindo a sua sensação de culpa;
- **Poder e Autoridade:** as pessoas dificilmente questionam a autoridade, antes pelo contrário na presença de uma figura de autoridade, a reação mais comum é a de tentar ser afável, na expectativa de mais tarde ser recompensado. Tal atitude possibilita a que o engenheiro social se faça passar por alguém de estatuto superior à vítima para conseguir o que pretende. Em [38] é apresentado um estudo relacionado com este fator. O estudo envolveu 22 enfermeiros de postos de trabalho diferentes, que através de uma chamada telefónica (contra as normas do hospital) de um médico que nunca tinham tido contacto, recebiam a ordem para efetuar a aplicação de um determinado medicamento, numa dosagem duas vezes superior a máxima diária. Apesar, de ser óbvio o questionamento dessa ordem apenas 5% dos enfermeiros não executaram a ordem do médico;
- **Integridade e Consistência:** as pessoas têm uma tendência em acreditar que os outros estão a ser verdadeiros, tanto nos seus atos quanto naquilo que dizem. Tal como descrito em [38], o engenheiro social tira partido deste fator para se aproximar do alvo.

No artigo realizado pela Unisys [7], são ainda destacados mais dois fatores que são explorados pelos engenheiros sociais: falta de interesse ou desatenção para com as informações que são disponibilizadas a terceiros por parte dos funcionários das empresas; a falta de treino adequado em práticas de segurança de informação por parte dos funcionários.

Uma das principais características dos engenheiros sociais é serem discretos e pacientes. Eles sabem esperar pelo momento certo para lançar um ataque, e por isso procuram de forma tranquila atingir o ponto emocional mais vulnerável da vítima, o qual servirá como distração de modo a desorientá-la, para logo a seguir atacá-la.

A vantagem de se conhecerem as vulnerabilidades da personalidade humana está na possibilidade de se construir uma linha de defesa contra a engenharia social. Tal permite desenvolver políticas de segurança de informação adequadas à realidade dos funcionários e alinhadas com os objetivos da empresa e adotando métodos e medidas de controlo que travem estes riscos.

2.4. Impacto dos ataques de engenharia social

Depois de conhecer algumas das táticas que estão por trás de um ataque de engenharia social, percebe-se que a engenharia social é um ataque ao fator humano da segurança. As ações das pessoas, ao contrário dos mecanismos de defesa tecnológicos como, *firewalls*, antivírus, sistemas de deteção de intrusão, não são controlados por um conjunto fixo de regras ou políticas.

Esta dependência do comportamento humano e do aproveitamento de funcionários vulneráveis faz com que os ataques de engenharia social sejam considerados os mais difíceis de gerir. Tal levanta sérias questões relativas ao nível de risco e impacto resultante de um ataque. Se considerarmos por exemplo, que os dados dos clientes de um determinado banco foram divulgados após um ataque, tal resultará em grandes prejuízos financeiros e de reputação, pois os clientes perderão a confiança nessa instituição e provavelmente, irão procurar uma outra alternativa.

Uma pesquisa da Check Point Software Technologies realizada entre julho e agosto de 2011 [39] sobre as técnicas usadas nos ataques de engenharia social, e do seu impacto nas empresas, revelou que 48% das organizações já foram vítimas de ataques de engenharia social e que cada ataque teve um elevado custo. Revelou ainda que as táticas mais comuns neste tipo de ataque são os de *phishing* e das publicações nas redes sociais com conteúdo malicioso, representando 47% e 39% do total de incidentes respetivamente. Este estudo contou com a participação de 853 profissionais da área de Tecnologia de Informação de 7 países, como Estados Unidos, Reino Unido, Canadá, Austrália, Nova Zelândia, Alemanha. Na Figura 5 são apresentados as fontes mais comuns das ameaças identificadas neste estudo.

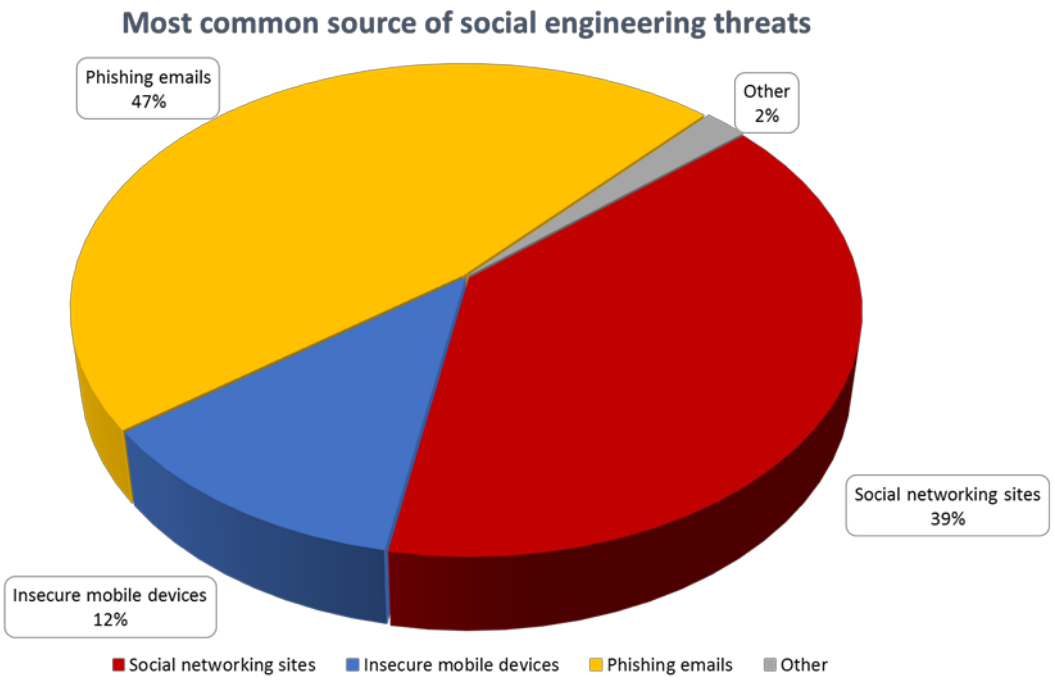


Figura 5 - Ameaças mais comuns - Check Point

Dados de 2014 apresentados no relatório de ameaças à segurança na internet pela Symantec [40] mostram que:

- O número de dados violados aumentou 62% em 2013 comparados com 2012;
- O número de identidades expostas cresceu 493%, atingindo um total de 552 milhões de vítimas;
- Os ataques de *ransomware*[6] cresceram 500%;
- Que 1 em cada 196 *emails* contém *malware*;
- 1 em cada 392 *emails* foram ataques de *phishing*.

Apesar de resultados tão assustadores, deve-se ainda levar em consideração as afirmações de Mitnick e Simon [15], que sustentam que a maioria das empresas acabam por não saber que sofreram um ataque. Se soubessem os números seriam provavelmente superiores.

Em [16], são apresentados alguns dos principais impactos resultantes de ameaças que utilizaram a engenharia social como tática de ataque:

- Informação sensível que no mercado negro se traduz em dinheiro;

[6] O Ransomware é uma especíe de malware (software mal-intencionado) que os criminosos instalam em seu computador sem seu consentimento. [41] Microsoft. "O que é ransomware?". Internet: http://www.microsoft.com/pt-br/security/resources/ransomware-whatis.aspx. [Oct, 2015].

- Espionagem e vigilância;
- Disseminação de *malware* para obter credenciais, acesso remoto, roubo de informação;
- Exposição de fotos sensíveis de celebridades. Por exemplo, a divulgação das fotos pessoais da atriz americana Scarlett Johansson que estavam armazenadas no icloud [42];
- Predadores sexuais fazem uso das redes sociais para atrair suas vítimas. Como exemplo, o caso de um predador sexual de 25 anos em Portugal que utilizou uma rede social para conhecer e seduzir duas crianças, ambas com 13 anos [43];
- A utilização da página da organização Wikileaks para divulgação de informações confidenciais. Tal teve um elevado impacto na relação entre os estados e organizações [44];
- Revelações feitas pelo ex-administrador de sistemas da CIA, Edward Snowden sobre existência dos programas de vigilância e espionagem. Estas revelações levaram o governo americano a culpar o governo chinês e russo por apoiar a fuga de um traidor [45], mas também foi alvo de críticas por parte de outros países [46].

Os ataques informáticos estão cada vez mais sofisticados, o lado humano é considerado como o elo mais fraco e as consequências dos ataques são cada vez maiores e abrangentes. Ao longo da próxima subsecção apresentam-se algumas das soluções que procuram reduzir o risco e o impacto destes ataques.

2.4.1. O que é feito para mitigar estes ataques

O aumento de ataques de engenharia social é algo bastante preocupante para as organizações. Para evitar ou diminuir o potencial risco de informações confidenciais serem acedidas, perdidas ou adulteradas sem autorização, as organizações necessitam de definir políticas de segurança específicas, bem como definir planos de educação e treino para os seus funcionários. Considerando a complexidade da engenharia social, tais medidas são extremamente importantes para reduzir os riscos. A este nível há ainda desafios a ultrapassar.

A solução para a segurança da informação não deve ser baseada apenas nos dispositivos tecnológicos. Tal como é dito por Assunção [47], "*é necessário os responsáveis entenderem que de nada adianta investir em softwares e hardwares, visando melhorar a segurança, se não for feito um plano contra a Engenharia Social*".

As pessoas devem ser aconselhadas a desconfiar de quaisquer interações anormais e orientadas a identificar possíveis ataques. É importante que todos tenham consciência de que

podem ser um alvo de ataque. Kevin Mitnick [15] defende que quanto mais o indivíduo acreditar que a sua posição é irrelevante para a organização, não se considerando um alvo, maior será a probabilidade de ser visado.

2.4.1.1. Políticas de segurança

Uma das formas para se tentar travar as oportunidades dos ataques de engenharia social é a criação de políticas de segurança internas. Estas políticas consistem na definição clara, de um conjunto de instruções que forneçam orientação para preservar as informações, combatendo e prevenindo possíveis ameaças ou ataques que possam comprometer a sua segurança.

O objetivo é que as pessoas tenham conhecimento das técnicas utilizadas pelos atacantes, e tenham a noção de que elas desempenham um papel importante na proteção da segurança da informação, independente do cargo que ocupam na organização. Precisam de acreditar que todos são relevantes. Necessitam também de ter consciência de que qualquer organização pode ser alvo de ataque, independentemente do seu sector de atividade. Tal como referido por Alves [10], a partir do momento em que essas ideias forem incorporadas, então as pessoas estarão melhor preparadas para reconhecer este tipo de ataque.

Segundo Fonseca [48], antes de criar o conjunto de regras das políticas de segurança de informação, é necessário fazer uma avaliação dos riscos, de modo a responder as questões como:

- Que informações precisam estar protegidas e qual o nível de proteção;
- Que tipo de ameaça pode atingir a organização;
- Qual o impacto se essas informações forem comprometidas.

Esta avaliação permitirá dar prioridade às informações que necessitam de proteção imediata e ainda possibilitará uma análise da relação custo/benefício sobre a informação a ser protegida.

É ainda muito importante que os funcionários sigam as regras da política de segurança e que as considerem parte integrante das suas tarefas diárias. Para isso, é fundamental que no momento do seu desenho e implementação se tenha em consideração os aspetos como: [48]

- O equilíbrio entre funcionalidade e segurança através do estudo do fluxo de informações;
- O uso de linguagem não técnica para facilitar o entendimento de todos;

- O enfatizar da importância dessas medidas de segurança e a responsabilidade para com isso;
- A inclusão de linhas orientadoras, objetivos bem definidos;
- O envolvimento dos funcionários na construção dos planos, de modo que as suas necessidades sejam consideradas;
- A elaboração de dois relatórios: instruções e procedimentos, de modo a que não perturbem o ambiente organizacional no momento da implementação;
- A criação de medidas que acompanhem a implementação das políticas, após sua implementação através de um processo de educação dos utilizadores às políticas adotadas.

As políticas de segurança devem ser alteradas e adaptadas às novas técnicas utilizadas pelos engenheiros sociais de acordo com o seu surgimento, e para que esta atualização seja feita regularmente, devem-se estabelecer procedimentos regulares com o objetivo de identificar novas ameaças. Importa contudo salientar, que as políticas de segurança não garantem a eliminação das possibilidades de ataques de engenharia social, mesmo que seguidas corretamente por todos. O objetivo é minimizar o risco a um nível que seja considerado aceitável.

2.4.1.2. Plano de treino e consciencialização

A criação e execução de planos de treino e consciencialização é fundamental para as organizações que veem como prioridade a questão da segurança das informações. Neste âmbito devem ser consideradas medidas motivadoras, como por exemplo, dramatização, vídeos educativos, para prender a atenção e aumentar a recetividade acerca da implementação do plano durante a formação dos funcionários. De acordo com Alves [10], o treino é importante para:

- Criar um “Firewall Humano”: preparar as pessoas para que estejam mais aptas a identificar um ataque de engenharia social;
- Fortalecer o lado humano da segurança: tornar as pessoas mais conscientes da importância da segurança das informações, estabelecendo uma cultura de segurança na organização;
- Realizar uma auditoria para identificar as vulnerabilidades de ataques de engenharia social na organização;

- Criar um plano de resposta a ataques para perceber como ocorreu e determinar qual o impacto desta falha de segurança na organização a fim de prever e prevenir novos ataques.

Um programa de consciencialização sobre a segurança da informação tem como principais objetivos o de influenciar as pessoas a adquirirem novos hábitos. Consciencializá-los sobre a importância em participar nos treinos, salientando o facto de que as informações precisam de ser protegidas e ainda de que cada um é imprescindível para a segurança dessas informações. Os planos de treino devem ser realizados com alguma regularidade para que as pessoas estejam preparadas para identificar as novas ameaças e técnicas de engenharia social que estão em constante evolução.

Para um resultado mais eficaz, o plano de treinamento pode ser adaptado de acordo com os requisitos de cada grupo dentro da organização, por exemplo: rececionista, administrativo, gestor, administrador de sistemas. Outro ponto importante é não excluir nenhum funcionário mesmo que ele não tenha acesso aos sistemas. Por exemplo, o segurança ou o funcionário da limpeza, pois os engenheiros sociais costumam utilizá-los para conseguirem obter acesso a locais restritos, o que posteriormente poderá proporcionar um ataque.

Ainda de acordo com Alves [10], existem alguns tópicos que são fundamentais para a elaboração de um bom plano de consciencialização sobre segurança da informação. Entre os quais estão:

- As principais táticas, técnicas e fatores psicológicos utilizadas pelos engenheiros sociais para manipular suas vítimas;
- Como proceder frente a uma solicitação suspeita;
- Quem informar sobre uma tentativa de ataque independentemente do seu sucesso;
- Os procedimentos para proteger as informações confidenciais;
- Métodos para confirmar a identidade das pessoas que solicitam algum tipo de informação, independentemente do cargo que ocupam;
- Como fazer a divulgação de informação restrita;
- Boas práticas para a utilização do correio eletrónico, de modo a evitar *malware* e *phishing*;
- Descrição de cada política de segurança e a sua importância na proteção da informação;
- Explicar a obrigação e a responsabilidade do cumprimento das regras, bem como, as consequências do seu incumprimento;

- Incentivar os funcionários a cumprir as políticas de segurança.

Segundo a pesquisa da Check Point Softwares Technologies, apresentada em [39], os novos funcionários e os subcontratados representam um maior risco e estão mais suscetíveis a técnicas dos engenheiros sociais por estarem menos familiarizados com as políticas de segurança da organização. Dessa forma, é fundamental que as organizações treinem seus funcionários assim que são admitidos, salientando a importância dos tópicos acima referidos.

3. Preparação e estratégia do processo de "engenharia social"

Atualmente é possível obter muitas informações sobre um alvo através da Internet e das redes sociais. Por isso, para conhecer melhor sua vítima, o primeiro passo do engenheiro social é fazer pesquisas na Internet, e ir às redes sociais para encontrar informações importantes que poderão ser utilizadas para um eventual ataque no futuro. Devido a essa facilidade, neste trabalho decidiu-se fazer um estudo sobre o comportamento das pessoas nas redes sociais e na forma como estas interagem com estranhos e cedem voluntariamente informação. Este trabalho é vital para perceber o estado atual e planear ações futuras que visem reduzir o potencial de exploração de um ser humano para levar a cabo um ataque.

Para a realização deste estudo foram utilizados dois cenários. O primeiro cenário envolveu a utilização de perfis em redes sociais, dirigidos a diferentes grupos etários, feitos apenas em Língua Portuguesa, aos quais podiam associar-se voluntariamente. O segundo cenário envolveu a criação de uma página *online,* cujo tema estava relacionado com a área da saúde e bem-estar.

O primeiro cenário tem por objetivo analisar a forma como as pessoas se relacionam e partilham dados com desconhecidos. O segundo cenário permitiu analisar a predisposição das pessoas em divulgarem dados pessoais num sistema, ainda que devidamente alertadas sobre os termos e condições da sua subscrição no *site*. Estes termos e condições foram claros ao afirmar que os dados pessoais recolhidos não seriam cedidos a terceiros, podendo no entanto, serem utilizados para fins de estudos de utilização segura da Internet.

Os dois cenários foram testados ao longo de um período de 45 dias. No caso do segundo cenário não foi feito o armazenamento de dados. Os dados inseridos foram analisados de forma automática e descartados de seguida.

Através da execução dos cenários descritos, foi feita uma análise geral sobre:

- O comportamento das pessoas em redes sociais, nomeadamente a percentagem e rapidez com que as pessoas de diferentes classes etárias e organizados por sexo se relacionam e trocam dados com desconhecidos;
- A quantidade de pessoas que fornecem voluntariamente dados pessoais organizadas por classe etária e por sexo;

- A quantidade de pessoas que fornecem voluntariamente dados sensíveis, como as credenciais de acesso. Os resultados foram igualmente organizados por classe etária e por sexo.

Este estudo procurou unicamente fazer uma análise geral do comportamento humano segundo uma perspetiva de engenharia social, de forma a identificar padrões de comportamento. Esta análise é fundamental para conhecer as vulnerabilidades humanas e definir programas de educação e treino específicos para cada classe etária envolvida. Por razões de privacidade não são revelados os dados pessoais obtidos, nem feitas referencias a pessoas nem às redes sociais utilizadas no estudo. Os nomes utilizados para os perfis das redes sociais foram criados para o efeito, não fazendo referencia a ninguém em específico.

3.1. Metodologia de análise

Este trabalho foi dividido em duas etapas.

Na primeira etapa foram utlizados quatro perfis numa rede social de ambos os sexos. Cada um dos perfis pertence a um diferente grupo etário, distribuído da seguinte forma:

- Idade menor ou igual a 20 anos – alunos do secundário.
- Idade entre 21 e 30 – alunos do ensino superior/profissionais em início de carreira.
- Idade entre 31 e 50 – pessoas no mercado de trabalho, que provavelmente, por fruto da idade, estão de alguma forma mais habituadas às tecnologias de informação e à partida com maturidade para lidar com situações estranhas.
- Idade maior que 50 anos – pessoas de maior idade para contemplar utilizadores tardios das tecnologias de informação.

Uma vez criados os perfis, houve necessidade de os tornar mais apresentáveis e credíveis perante os utilizadores desconhecidos. Neste sentido, os quatro perfis disponibilizam algumas informações, como por exemplo, a cidade em que vivem, a escola em que estudaram, os gostos musicais e cinematográficos, algumas publicações e também algumas fotografias. Tal como foi referido anteriormente, os perfis ficaram ativos durante 45 dias. O engenheiro social vestiu o papel de cada um dos perfis e durante o período de análise construiu uma imagem perante os seus seguidores. Esta fase foi importante para a segunda etapa.

Para a segunda etapa foi criado um *site* com divulgação de notícias relacionadas com a área da saúde e bem-estar. A página permitia ao utilizador fazer subscrição das notícias, sendo para isso necessário que respondesse a algumas perguntas com o objetivo de personalizar o

recebimento de *emails* com informações do seu interesse. A página esteve *online* durante 45 dias. Esta página começou por ser divulgada através das redes sociais, nomeadamente através dos perfis criados na etapa um.

3.1.1. Cenário 1 – Utilização de perfis em redes sociais

Foram utilizados dois perfis femininos e dois masculinos com idades diferentes. Segue uma descrição dos quatro perfis utilizados para o estudo.

- ✓ **Perfil de Luana Sampaio:** perfil feminino com idade de 16 anos, solteira, vive na Lixa e é estudante da escola secundária da Lixa. Entre seus interesses estão:
  - Músicas: Beyoncé, Alicia Keys, Adele, One Direction, Taylor swift, Justin Timberlake, entre outros.
  - Filmes: A saga Twilight, Harry Porter, Os Jogos da Fome, Encalhados, A culpa é das estrelas, entre outros.

Nas Figuras 6 e 7 pode-se ver a página de entrada no perfil da "Luana Sampaio".

Figura 6 - Perfil de Luana Sampaio

Figura 7 - Publicações do perfil de Luana Sampaio

- ✓ **Perfil de Daniel Coelho:** perfil masculino com idade de 26 anos, solteiro, vive em Setúbal e estudou na Universidade do Minho, gosta de futebol e torce pelo Benfica. Entre seus interesses estão:
  - Músicas: Eminem, Linkin Park, Bob Marley, Miley Cyrus, Maroon 5, Adele, Fleur East, entre outros.
  - Filmes: Homem de Negro, Sherlock Holmes, Avatar, Os Jogos da Fome, Sniper Americano, entre outros.

Nas Figuras 8 e 9 é ilustrada a página de entrada do perfil do "Daniel Coelho".

Figura 8 - Perfil de Daniel Coelho

Figura 9 - Publicações do perfil de Daniel Coelho

- ✓ **Perfil de Nuno Ferreira:** perfil masculino com idade de 45 anos, solteiro, vive em Lisboa e estudou na Universidade Nova de Lisboa, gosta de viajar e suas equipas favoritas são o Benfica e o Real Madrid. Entre seus interesses estão:
    - Músicas: João Veloso, The Gift, U2, Guns 4 Roses, Jorge Palma, Pink Floyd, Maroon 5, entre outros.
    - Filmes: O Jogo da Imitação, Sherlock Holmes, A Teoria de Tudo, Avatar, Os Jogos da Fome, Sniper Americano, entre outros.

O perfil público do “Nuno Ferreira” é ilustrado nas Figuras 10 e 11.

Figura 10 - Perfil de Nuno Ferreira

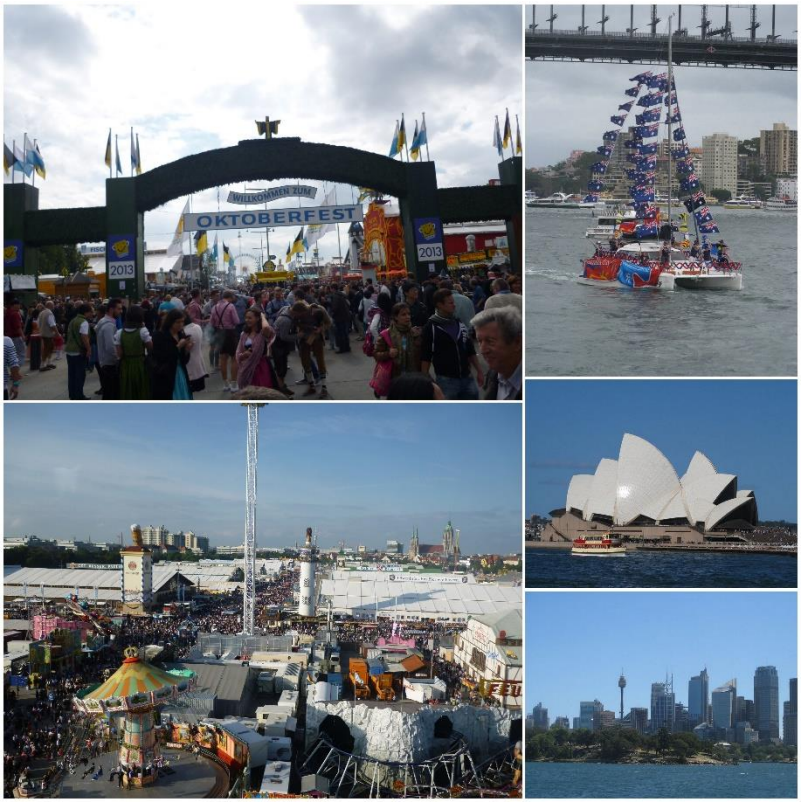


Figura 11 - Publicações do perfil de Nuno Ferreira

- ✓ **Perfil de Sandra Moniz:** perfil feminino com idade de 51 anos, solteira, vive em Coimbra e estudou na Universidade de Coimbra, gosta de política, ler, viajar e adora seu gato de estimação, cujo nome é Jimmy. Entre seus interesses estão:
    - Músicas: Eminem, Madona, Bob Marley, Queen, Maroon 5, Adele, Coldplay, Rita Guerra, entre outros.

- Filmes: Serena, Cake, Sherlock Holmes, Avatar, Birdman, Os Jogos da Fome, Sniper Americano, entre outros.

A página de entrada e alguns dos *posts* da "Sandra Moniz" são ilustrados nas Figuras 12 e 13 respetivamente.

Figura 12 - Perfil de Sandra Moniz

Figura 13 - Publicações do perfil de Sandra Moniz

Como se verifica pelas imagens ilustradas, em nenhum dos perfis são mostradas imagens que permitam identificar pessoas. Tal como dito anteriormente, o "engenheiro social" foi alimentando os perfis de forma regular, construindo uma imagem de si próprio perante os seus novos "amigos".

3.1.2. Cenário 2 – Site de notícias relacionadas com a saúde e o bem-estar

Para o cenário 2 foi criada uma página *online* com o nome Blog Pura Saúde. O objetivo desta página, do ponto de vista dos utilizadores, é partilhar informações relacionadas com a área da saúde e bem-estar, como por exemplo, notícias sobre dietas, exercícios físicos, doenças relacionadas com a obesidade e o sedentarismo, tabaco, entre outras. O cabeçalho da página principal do blogue é ilustrada na Figura 14. Como se pode ver pela figura houve cuidado em criar uma página com uma boa imagem para criar a sensação de realismo.

Figura 14 - Cabeçalho do Blog Pura Saúde

Através da página principal do Blog Pura Saúde, o utilizador tinha acesso a uma pequena dica de saúde chamada "Dica da Semana". Esta área foi criada com o objetivo de sensibilizar o utilizador a respeito das boas práticas da saúde. A dica era alterada semanalmente. Um exemplo do que é apresentado ao visitante pode ser visto na Figura 15. Ainda neste bloco, havia o botão "Subscrever notícias" que permitia ao utilizador fazer a subscrição de notícias através do preenchimento de um formulário com algumas questões pessoais.

Figura 15 - Dica da semana e botão de subscrição do blogue

No corpo da página do blogue, era apresentado um carrossel, tal como ilustrado na Figura 16, com blocos de notícias relacionadas com o tema do blogue. Para ver as notícias por completo, bastava clicar no botão “Saiba mais”. Também se podiam utilizar as setas para navegar e conseguir visualizar as notícias mais antigas.

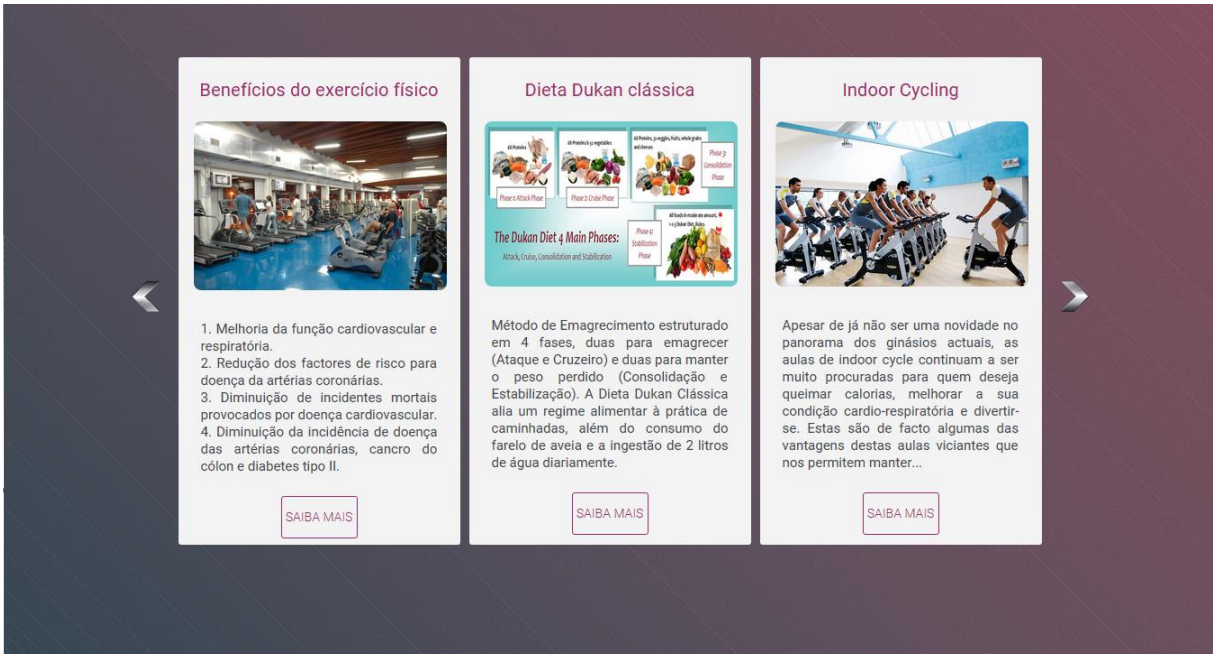


Figura 16 - Carrossel de notícias do Blog Pura Saúde

No rodapé da página do blogue encontrava-se os logótipos das redes sociais mais comuns (Figura 17). Estes logótipos funcionavam como um *link* tornando possível para o utilizador a divulgação e partilha das notícias do Blogue nas suas respetivas páginas sociais.

Figura 17 - Rodapé do Blog Pura Saúde

Na Figura 18 é ilustrada a página por completo permitindo assim ter uma ideia integrada do seu aspeto e funcionalidades apresentadas aos visitantes.

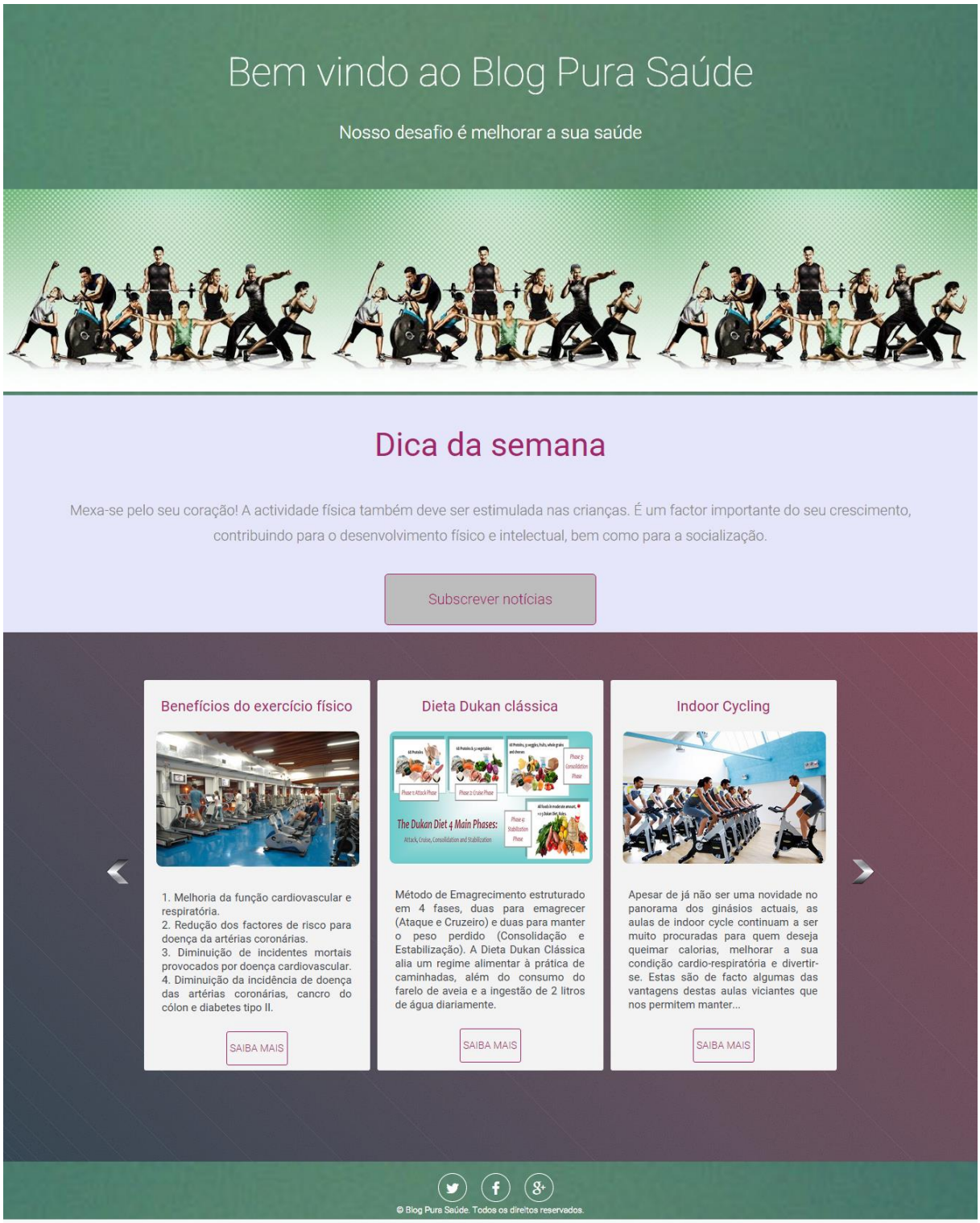


Figura 18 - Página principal do Blog Pura Saúde

Através do botão “Subscrever notícias” da página era possível subscrever uma *newsletter*. Clicando nessa opção o visitante é direcionado para uma página onde se encontrava um formulário com algumas questões pessoais que deveriam ser preenchidas pelos utilizadores, caso desejassem receber um *email* com as notícias publicadas no blogue.

Para a subscrição da *newsletter* é apresentado um formulário. Este formulário é apresentado na Figura 19. Os campos/questões que constavam no formulário eram:

- *Email*
- *Password*
- Nome completo
- Morada
- Localidade
- Sexo
- Código postal
- Distrito
- Telefone
- Data de Nascimento
- Possui alguma doença?
- É fumador?
- Peso
- Altura
- Pratica exercício físico quantas vezes por semana?
- Concorda com os termos e condições?

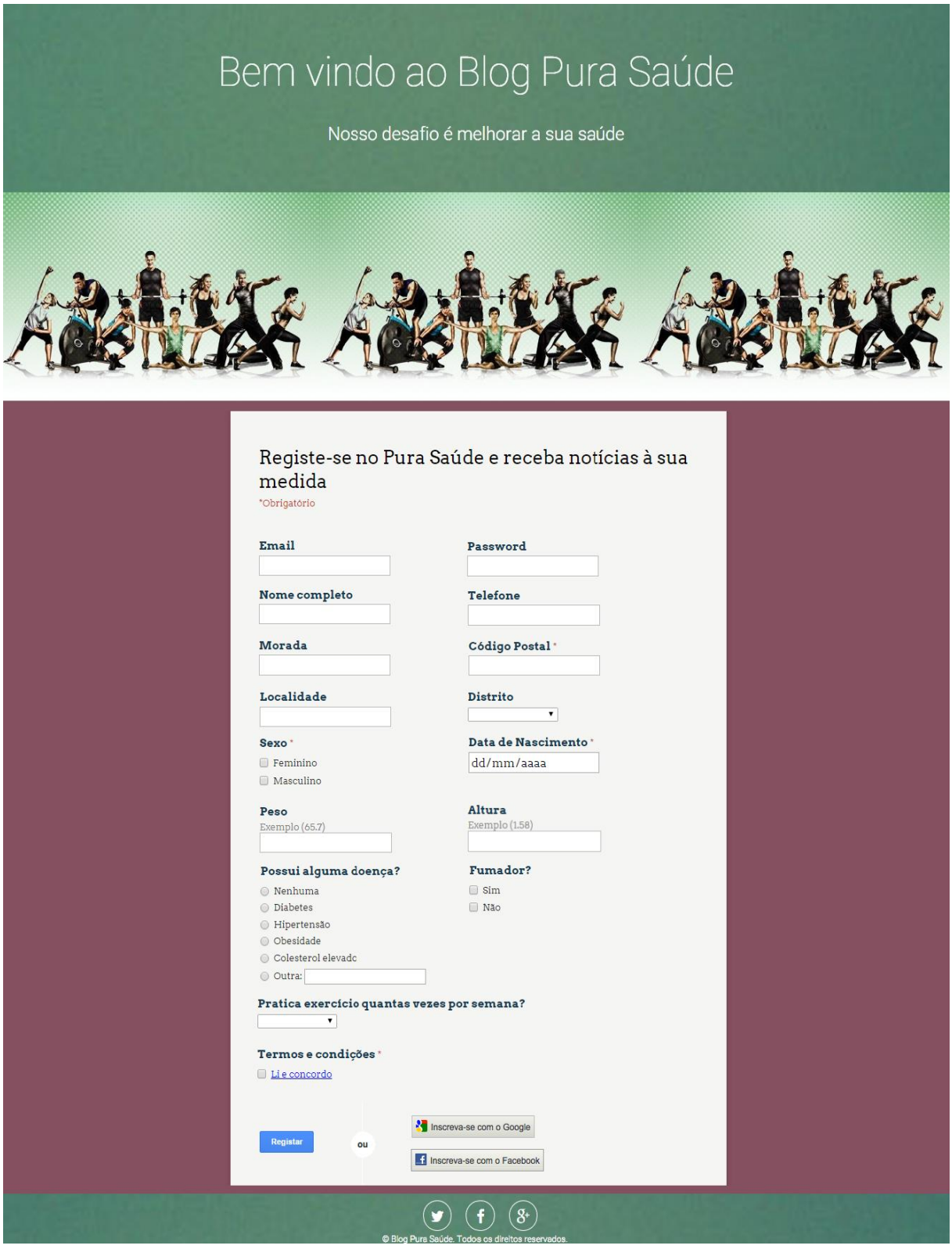


Figura 19 - Formulário de registo para a subscrição de notícias

No formulário de registo da *newsletter*, os campos com preenchimento obrigatório eram:

- código postal;
- sexo;
- data de nascimento;
- aceitação dos termos e condições de utilização.

O objetivo dessa obrigatoriedade era o facto de nos permitir gerar estatísticas dos subscritores com base na faixa-etária, localidade e sexo. Os outros campos eram de carácter facultativo, ficando o seu preenchimento ao critério do utilizador. Estes campos servem para analisar qual a predisposição dos utilizadores em fornecer dados pessoais, mesmo quando não são exigidos.

Ao utilizador era facultado o preenchimento de campos não obrigatórios relacionados com a introdução do *email* e *password*. Dentre as suas opções, estão:

- O não preenchimento dos campos email e password;
- O preenchimento dos campos no formulário;
- ou ainda o registo através de suas contas Google ou Facebook. Nesta opção, ao selecionar um dos botões, era direcionado para uma nova janela que lhe pedia a introdução das suas credenciais de acesso, como ilustram as Figuras 20 e 21.

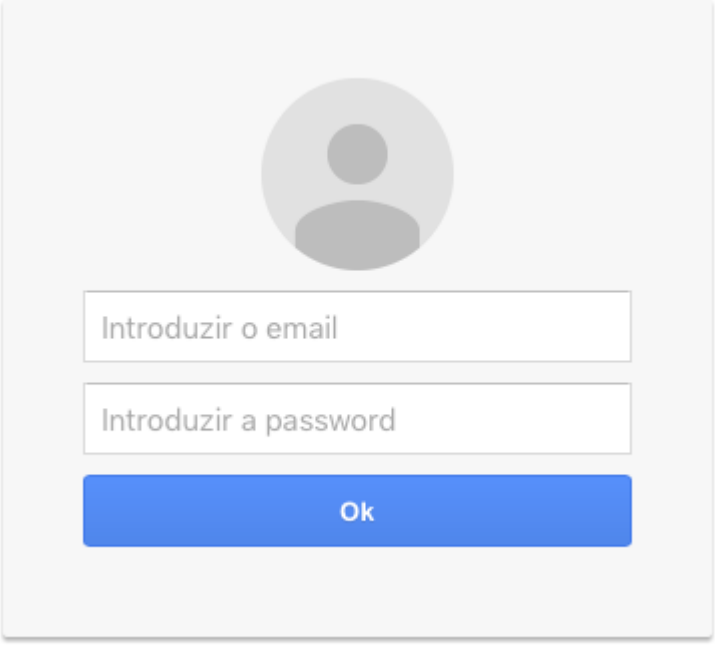


Figura 20 - Login da conta Google

Figura 21 - Login conta Facebook

É de referir que relativamente ao armazenamento das informações, o objetivo era o de respeitar a privacidade do utilizador. Desta forma, não foram guardados na base de dados do blogue, os dados dos visitantes. Após o preenchimento do formulário, os dados inseridos foram analisados automaticamente via API disponibilizada pelos sistemas de autenticação e descartados de imediato.

Todas as informações recolhidas apenas serviriam de fonte para a investigação sobre a negligência ou despreocupação por partes dos utilizadores da Internet em divulgar suas informações pessoais em *sites* pouco fiáveis e a partilha de informações em redes sociais com perfis desconhecidos. Aos utilizadores interessados na *newsletter* foi apresentado um *disclaimer* com termos e condições sobre o *site*. O conteúdo do *disclaimer* é apresentado nas Figuras 22, 23 e 24.

É de salientar que foi especificado, conforme se pode observar no ponto 5 da figura 24 que as informações disponibilizadas seriam utilizadas em prol de um estudo sobre navegação segura.

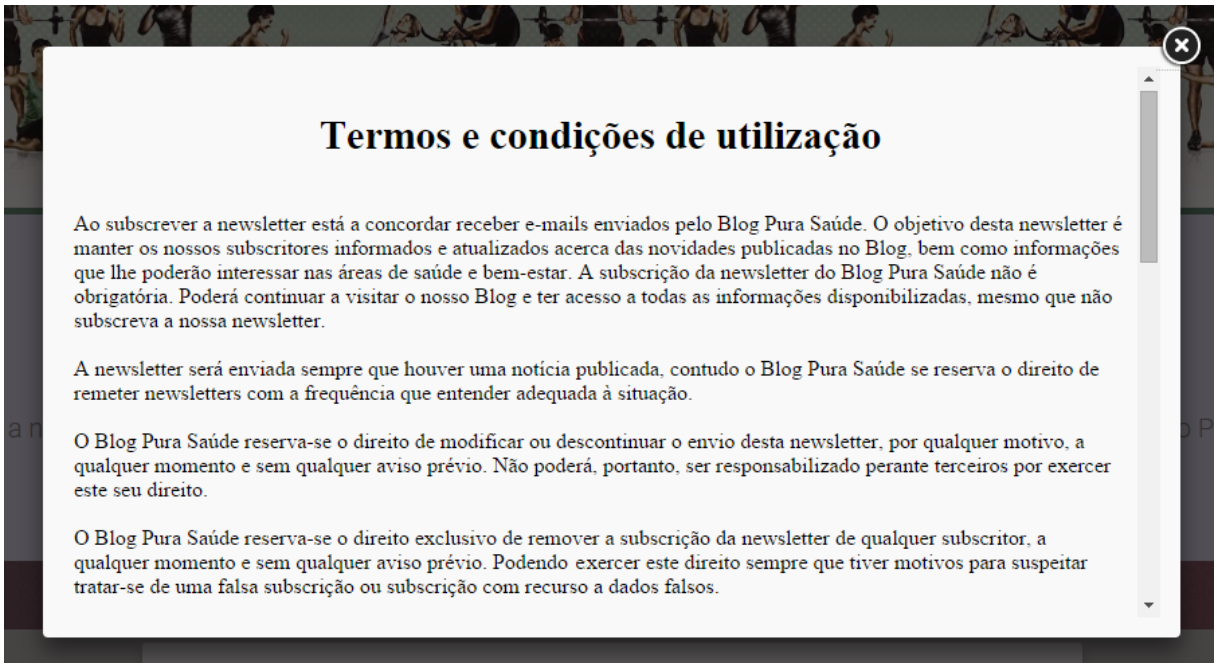
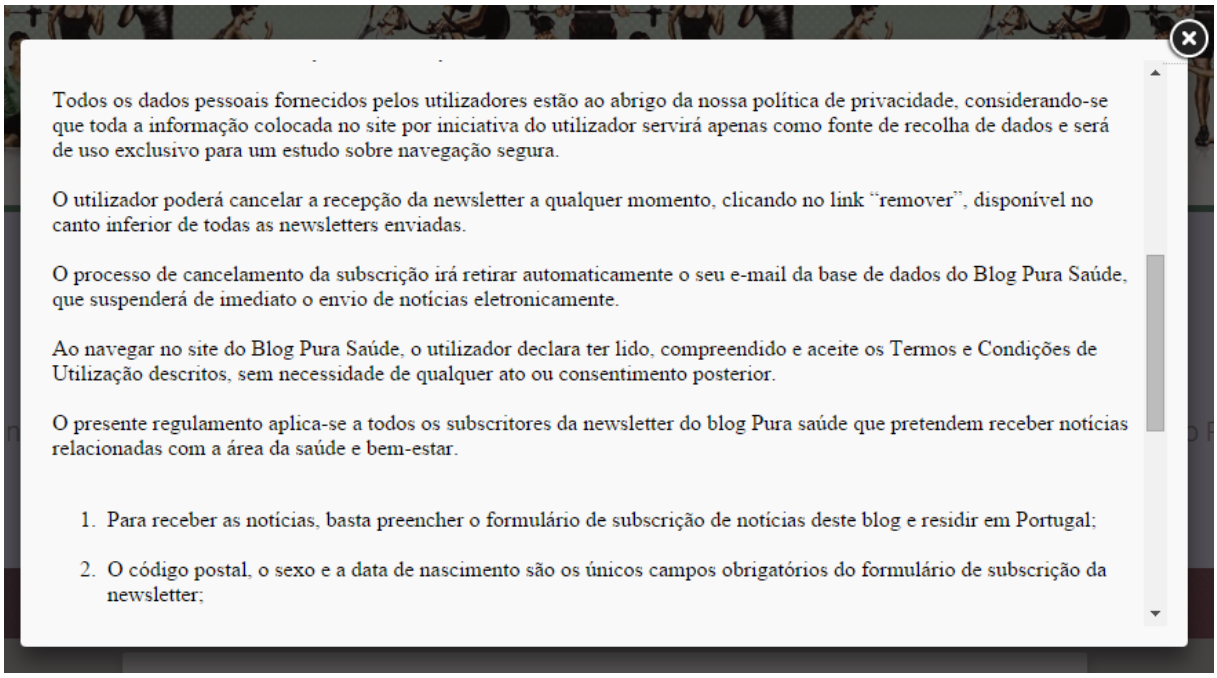


Figura 22 - Página 1 dos Termos e condições de utilização da subscrição da newsletter



Todos os dados pessoais fornecidos pelos utilizadores estão ao abrigo da nossa política de privacidade, considerando-se que toda a informação colocada no site por iniciativa do utilizador servirá apenas como fonte de recolha de dados e será de uso exclusivo para um estudo sobre navegação segura.

O utilizador poderá cancelar a recepção da newsletter a qualquer momento, clicando no link "remover", disponível no canto inferior de todas as newsletters enviadas.

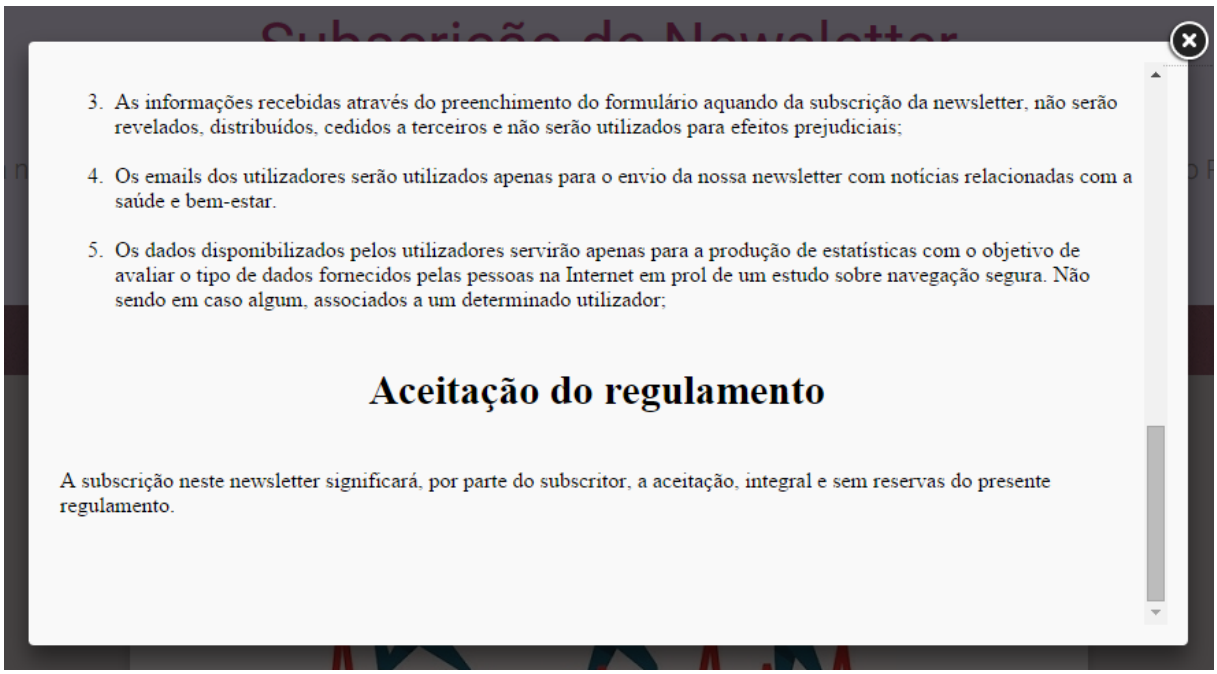
O processo de cancelamento da subscrição irá retirar automaticamente o seu e-mail da base de dados do Blog Pura Saúde, que suspenderá de imediato o envio de notícias eletronicamente.

Ao navegar no site do Blog Pura Saúde, o utilizador declara ter lido, compreendido e aceite os Termos e Condições de Utilização descritos, sem necessidade de qualquer ato ou consentimento posterior.

O presente regulamento aplica-se a todos os subscritores da newsletter do blog Pura saúde que pretendem receber notícias relacionadas com a área da saúde e bem-estar.

1. Para receber as notícias, basta preencher o formulário de subscrição de notícias deste blog e residir em Portugal;
2. O código postal, o sexo e a data de nascimento são os únicos campos obrigatórios do formulário de subscrição da newsletter;

Figura 23 - Página 2 dos Termos e condições de utilização da newsletter



3. As informações recebidas através do preenchimento do formulário aquando da subscrição da newsletter, não serão revelados, distribuídos, cedidos a terceiros e não serão utilizados para efeitos prejudiciais;
4. Os emails dos utilizadores serão utilizados apenas para o envio da nossa newsletter com notícias relacionadas com a saúde e bem-estar.
5. Os dados disponibilizados pelos utilizadores servirão apenas para a produção de estatísticas com o objetivo de avaliar o tipo de dados fornecidos pelas pessoas na Internet em prol de um estudo sobre navegação segura. Não sendo em caso algum, associados a um determinado utilizador;

Aceitação do regulamento

A subscrição neste newsletter significará, por parte do subscritor, a aceitação, integral e sem reservas do presente regulamento.

Figura 24 - Página 3 dos Termos e condições de utilização da subscrição da newsletter

3.2. Conclusão do capítulo

Ao longo deste capítulo apresentamos dois cenários de análise que foram criados com o intuito de avaliar o comportamento das pessoas. Os dois cenários combinam-se na medida em que há uma primeira fase em que o dito "engenheiro social" define uma estratégia de aproximação aos públicos-alvo e cria, ao longo do tempo, um relacionamento social com as

pessoas. Numa segunda fase, após ter algum histórico de atividade o “engenheiro social” espalha um *site* como sendo útil e apela às pessoas que sigam esse site. O *site* criado pelo “engenheiro social” foi criado com um propósito bem definido para que as pessoas depositem dados que lhes parecem fazer sentido, mas que nas mãos de um “engenheiro social” podem ser usados para fins que não os desejáveis.

No próximo capítulo serão apresentados os resultados obtidos em cada uma das fases. As conclusões sobre os resultados são igualmente apresentadas ao longo do capítulo.

4. Análise comportamental sobre ataques de engenharia social – Análise de resultados

Um “engenheiro social” define um conjunto de estratégias para obter informação estratégica. Estas estratégias podem ser mais diretas ou envolver um conjunto de fases e tarefas. É reconhecido como um trabalho de paciência que terá que ser bem elaborado e executado sob pena de ser detetado e fracassar. Tal como foi referido anteriormente, os engenheiros sociais têm hoje em dia a vida mais facilitada. As pessoas expõem-se mais nas redes sociais, e na Internet é possível obter informação sobre as organizações e os seus funcionários. A Internet é igualmente um meio ao dispor dos engenheiros sociais na medida em que de forma simples e rápida, implementam armadilhas e tentam conduzir as pessoas para estas.

No capítulo anterior foram apresentadas duas estratégias e os planos para estudar o comportamento das pessoas. Estas estratégias foram adotadas de outras exploradas no passado e referidas ao longo do capítulo 2. As estratégias, apresentadas sobre a forma de cenários são complementares na medida em que numa primeira fase, o engenheiro social constrói uma identidade tentando tornar-se o mais credível possível e numa segunda fase tenta fazer com que as pessoas exponham voluntariamente dados com diferentes níveis de sensibilidade.

Neste capítulo apresentamos os resultados obtidos por cenário e é feita uma análise sobre os mesmos.

4.1. Resultados do cenário 1: Construção de um perfil social para aproximação aos potenciais alvos de um engenheiro social

Nesta secção são apresentados os resultados relativos ao cenário um, isto é, relativamente à adesão das pessoas aos perfis de rede social criados. Os resultados mostram o número total de pessoas que aderiram aos perfis utilizados pelo engenheiro social separados por sexo e por faixa etária. Esta separação visa uma análise mais fina dos comportamentos e será útil para a definição de programas de educação e treino considerando as especificidades encontradas nestes grupos de pessoas.

4.1.1. Número de pessoas que aderiram aos perfis

A Figura 25 ilustra o número de pessoas que aderiram a cada perfil utilizado na rede social.

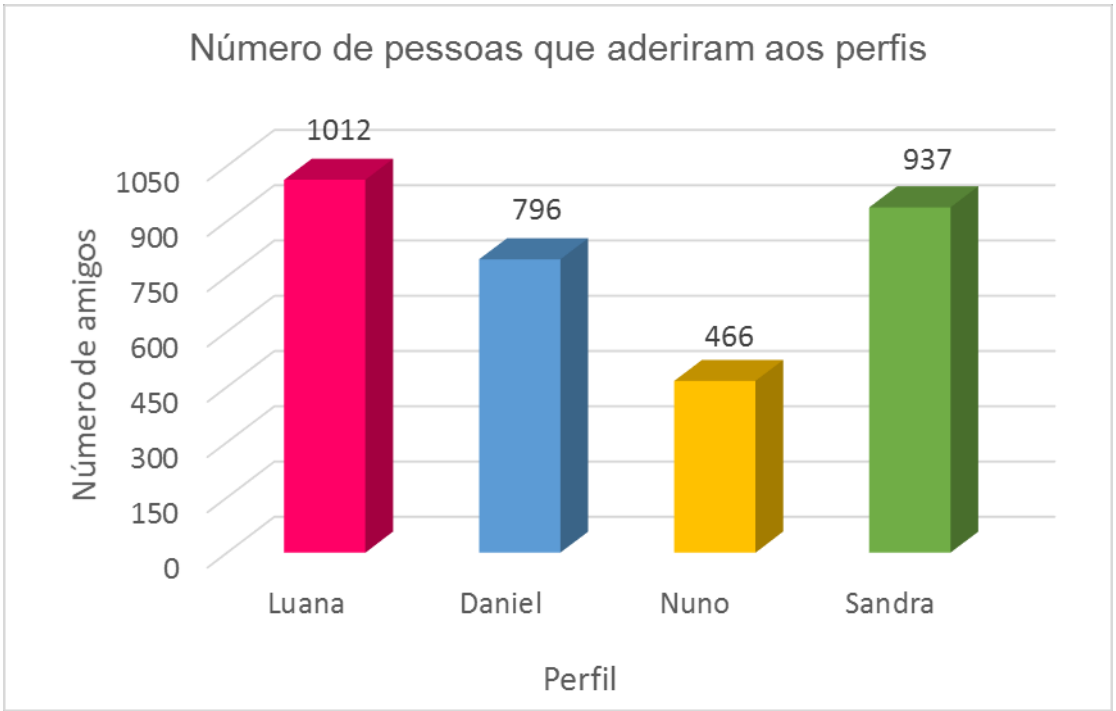


Figura 25 - Número de pessoas que aderiram aos perfis na rede social

Como se pode ver pela Figura 25, o perfil de Luana foi o que obteve o maior número, com 1.012 adesões e o perfil da Sandra vem logo a seguir com 937 adesões. Relembra-se que o perfil da Luana corresponde à faixa etária dos menores ou igual a 20 anos. O perfil da Sandra corresponde aos iguais ou maiores de 50 anos. Os resultados mostram que a utilização de perfis femininos nas redes sociais atrai um maior número de pessoas, isto poderá ser um indicador a considerar pelo engenheiro social na sua abordagem.

A Figura 26 mostra o número total de pessoas que aderiram aos quatro perfis e a percentagem que cada perfil representa em relação ao número total de subscritores.

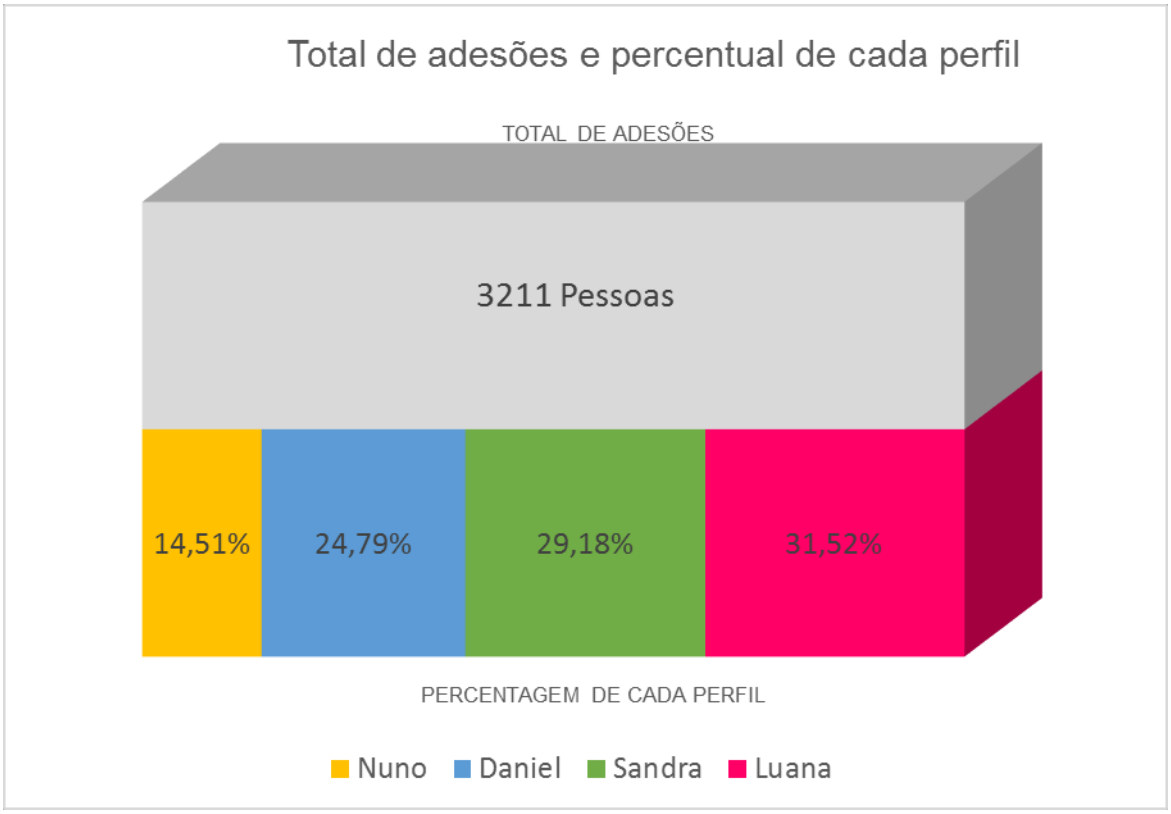


Figura 26 - Total de adesões e percentagem de cada perfil

O engenheiro social após ter ativado os seus perfis, fez alguns pedidos de amizade *ad-hoc* para construir o seu perfil inicial. Após esta fase, acompanhou a evolução dos pedidos enviados e dos pedidos recebidos. Esta evolução é ilustrada na Figura 27. Do lado esquerdo pode-se ver a percentagem de pedidos de amizade enviados pelo engenheiro social, a percentagem de pedidos que o engenheiro social recebeu por parte dos membros da rede social e a percentagem de pedidos que o engenheiro social recusou por considerar tratar-se de perfis falsos.

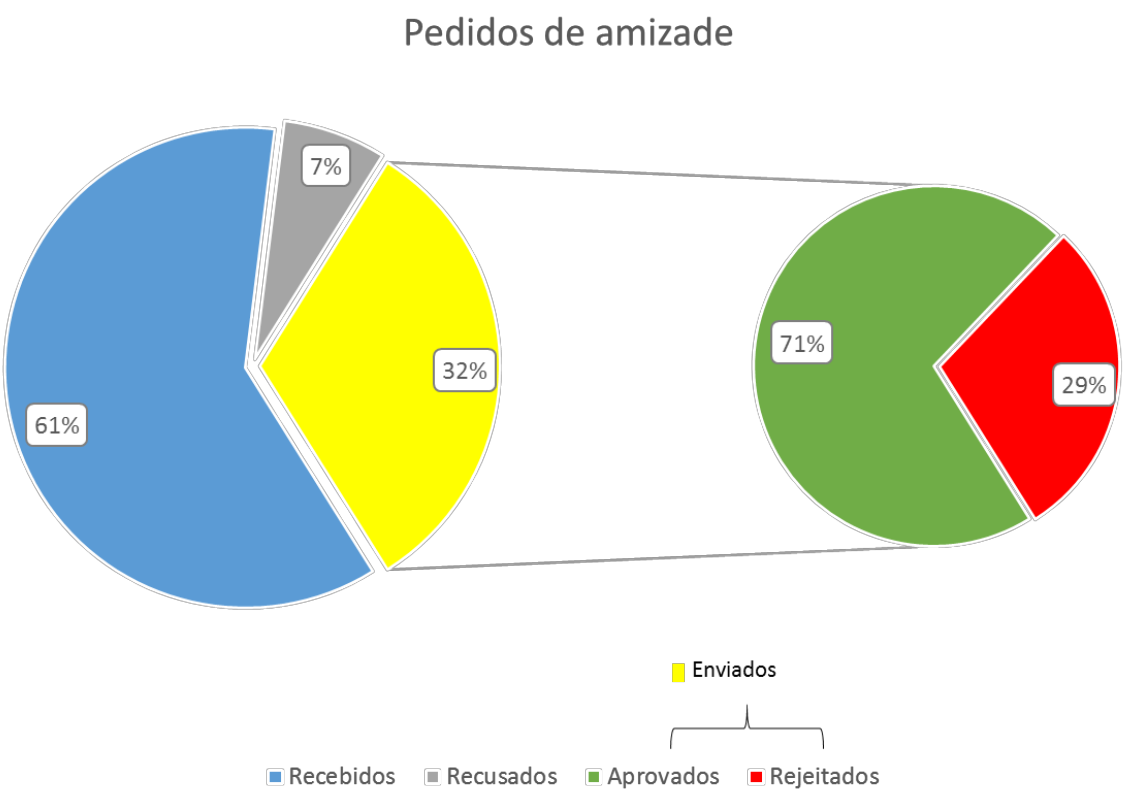


Figura 27 - Pedidos enviados e recebidos

Pela Figura 27, pode-se observar que os perfis receberam mais solicitações de amizades do que enviaram (68% versus 32%). Os quatro perfis obtiveram um total de 68% de pedidos de amizade (61% recebidos + 7% recusados). Verificaram-se 7% de pedidos recusados, isto por aparentemente se tratarem de perfis falsos. Esta conclusão advém do facto dos perfis conterem pouquíssima informação, alguns possuíam apenas o nome e a imagem do perfil, e do facto de terem sido criados recentemente. Dos 32% envios de pedidos de amizade, 71% foram aceites e apenas 29% rejeitaram a solicitação, ou seja, uma grande percentagem das pessoas aceitaram ter na sua rede de amigos, uma pessoa desconhecida.

Outra análise efetuada relativamente aos pedidos recebidos e enviados tem a ver com a velocidade a que estes pedidos foram aceites. Este indicador é útil na medida em que ajuda a perceber, quanto tempo terá um engenheiro social que esperar para atrair pessoas para a sua lista de amizades pessoais. Na Figura 28 é ilustrada a evolução do número de adesões dos quatro perfis agregados por semana.

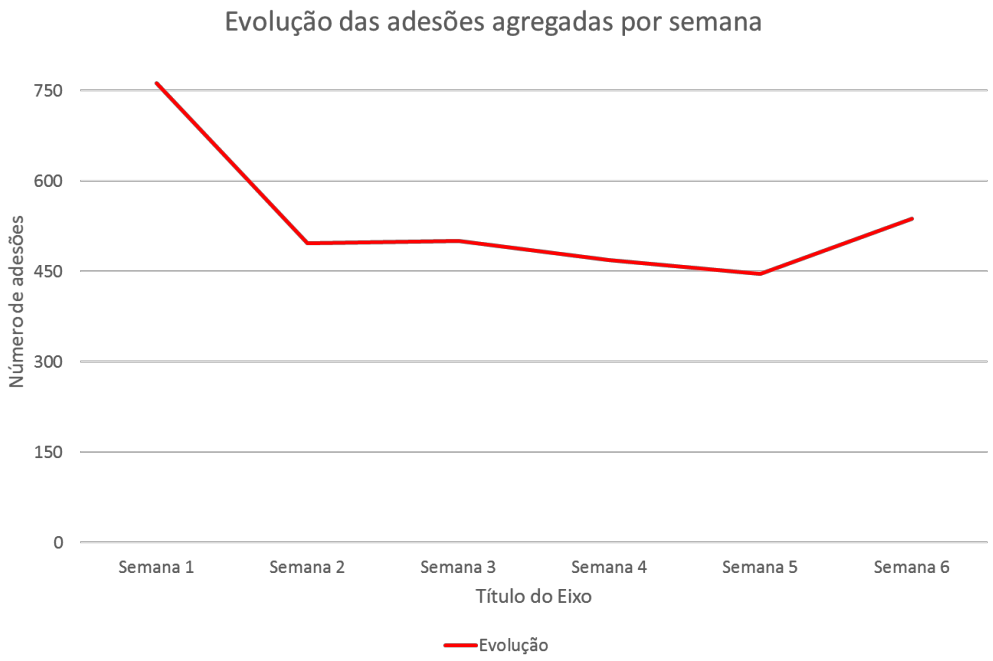


Figura 28 - Evolução da adesão por semana

Pode-se observar pelo gráfico ilustrado na Figura 28, que houve uma grande adesão na primeira semana, chegando a ultrapassar o número de 700 pessoas a aderirem aos perfis. Verificou-se que a falta de confiança, resultante do facto dos perfis utilizados ainda não terem um número considerável de amigos e com poucos *posts* publicados, não foi um problema para as pessoas se associarem. A partir da segunda semana, o número de adesões variou entre os 400 e os 600 aderentes, por semana.

Pelo gráfico apresentado no início da subsecção, percebeu-se que os perfis femininos foram os que conquistaram mais adesões. Detalhando um pouco mais estes resultados, e tal como ilustrado na Figura 29, os perfis femininos obtiveram um total de 1.949 “amigos,” representando um percentual de 60,7% do número total de adesões, enquanto os perfis masculinos alcançaram o número total de 1.262 representando 39,3% do total de adesões.

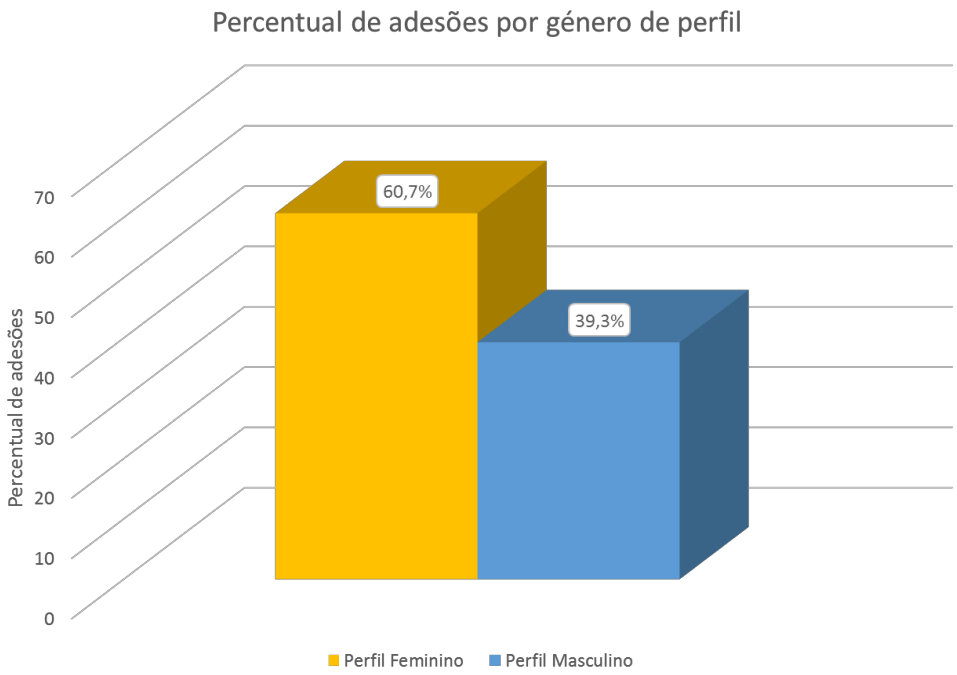


Figura 29 - Percentual de adesões por género de perfil

A análise por perfil e por género ajuda a perceber se são mais homens ou mulheres a aderir aos perfis masculinos ou femininos. Esta análise permite ao engenheiro social, perceber se deve fazer uma abordagem com um determinado tipo de perfil para maximizar o sucesso junto de um determinado público masculino ou feminino, consoante as suas intenções. Outra perspetiva, e a que mais interessa neste estudo, é a de identificar necessidades de educação e treino em função da faixa etária e sexo.

Na Figura 30 é ilustrado o número de amigos de cada perfil separados por género. Pela figura observa-se que os perfis femininos possuem um número maior de “amigos” do sexo masculino, sendo o contrário nos perfis masculinos.

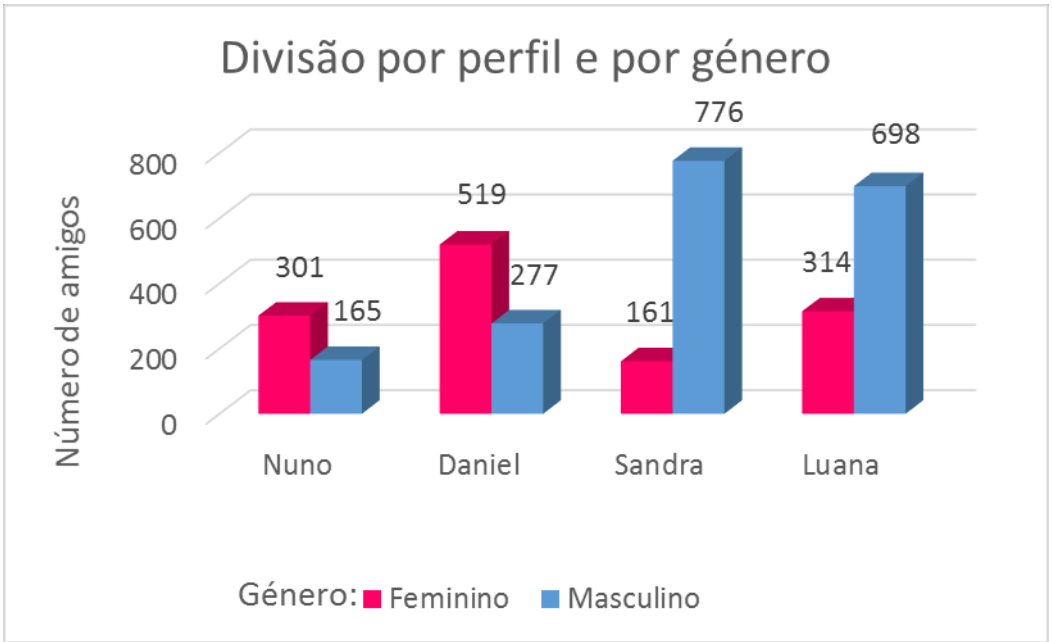


Figura 30 - Divisão por perfil e género

Outra análise que se pode fazer pela Figura 30 é que, de acordo com os resultados, o sexo masculino está mais predisposto a ligar-se em rede, independentemente do sexo do "novo amigo". Esta conclusão é reforçada pela análise do número de adesões separadas por género e faixa etária. Os resultados desta análise estão sumariados na Figura 31, e como se pode verificar, em todas as faixas etárias, o número de adesões das pessoas do sexo masculino é superior ao feminino. Também se conclui que os homens aderem mais facilmente a perfis femininos e as mulheres a perfis masculinos. Este estudo sugere que o engenheiro social ao tentar recolher informações de pessoas de determinado sexo, utilizará perfis do sexo oposto. Se o público destino for indiferenciado então o engenheiro social irá optar por construir um perfil do sexo feminino, maximizando assim, as adesões de pessoas do sexo masculino e feminino.

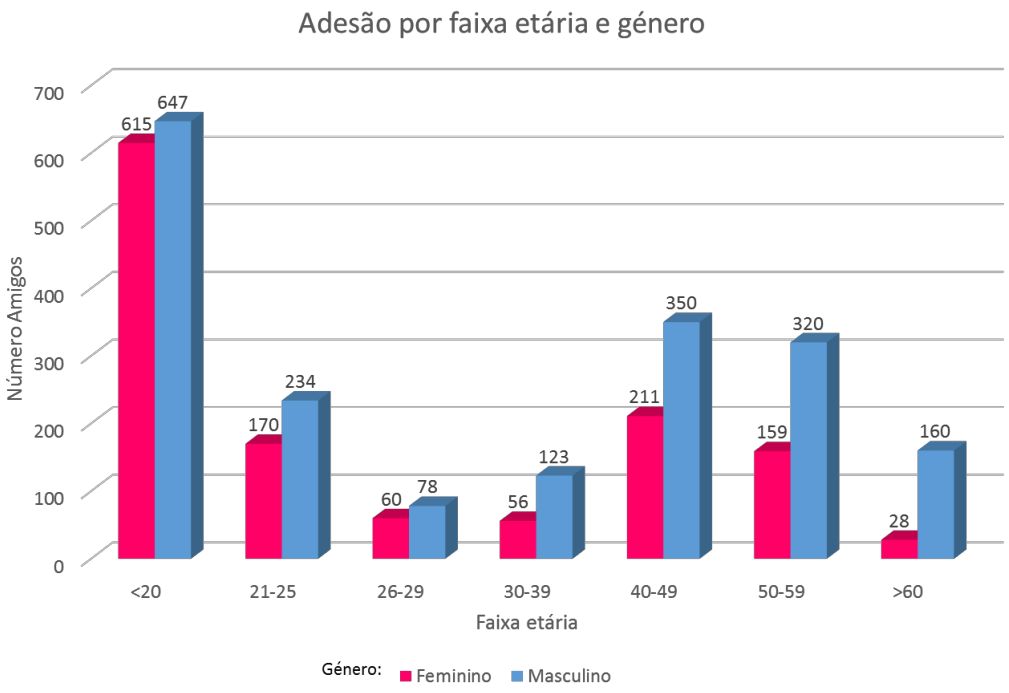


Figura 31 - Adesão por faixa etária e género

Uma última análise realizada no âmbito do cenário um, foi a percentagem de adesões de todos os perfis, divididos por faixa etária. O resultado da análise está ilustrado na Figura 32. Para este estudo foram consideradas sete faixas etárias assim distribuídas: de idade menor ou igual a 20 anos, de 21 a 25 anos, de 26 a 29 anos, de 30 a 39 anos, de 40 a 49 anos, de 50 a 59 anos e de idade maior ou igual a 60 anos.

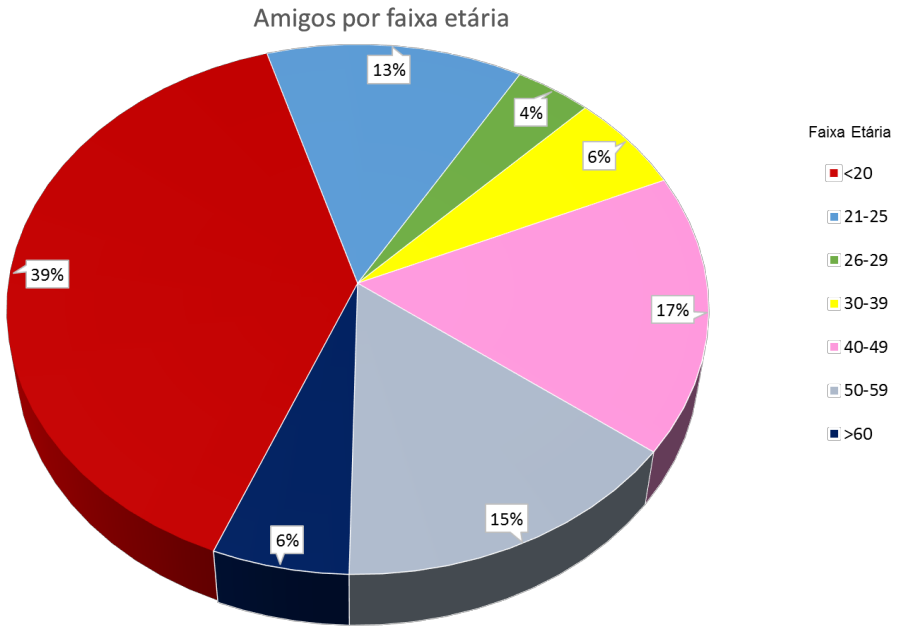


Figura 32 - Adesão por faixa etária

De acordo com a Figura 32, podemos observar que os jovens até aos 20 anos obtiveram o maior percentual do total de adesões, chegando a atingir o valor de 39%. Em segundo e terceiro lugar, temos as faixas etárias dos 40 a 49 e dos 50 aos 59 anos, com 17% e 15% respetivamente. Se agruparmos as duas primeiras faixas etárias, isto é dos menores que 20 anos e das pessoas que de acordo com o seu perfil têm entre 21 a 25 anos, obtemos 52% do total de adesões, ou seja, mais de metade dos utilizadores que se tornaram “amigos” dos perfis possuem até 25 anos. Este resultado revela que os jovens estão mais predispostos a aceitar ligações com estranhos.

No que diz respeito a potenciais perigos de utilização de Internet, os dados apresentados ao longo desta secção serão confrontados na segunda parte do estudo (cenário dois) apresentado na secção 4.2.

4.1.2. A evolução da construção do perfil social

Enquanto na subsecção anterior, foram apresentados os resultados globais da adesão das pessoas a um novo amigo, nesta mostram-se evidências da evolução do perfil social construído pelo engenheiro social. O objetivo é dar a conhecer a recetividade do novo perfil por parte dos novos amigos. Esta análise ajuda-nos a perceber quão simples será para o engenheiro social fazer uma aproximação mais efetiva das pessoas conquistando o seu espaço entre os membros, a partir da associação como simples amigo.

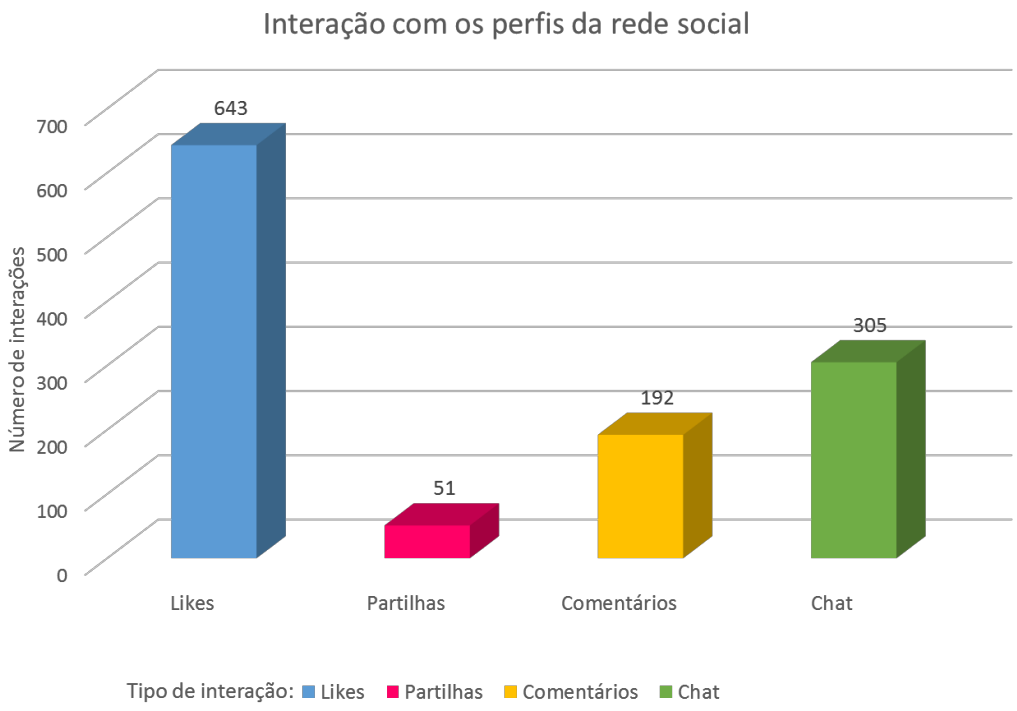


Figura 33 - Interação com os perfis da rede social

A Figura 33 ilustra o tipo de interações das pessoas com os perfis. Os quatro perfis obtiveram 643 *likes*, 192 comentários, 51 partilhas e 305 conversas no *chat*. Estes números mostram que é relativamente fácil para o engenheiro social iniciar uma aproximação com o alvo, observando-se uma espontaneidade na adesão à partilha de informações e na criação de laços de "amizade".

Foi através destes perfis que se fez a divulgação da página do Blogue Pura Saúde utilizada no cenário dois. Ou seja, num primeiro momento, criou-se um ambiente *online* confiável através das publicações e comentários feitos, tanto pelos perfis, quanto pelos "amigos" e a partir daí, foi feita a divulgação. A título de exemplo, a Figura 34, ilustra uma publicação do Blogue a partir do perfil do Daniel Coelho.

Figura 34 - Divulgação do Blogue através do perfil de Daniel Coelho

4.2. Resultados do cenário 2: Recolha de dados pessoais por parte do engenheiro social

Nesta seção são apresentados os resultados relativos ao cenário dois. Neste cenário o engenheiro social distribui pela sua rede de amigos, um *link* para uma página web de saúde e bem estar. Este *site* solicita o preenchimento de dados em troca de informações e dicas úteis às pessoas. O objetivo da análise é perceber qual é a predisposição e sensibilidade das pessoas para o preenchimento de dados pessoais. A análise mostra a quantidade de pessoas que voluntariamente fornecem dados, distribuídas por região do país, idade e sexo.

4.2.1. Adesão ao Blogue Pura Saúde

A Figura 35 dá a conhecer o número total de pessoas que fizeram a subscrição da *newsletter* do Blogue Pura Saúde e ainda o número referente a cada género. Assim, e como se pode ver pela figura, o número de pessoas que subscreveram foram 220, sendo 175 subscritores do sexo feminino e 45 do sexo masculino.

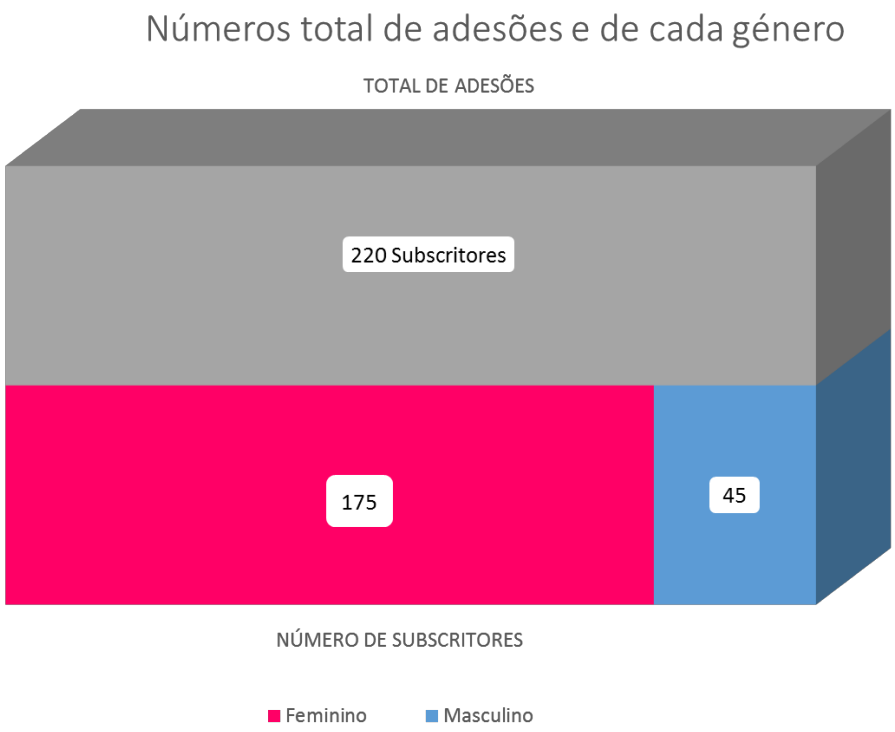


Figura 35 - Número total de adesões e de cada género

Estes dados revelam desde logo, que no âmbito do estudo e do tipo de notícias do *site*, as pessoas do sexo feminino aderem mais ao preenchimento de formulários e a divulgar informações pessoais do que os homens. Isto não significa que perante uma temática diferente os dados não sejam outros.

Na Figura 36 é ilustrada a percentagem de subscritores da *newsletter* organizada por distrito. Como se pode ver pela figura, os distritos de Lisboa e Porto ficaram em primeiro e segundo lugar com 26% e 18%, respetivamente. Aveiro e Setúbal em terceiro e quarto. Os distritos de Beja, Bragança, Guarda, Portalegre, Viana, Vila Real, Viseu e as Ilhas tiveram a menor representação percentual, sendo de aproximadamente 1% cada.

Tal como seria de esperar, constata-se que a distribuição é sensivelmente proporcional a dimensão urbana dos respetivos distritos, verificando-se que os dois maiores centros urbanos do país representam quase metade do total dos subscritores. Em todo o caso, verifica-se que os distritos de Aveiro e Braga escapam a esta lógica. O primeiro por estar sobre-representado e o segundo sub-representado na respetiva amostra.

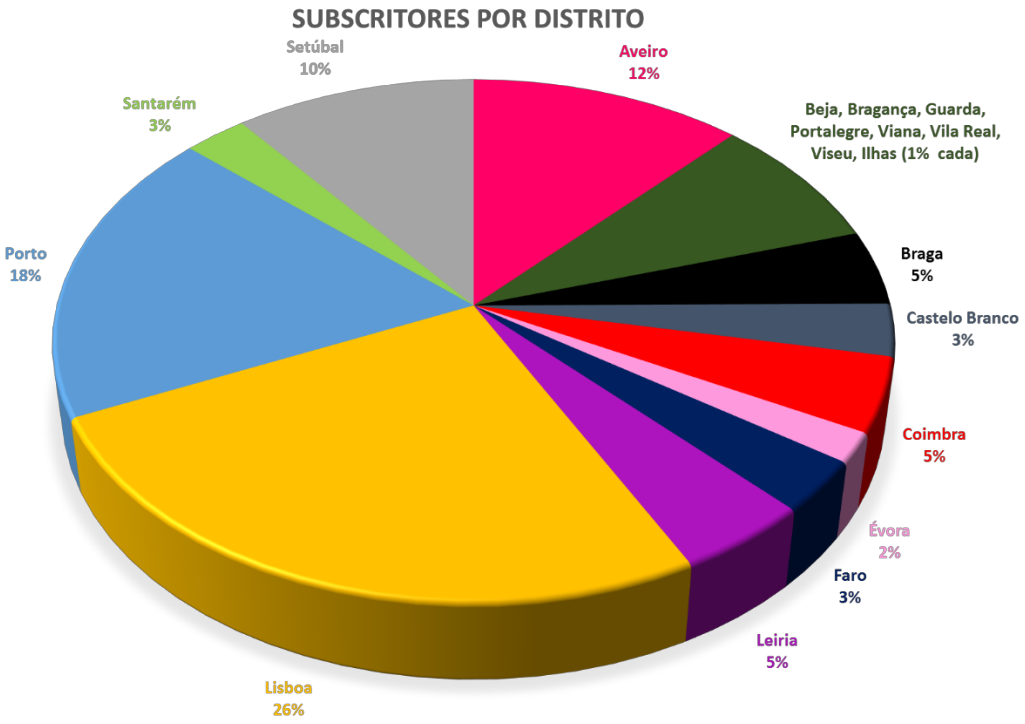


Figura 36 - Subscritores por distrito

As análises do número de subscritores organizados por faixa etária e por faixa etária e sexo também foram efetuadas.

Na Figura 37 é apresentada a percentagem de subscritores da *newsletter* separados por faixa etária. Tal como na análise feita no cenário um, os dados foram separados em sete faixas etárias. O objetivo é analisar o estado de consciencialização de cada faixa etária.

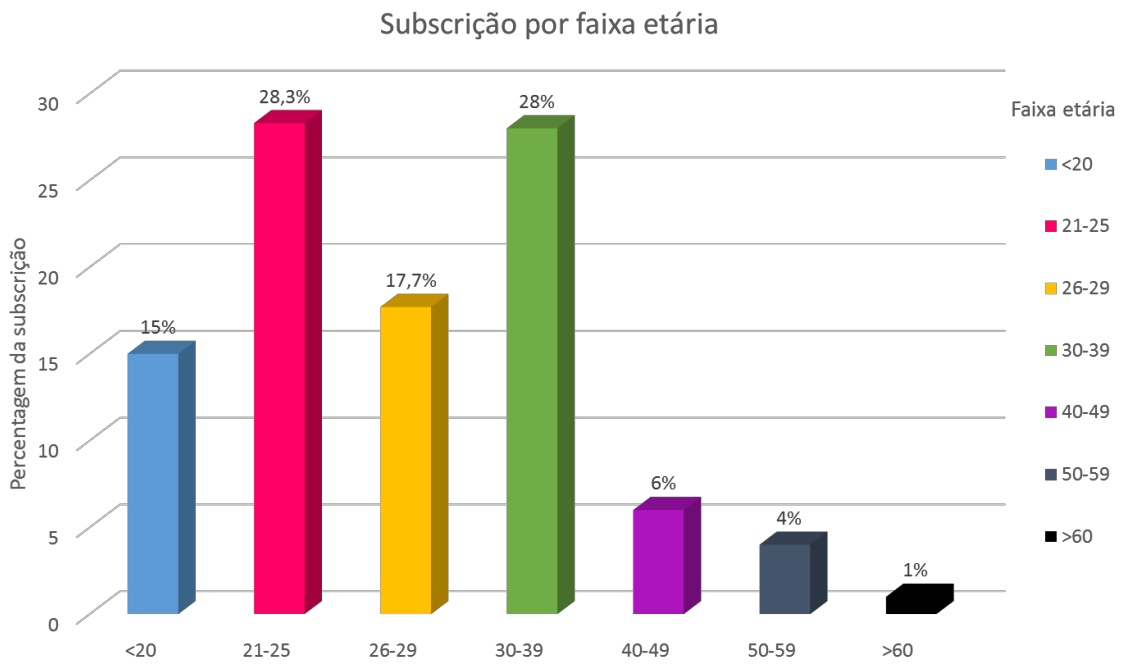


Figura 37 - Subscrição por faixa etária

Com base nos resultados obtidos, e tal como ilustrado na Figura 37, verificou-se que as faixas etárias dos 21 aos 25 anos e dos 30 aos 39 anos obtiveram resultados semelhantes e também os mais elevados, representando 28,3% e 28% do total de subscrições respetivamente. Se as quatro primeiras faixas etárias forem agrupadas, obtém-se um total de 89% dos subscritores, ou seja, as pessoas com idade até aos 39 anos, representam quase a totalidade das pessoas que cederam voluntariamente as suas informações aquando do preenchimento do formulário de subscrição. Estes resultados estão de certa forma em linha com a predisposição encontrada no cenário um, no que diz respeito à facilidade com que estabelecem relacionamentos. Em todo o caso, e como veremos mais adiante pelo tipo de informação cedida, este cenário revela uma falta de consciencialização dos mais jovens para a problemática da segurança na proteção de dados pessoais. Também se verificou no presente estudo que a adesão foi substancialmente reduzida a partir da faixa etária dos 40 anos.

Na Figura 38 é feita a divisão da percentagem de subscritores separada por faixa etária e por género. De acordo com os dados, pode-se observar que com exceção dos maiores de 60 anos, onde o valor percentual é o mesmo para homens e mulheres, nas restantes faixas etárias o percentual de subscrição de pessoas do sexo feminino é superior ao masculino. O que vem a confirmar, que neste tipo de cenário, as mulheres estão mais predispostas a fornecer dados pessoais do que os homens.

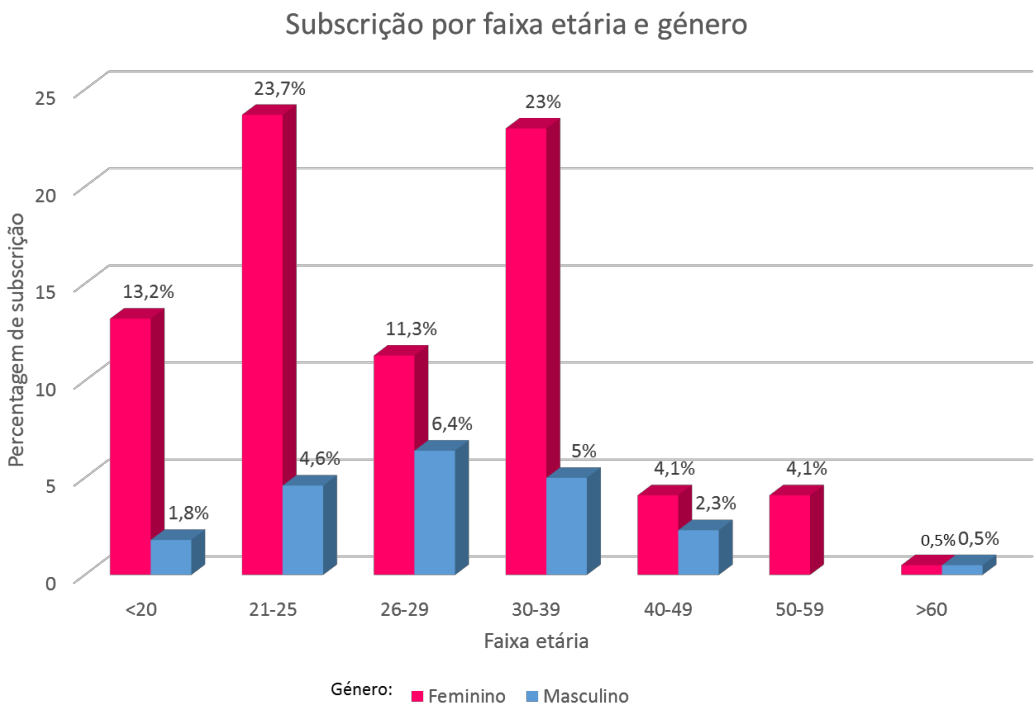


Figura 38 - Subscrição por faixa etária e género

Um dos grandes objetivos do estudo era chegar ao nível de informação partilhada pelas pessoas. Pelos resultados anteriores percebeu-se a maior predisposição do sexo feminino para subscrever a *newsletter* do blog. Falta ainda saber qual o tipo de informação que as pessoas revelaram no momento da subscrição. Estes dados são apresentados e discutidos ao longo da próxima subsecção.

4.2.2. Dados obtidos a partir do cenário 2

Os dados obtidos com a execução deste cenário são apresentados considerando:

- A quantidade de pessoas que preencheu determinado campo;
- A análise à quantidade de pessoas que inseriu as credenciais de acesso no formulário;
- A quantidade de credenciais que se veio a confirmar válidas, isto é, que permitem o acesso a outros serviços (ex.: email).

Para cada caso é feita a divisão entre faixas etárias e género.

A figura 39 ilustra os campos do formulário de subscrição que deveriam ser preenchidos por aqueles que desejassem subscrever a *newsletter* do Blogue Pura Saúde. Por cada campo é indicado o número de pessoas que inseriu dados. Tal como dito anteriormente, apenas os

campos *email*, data de nascimento, sexo, código postal e a aceitação dos termos e condições da subscrição eram obrigatórios.

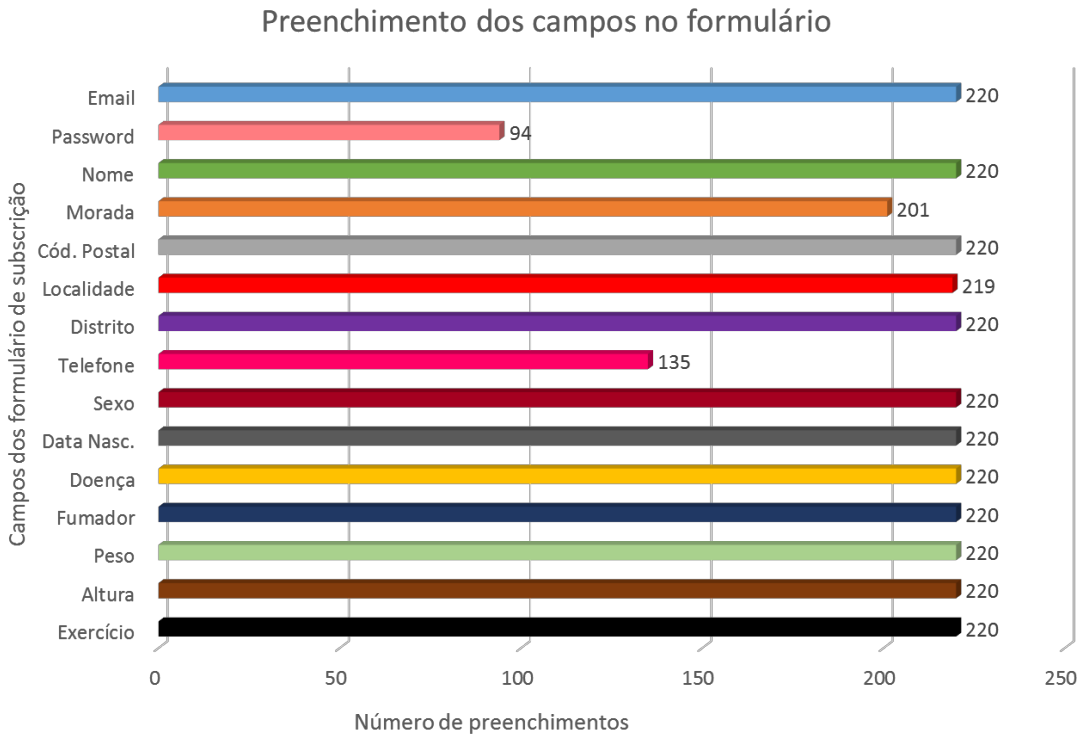


Figura 39 - Número de preenchimento dos campos no formulário de subscrição

O que se observa pela Figura 39, é que apesar da maioria dos campos não serem de preenchimento obrigatório, estes foram preenchidos pela esmagadora maioria dos subscritores. A figura mostra ainda, que a totalidade dos subscritores preencheu 8 campos facultativos. Isto mostra a predisposição das pessoas em cederem suas informações mesmo quando não são consideradas obrigatórias.

Nos resultados é de salientar o número de pessoas que preencheu o campo *password*. Não era um campo obrigatório e vemos que foi preenchido por 43% dos subscritores. De seguida será feita uma análise mais detalhada sobre o preenchimento de credenciais de login.

4.2.2.1. Resultados referentes ao preenchimento dos campos password e email no formulário de subscrição da newsletter

O facto de uma percentagem considerável de subscritores ter preenchido o campo de *password,* constitui uma grande surpresa e levanta sérias questões sobre os comportamentos das pessoas, perante um pedido de preenchimento de dados online. Tal como já foi dito, e ilustrado na Figura 39, das 220 pessoas que preencheram o formulário de subscrição, 94

preencheram os campos *email* e *password*, ou seja, 43% dos subscritores preencheram ambos os campos, como se pode observar na Figura 40.

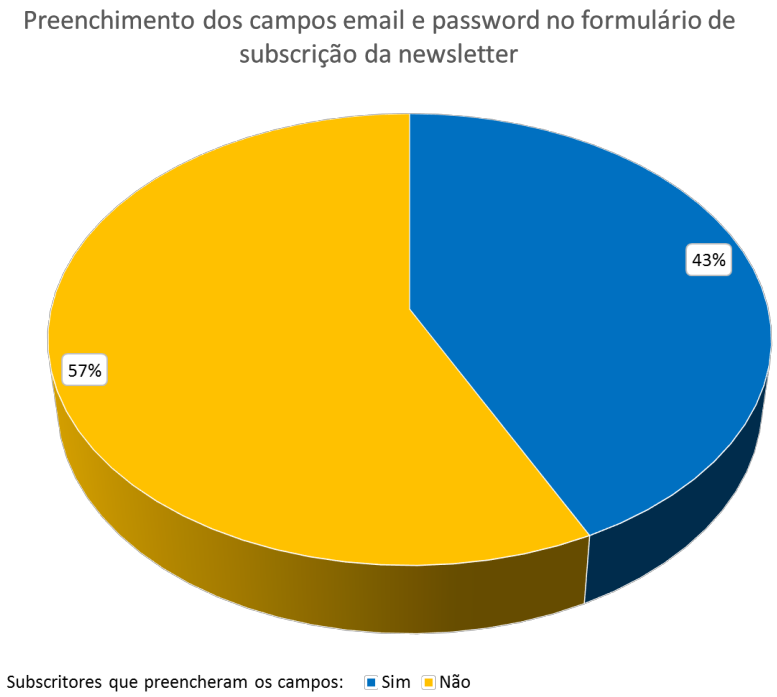


Figura 40 - Percentagem do preenchimento dos campos email e password na subscrição

Dos 43% de *passwords* inseridas, foi feita uma análise por género. O resultado desta análise é ilustrado na Figura 41.

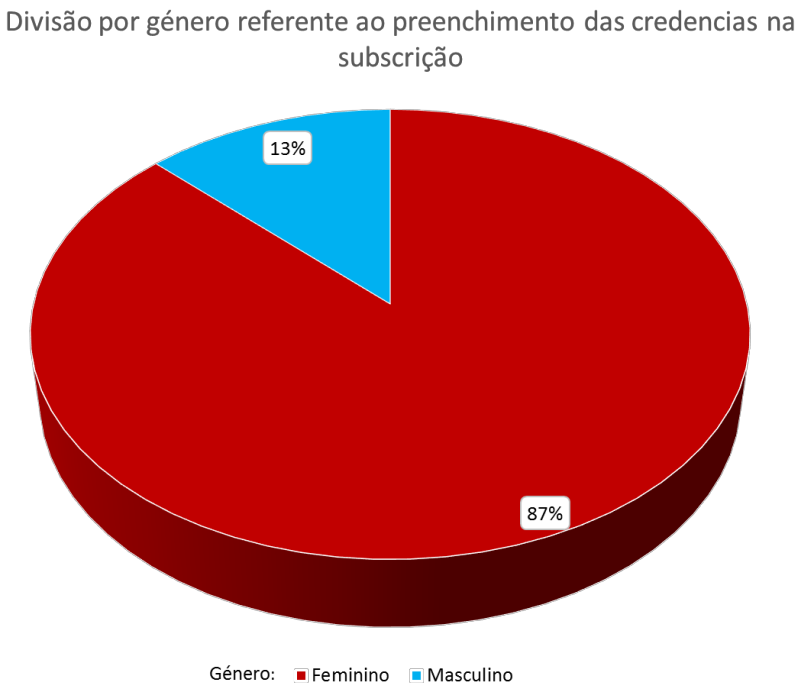


Figura 41 - Percentual por género do preenchimento das credenciais

O que se verifica é que além do resultado global de subscrição da *newsletter* ter sido feito maioritariamente por pessoas do sexo feminino, foram também elas, as responsáveis pelo maior preenchimento dos campos referentes as credenciais de acesso, representando 87% do total de pessoas que inseriram estes dados, como se pode ver na Figura 41.

A análise por género e idade é também relevante para perceber que faixa etária divulgou os dados. O resultado desta análise é ilustrado na Figura 42. Pela figura pode-se ver que em todas as faixas etárias, as mulheres tiveram uma percentagem superior à dos homens. Agrupando as quatro primeiras faixas etárias obtém-se 86,2% do total de pessoas, ou seja mais de dois terços dos subscritores que cederam essas informações, situam-se em idades inferiores a 40 anos. Entre os quais, 73,4% são mulheres. Isso mostra, de acordo com o estudo, que as mulheres mais jovens aderem mais facilmente e de forma mais descuidada a esse tipo de solicitações.

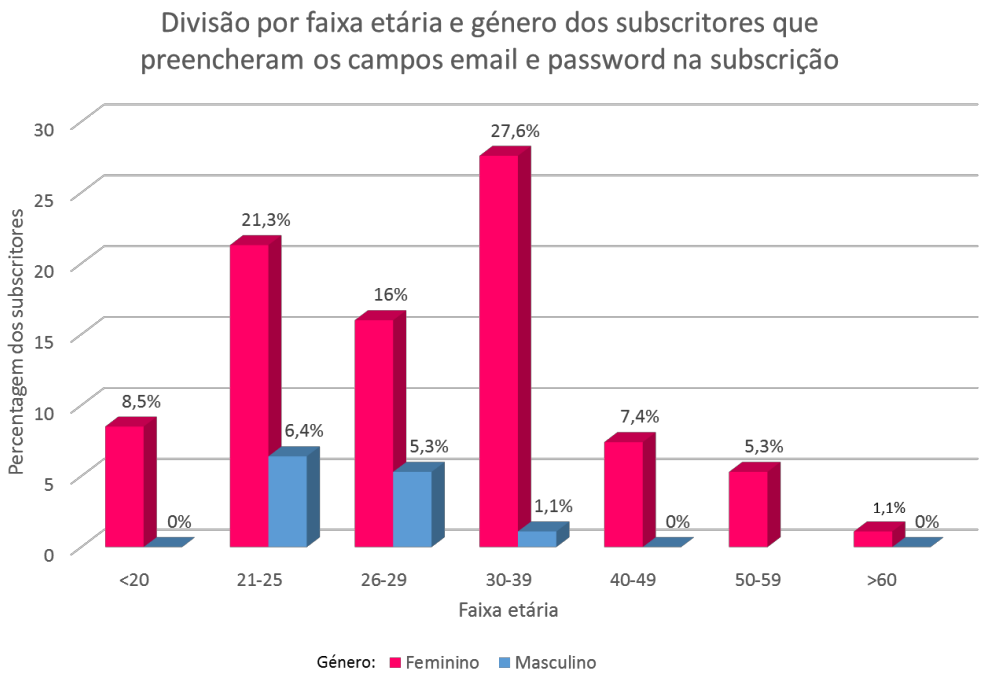


Figura 42 - Percentual por faixa etária e género do preenchimento das credenciais na subscrição

4.2.2.2. Resultados referentes às credenciais válidas

Sempre que um subscritor do Blogue Pura Saúde preenchia os campos *email* e *password*, o sistema despoletava uma verificação automática para verificar se as credenciais eram as mesmas. A verificação *online* baseou-se nos mecanismos de autenticação como o OAuth e SDKs disponíveis para um vasto conjunto de serviços (dropbox, facebook, gmail). Assim que um utilizador escolhia a forma de registo, tirando partido de contas já disponíveis, a aplicação de teste intercetava os dados inseridos e via API do OAuth ou SDK, acedia normalmente ao serviço para verificar o retorno da API. Desta forma, foi possível verificar a validade das credenciais junto de outros serviços (email, redes sociais, contas de serviços cloud). Após verificação, as credenciais eram descartadas pelo sistema.

Através da verificação automática às credenciais, verificou-se que 87% das pessoas que preencheram os campos *email* e *password,* tiveram um resultado positivo. Ou seja, 87% dessas pessoas utilizaram um endereço de *email* e *password* válidos e utilizados para outros serviços, como por exemplo, email pessoal, como se pode observar na Figura 43.

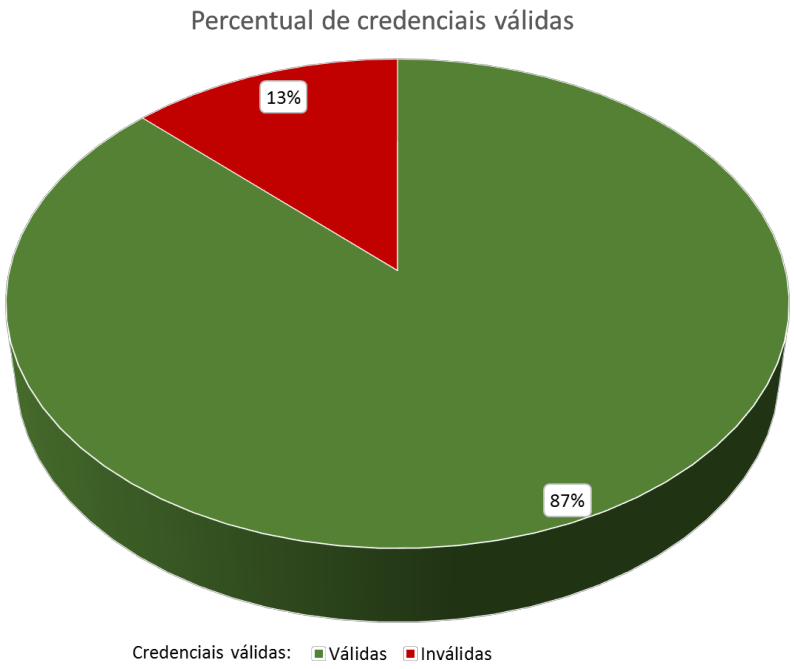


Figura 43 - Percentual de credenciais válidas

Na Figura 44 é ilustrada a divisão por género das pessoas que inseriram as credenciais de acesso válidas.

Figura 44 - Percentagem de credenciais válidas por género

Como se pode ver pela Figura 44, a percentagem de mulheres que disponibilizaram as suas credenciais de acesso é bastante elevada, chegando a atingir 86% do total de credenciais válidas. Uma análise mais fina revela as faixas etárias das pessoas que inseriram credenciais válidas no blogue. Os resultados desta análise mais fina são ilustrados na Figura 45.

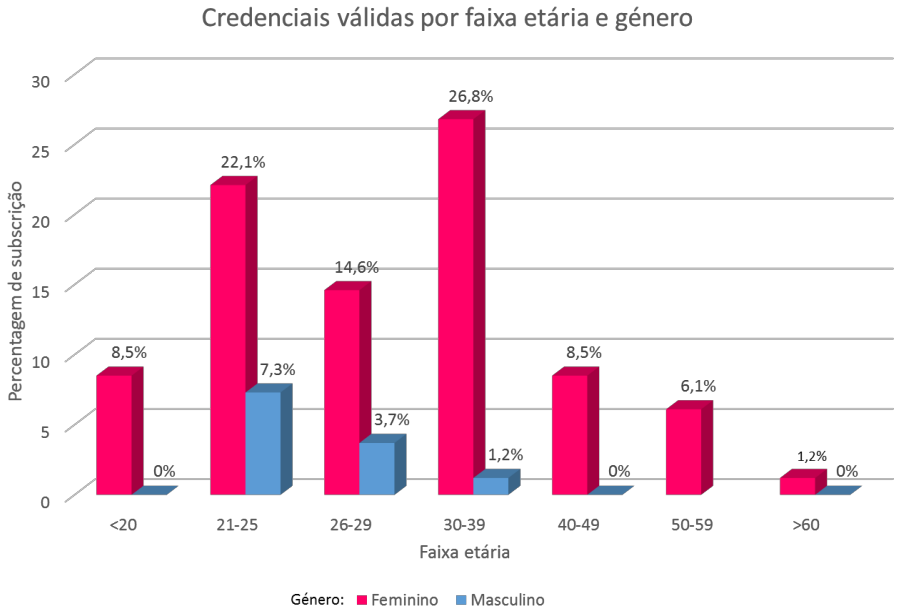


Figura 45 - Credenciais válidas por faixa etária e género

Como se verifica pela Figura 45, as mulheres possuem um valor superior ao dos homens, verificando esta situação em todas as faixas etárias. Ao agrupar o resultado das quatro primeiras faixas etárias, ou seja, mulheres com idade até aos 39 anos, o valor da percentagem de credenciais com resultado positivo é de 72%.

4.3. Valor referencial dos dados recolhidos no *site*

A recolha de dados, aparentemente inofensiva e voluntária por parte dos utilizadores, revela uma falta de consciência sobre a utilização da Internet. Verifica-se pelos resultados apresentados que foi relativamente fácil ao engenheiro social aproximar-se de um vasto conjunto de pessoas. Mais tarde abordou essas pessoas, partilhando informação, que à partida seria útil para todos. Ainda que de credibilidade duvidosa para muita gente da área da informática, o blogue acabou por ter adesão de várias pessoas e algumas das quais subscreveram a *newsletter* indicando dados pessoais entre os quais credenciais de acesso válidas.

Utilizando os dados obtidos e sem considerar nesta fase o potencial de exploração tirando partido das credenciais de acesso, utilizaram-se ferramentas para quantificar o valor dos dados recolhidos, isto é, quanto é que um atacante poderia ganhar com os dados.

Relembra-se que a subscrição da *newsletter* do Blogue Pura Saúde obteve a adesão de 220 pessoas. Para analisar qual o valor monetário dos dados no mercado negro, foram utilizadas duas fontes. A primeira fonte [49] é uma calculadora que mostra o valor individual que cada informação pode ter no mercado negro. A segunda fonte é a de um *site* disponível em [50] que mostra os valores dos dados em conjunto e que valor poderiam ter ao serem vendidos no mercado negro do Brasil, da Rússia ou da China.

A Figura 46 mostra a calculadora utilizada para o cálculo do valor dos dados recolhidos no *site*, caso estes fossem vendidos no mercado negro. De acordo com a calculadora, o valor das informações é:

- Morada = 0,50$
- Código postal = 0,50$
- Data de Nascimento = 2,00$
- Telemóvel = 10,00$

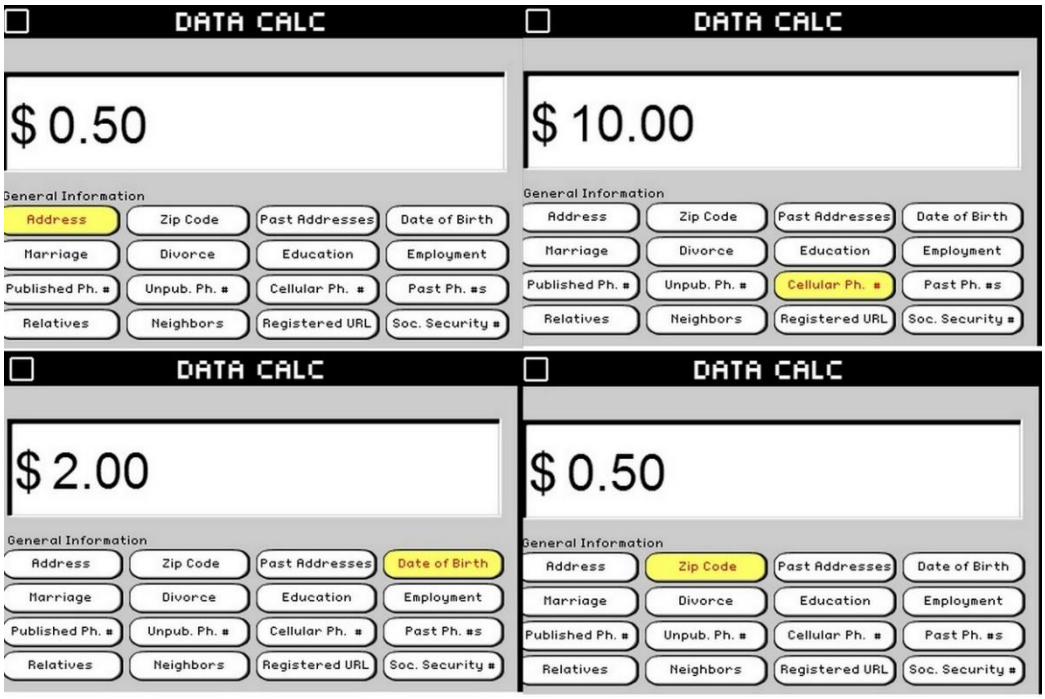


Figura 46 - Calculadora de dados

De acordo com o *site* da calculadora [49], nos EUA, os dados indicados mais o número de segurança social são suficientes para a abertura de uma nova conta bancária. Com a

calculadora, e tomando por base o número de preenchimentos dos campos no formulário de subscrição da *newsletter,* o valor dos dados recolhidos, tal como apresentado na Tabela **1** pode ascender a 2.010 dólares.

Campo do formulário	Quantidade	Valor ($)	Subtotal ($)
Morada	220	0,50	110,00
Código Postal	220	0,50	110,00
Data de Nascimento	220	2,00	440,00
Telemóvel	135	10,00	1350,00
Valor Total			**2010,00**

Tabela 1 - Cálculo do valor dos dados recolhidos

Para a segunda fonte do cálculo do valor dos dados recolhidos foi utilizado o *site* Trendmicro [50] como referência. O *site* refere o mercado negro global de dados pessoais roubados. De acordo com a fonte, cada tipo de dados possui um preço diferente e são vendidos de forma agrupada. A Figura 47 mostra o valor da informação em três países diferentes: Brasil, China e Rússia.

Figura 47 - Valor da informação no mercado negro por país

Como se verifica pela Figura 47, o valor da informação varia de país para país. A quantificação dos valores para os dados obtidos não é linear, na medida em que são referidos conjuntos de dados sem especificar o tamanho desse conjunto. Contudo e para efeitos de exercício se considerarmos que na China, um conjunto contém 10 credenciais, e o número de credenciais validadas no Blogue Pura Saúde foi 84, teríamos aproximadamente o valor de 8 x 163 = 1.304,00$.

Se considerarmos uma lista de números de telemóveis, que no Brasil vale entre 290 e 1236 dólares, composta por 50 números e assumindo o valor de 290$ (valor mais baixo), então teríamos pelo menos duas listas para vender (135 números) o que daria 580,00$.

Considerando a facilidade em obter estes dados e os valores praticados no mercado negro, o negócio de roubo de informações é apetecível. A única forma de reduzir este negócio é a consciencialização por parte das pessoas. Pessoas mais informadas vão ter mais cuidado no tipo de informação que divulgam, protegendo-se diretamente e protegendo as organizações para as quais trabalham/cooperam.

4.4. Análise sobre os resultados obtidos

Ao analisar os resultados pode-se verificar que apenas com alguns pedidos de “amizade” foi possível extrair alguns dados relevantes dos utilizadores, como por exemplo, data de nascimento, local onde vive, fotos pessoais, local de trabalho, escola em que estuda, ambientes frequentados, amigos próximos, familiares, informações sobre viagens futuras. Ou seja, com todas essas informações disponíveis, é fácil para um engenheiro social fazer um pequeno estudo e ficar a conhecer os hábitos pessoais do utilizador em questão e com isso, estabelecer padrões sociais. Tal facilita a criação de um perfil de comportamento para iniciar uma aproximação com as pessoas com o objetivo de recolher outros dados relevantes para um eventual ataque no futuro. Um exemplo de tal prática foi noticiado pelo TechTudo em julho de 2011 [51]. De acordo com a notícia, o californiano George Bronk de 24 anos, foi condenado a quatro anos de cadeia após invadir o Facebook de várias mulheres. O *hacker* procurava no perfil das vítimas, pistas que o levassem a descobrir senhas de *emails* e posteriormente da própria máquina alvo.

As redes sociais oferecem mecanismos de privacidade e ainda um pequeno tutorial de como configurá-la. Verificou-se durante o estudo, que nem todos os utilizadores recorrem a mecanismos de privacidade disponíveis. E, apesar da maioria dos perfis analisados terem opções de privacidade ativadas, o que impedia que os seus dados fossem visualizados por utilizadores que não possuíam nenhum tipo de interação com eles, revelando alguma preocupação em proteger suas informações pessoais, tal facto não foi um impedimento. Um simples pedido de amizade, após aceite, revelou as informações anteriormente escondidas. Isto mostra que apesar dos mecanismos de proteção à informação disponibilizados pelas redes sociais, a ingenuidade, a curiosidade ou necessidade natural de querer “socializar” faz do ser humano o elo mais fraco na corrente de segurança, tornando a engenharia social um método perigoso e eficaz.

Verificou-se também, que existe facilidade em criar uma rede de amizades através dos amigos em comum. Ou seja, um desconhecido envia uma solicitação de amizade a alguém que aceita o pedido e a partir daí, o desconhecido pode enviar novos pedidos aos amigos desta pessoa e muito provavelmente estes amigos também aceitarão. Ao possuir um ou mais amigos em comum, o perfil deste desconhecido torna-se mais facilmente confiável, possibilitando a extensão da sua rede de amizades.

Em 2014 foi disponibilizado um estudo [52] sobre cibercrimes, realizado pelo FBI através do IC3. O estudo destaca os esforços do IC3 para prevenir e reduzir o impacto de crimes na Internet e revela o aumento do uso das redes sociais como fonte valiosa de captação de dados

pessoais para os criminosos. De acordo com este estudo[52], cresce também o número de queixas apresentadas por pessoas vítimas de fraude praticadas por engenheiros sociais. Os resultados obtidos e apresentados ao longo deste capítulo estão em sintonia com as conclusões dos estudos do FBI e IC3.

Ao comparar o resultado do estudo, utilizando para isso, o número de utilizadores que aderiram aos pedidos de amizade e que disponibilizaram os seus dados a desconhecidos nas redes sociais, com os números de vítimas queixosas de crimes na internet recolhidos pelo *report* apresentado em [52] agregados por género, verifica-se uma semelhança nos resultados. No *report* há uma pequena maioria masculina que apresenta queixa de ter sido vítima de um crime na Internet. Nos resultados que obtivemos também é visível que os homens estão mais predispostos a aceitar solicitações de amizades de pessoas desconhecidas, deixando assim, todas as suas informações visíveis. A Figura 48 dá a conhecer mais em concreto os resultados obtidos com o cenário um e os resultados apresentados do *report* divulgado em [52].

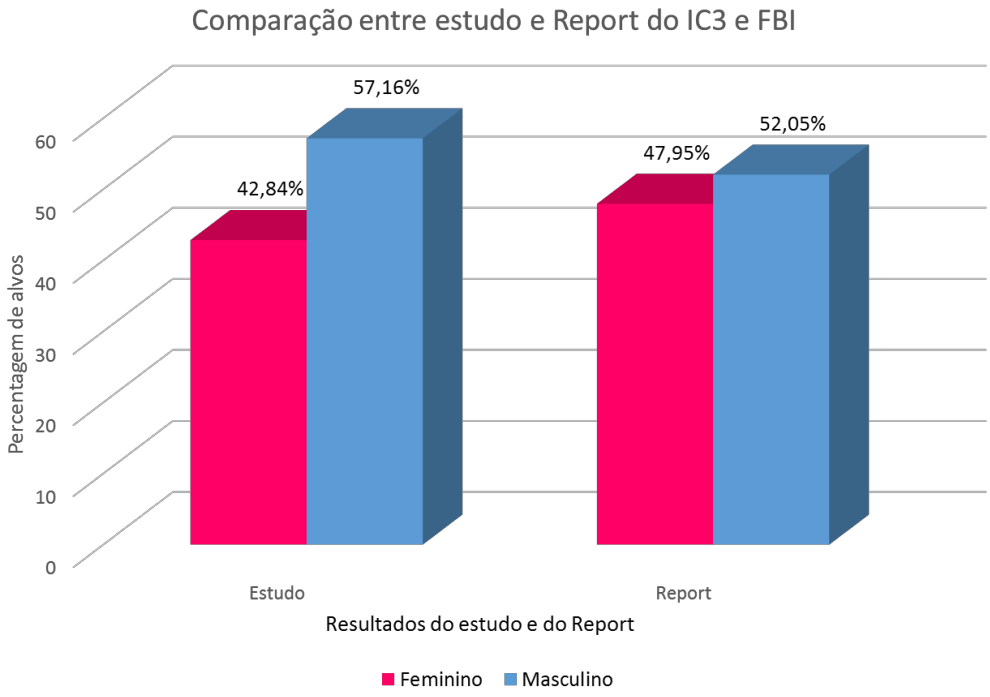


Figura 48 - Comparação entre o relatório do FBI e IC3 e os resultados obtidos no âmbito do estudo

Para efeitos de comparação com o *report* indicado, foi feita a agregação dos resultados obtidos com o estudo por faixas etárias equivalentes. Esta agregação, é ilustrada na Figura 49. Como se pode ver pela figura, verificaram-se resultados semelhantes nas faixas etárias superiores a 20 anos. O resultado obtido nos menores de 20 anos, apresentou uma disparidade. No *report* do FBI/IC3, o número de jovens que apresentam queixa junto aos

órgãos competentes e portanto, assumem terem sido vítimas de um crime na internet é a mais baixa entre as faixas etárias mostradas. Já no estudo, a percentagem dos menores de 20 anos é bastante elevada. Este estudo não permitiu concluir as razões da diferença naquela faixa etária, pelo que teriam que ser desenvolvidos outros estudos, por exemplo, inquéritos direcionados a este grupo, no sentido de confirmar a tendência e a partir daí identificar as suas causas e adotar um plano de ação de consciencialização.

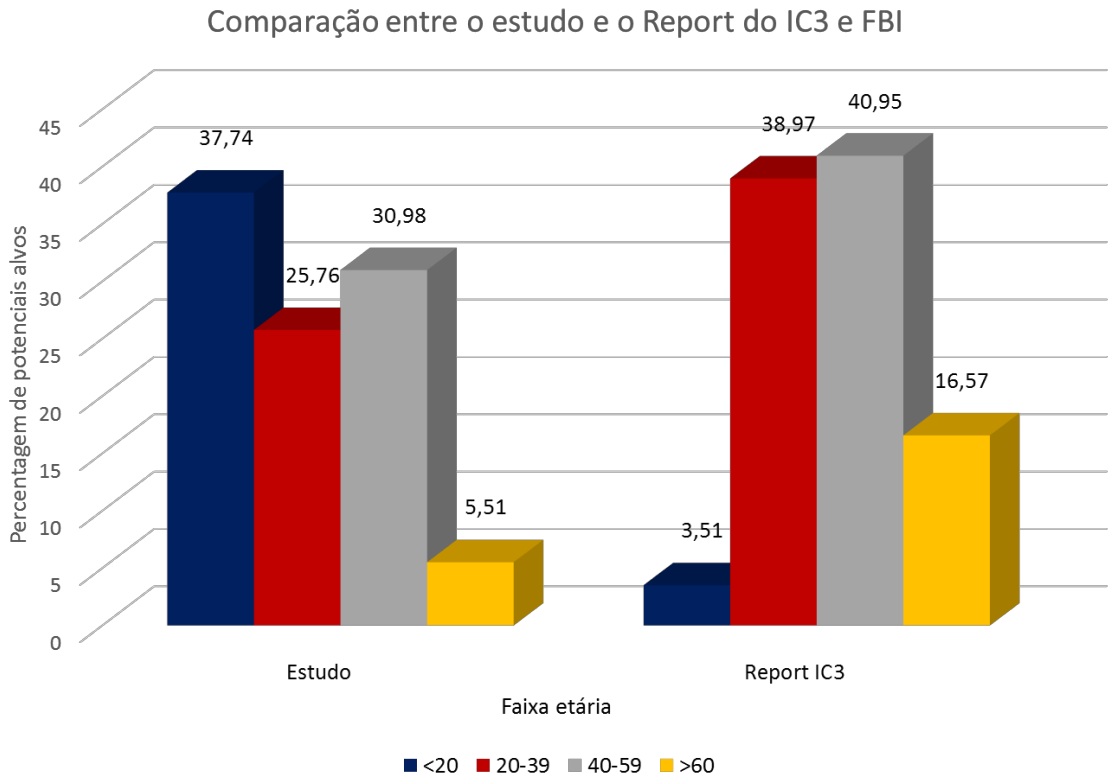


Figura 49 - Comparação entre o estudo e o Report do IC3/FBI por faixa etária

O relatório de ameaças à segurança na internet realizado pela Symantec [40] revela que o número de dados acedidos sem consetimento aumentou 62% em 2013 comparados com 2012. De acordo com o relatório, também se verificou um crescimento nos ataques de phishing em que muitas das tentativas de ataque consistem em páginas de login falsas para redes sociais populares. As credenciais de *login* parecem ser uma das principais informações procuradas pelos atacantes com o objetivo de utilizar estas contas para espalhar campanhas de *spam* e *phishing* ou aceder a sistemas para obter informação mais sensível. O relatório revela ainda que 12% dos entrevistados disseram já terem tido suas contas sociais invadidas. Um outro relatório da área é da Ofcom [53] realizado em 2013. Este relatório, mostra que 55% das pessoas utilizam a mesma *password* para mais de um serviço. Esta é uma má prática no que diz respeito à segurança dos dados, pois se o acesso de uma conta for comprometida, o atacante poderá ter acesso a todos os serviços que utilizem esta mesma *password*. Ao

confrontar os resultados obtidos no cenário 2 do estudo com os destes dois últimos relatórios, verifica-se que há uma semelhança nos números obtidos.

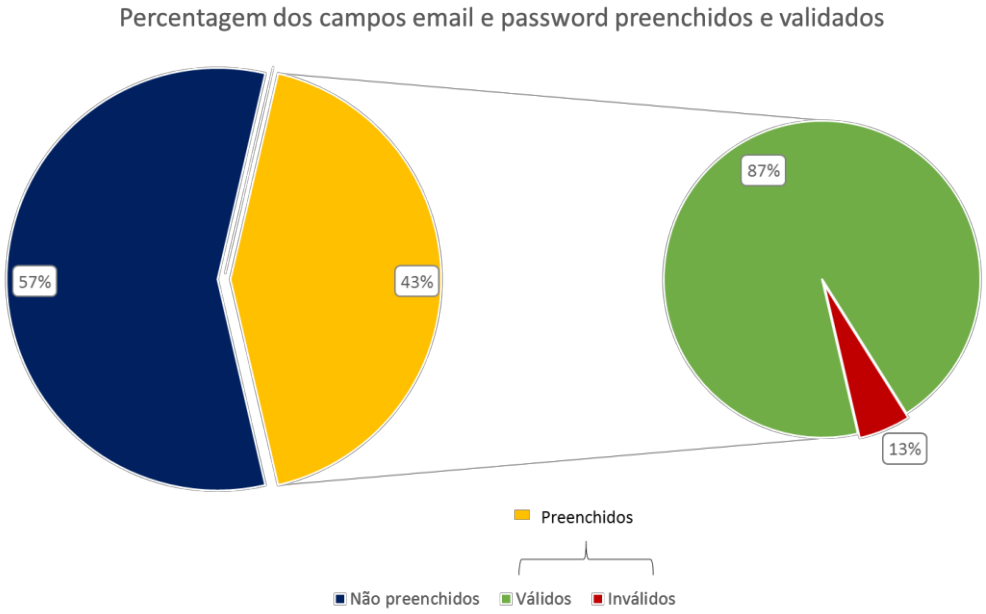


Figura 50 - Percentagem dos campos email e password preenchidos e validados

5. Conclusão

A preocupação com as questões da segurança da informação tornou-se indispensável para as organizações e para as pessoas. A proteção dessa informação ainda está muito centrada em dispositivos tecnológicos para a deteção e prevenção de ataques. Estes sistemas são muito importantes, mas incapazes de lidar com uma superfície de ataque que é cada vez mais explorada para levar a cabo ataques informáticos. Esta superfície é o ser humano que pelas mais diversas razões e motivações representa o elo mais fraco da segurança de informação. É o elo mais fraco porque dada a natureza humana é o mais difícil de tratar. Conscientes desta limitação, os atacantes também referidos por engenheiros sociais exploram estas vulnerabilidades para levar a cabo os seus ataques. As organizações de maior ou menor intensidade reconhecem o problema e urge a implementação de práticas de segurança eficazes que permitam lidar com este problema. Para lidar com eles de forma eficaz é fundamental conhecer a sua dimensão.

Este trabalho abordou a questão da engenharia social e suas práticas, tendo como foco o fator humano na segurança da informação. Tal como foi referido a engenharia social é um tipo de ataque que aproveita da vulnerabilidade das pessoas para obter informações confidenciais ou acesso não autorizado a sistemas, e por isso muito difícil de controlar. Tomar consciência da sua existência, educar e treinar as pessoas para a sua ocorrência e impactos são ações que devem ser consideradas para minimizar os riscos e para definir procedimentos de resposta a incidentes de segurança informática. Por isso, em concreto, este trabalho focou a componente de análise comportamental, isto é, estudou através de dois cenários como é que as pessoas lidam com a abordagem e metodologias usadas pelos engenheiros sociais. O teste aos diferentes públicos, no que diz respeito à sua manipulação por via da engenharia social, permitiu analisar o nível de consciencialização das pessoas sobre os perigos que correm na Internet. Pelos resultados percebeu-se que há diferentes comportamentos mediante o grupo etário e o género em análise. Por exemplo, no cenário 1 houve uma adesão maior de utilizadores masculinos, quase 60%, e também de utilizadores até 20 anos, com cerca de 39% do total. Observou-se também que não foi difícil criar uma rede de amigos, pelo contrário, houve mais pedidos de amizade recebidos que enviados (68% contra 32%), e ao fim de 45 dias, já haviam aderido 3.211 pessoas aos quatro perfis criados no âmbito do estudo. O nível de interação entre os perfis e seus “amigos”, (1.191), revela uma predisposição das pessoas se relacionarem com desconhecidos, nas redes sociais. Esses números confirmam que as redes sociais são para os engenheiros sociais uma grande base de dados, com informações à disposição de todos. Sejam quais forem os motivos que levam as pessoas a

divulgarem tantas informações, e a disponibilizarem-nas a desconhecidos, é evidenciado o despreparo dos utilizadores em relação à segurança da informação.

No cenário 2, verificou-se que, ao contrário do cenário 1, o número de subscritores do sexo feminino foi bastante superior ao masculino, quase 80% (a este fenómeno não será alheio o conteúdo do blogue mais vocacionado para o público feminino). Verificou-se haver uma percentagem considerável de subscritores que preencheram os campos *email* e *password* (43%). Foram também as mulheres que mais preencheram estes campos, cerca de 87%. Outro dado muito relevante, é o de que 87% das credenciais de acesso introduzidas no blogue serem válidas em outro serviço, o que levanta sérias questões sobre os comportamentos das pessoas perante um pedido de preenchimento de dados *online*.

Considerando os resultados obtidos e conhecendo-se o comportamento de risco das pessoas, permite a elaboração de planos de educação e treinos específicos. Estes planos, ao serem focados no público-alvo, potenciam o alcance da consciencialização sobre os perigos a que estão expostos e do conhecimento das principais estratégias utilizadas pelos engenheiros sociais. Para que estes planos sejam aplicados no terreno e tenham resultados, é importante envolver diversas entidades (empresas, municípios, escolas, …) na implementação das políticas de segurança através da informação e sensibilização dos respetivos dirigentes e dos responsáveis dos serviços especializados nas tecnologias de informação e comunicação a respeito das vulnerabilidades dos utilizadores e dos perigos que essas vulnerabilidades comportam para a segurança das informações.

O estudo aqui realizado é importante a diversos níveis. Desde logo permite ter uma ideia concreta sobre os comportamentos humanos e perceber a sensibilidade das pessoas perante uma potencial abordagem de um engenheiro social. De forma mais direta, a metodologia usada e os resultados servem como instrumento facilitador na definição de programas de educação e treino específicos, tendo em consideração as vulnerabilidades dos públicos-alvo, de maneira a prevenir uma das formas mais comuns de fraude, a engenharia social, que afeta o componente mais frágil do sistema, o utilizador. Desde logo, se podem desenhar programas orientados à adoção de princípios de “higiene computacional” capazes de refletir no público-alvo o impacto individual da ciber segurança. Programas vocacionados para a “cidadania digital” capazes de evidenciar os comportamentos individuais e coletivos na segurança do ciber espaço. E numa vertente mais organizacional, o desenho de cursos vocacionais ao desenvolvimento e aplicação de políticas de ciber segurança eficazes.

5.1. Trabalho futuro

Um possível trabalho futuro que permitiria validar a metodologia usada seria realizar o estudo numa organização real. Os resultados obtidos a partir de uma organização permitiam estender a metodologia do engenheiro social por forma a perceber até que nível de intrusão se conseguiria chegar. O teste a diferentes perfis dentro da empresa permitiria também perceber o nível de consciência das pessoas e identificar perfis alvo de treino. Os exercícios de treino e materiais produzidos podiam ser criados em função das especificidades desses mesmos perfis contribuindo para uma melhor interiorização das boas práticas. A conceção de programas formativos com base nos resultados obtidos e no aprofundamento do estudo é também uma área a explorar.

6. Bibliografia

[1] E. d. Argaez. "Internet World Stats". Internet: http://www.internetworldstats.com/stats.htm. [Oct, 2015].

[2] B. Krebs. "The Case for N. Korea's Role in Sony Hack". Internet: http://krebsonsecurity.com/2014/12/the-case-for-n-koreas-role-in-sony-hack/. [Jul, 2015].

[3] V. Staff. "The Ashley Madison hack: everything you need to know". Internet: http://www.theverge.com/2015/8/19/9178965/ashley-madison-hacked-news-data-names-list. [Aug, 2015].

[4] TVI24. "Conheça as localidades com maior número de traidores". Internet: http://www.tvi24.iol.pt/tecnologia/ashley-madison/conheca-as-localidades-com-maior-numero-de-traidores?utm_campaign=ed-tvi24&utm_source=facebook&utm_medium=social&utm_content=-post. [Oct, 2015].

[5] L. Kessem. "Carbanak: How Would You Have Stopped a $1 Billion APT Attack?". Internet: https://securityintelligence.com/carbanak-how-would-you-have-stopped-a-1-billion-apt-attack/. [Feb, 2015].

[6] R. Pais, F. Moreira, and J. Varajão, "Engenharia Social (ou o carneiro que afinal era um lobo)," ed: Almedina, 2013, p. 11.

[7] M. C. P. Peixoto. (2006). *Engenharia social e segurança da informação na gestão corporativa*. Available: https://books.google.pt/books?id=qY5ePgAACAAJ

[8] U. Corporation. Feb, 2005, Política Nacional de Segurança da Informação. Available: https://www.fccn.pt/fotos/editor2/Seguran%C3%A7a/CERT/PolSegRCTS1112/ensi_politica_nacional_de_seguranca_da_informacao.pdf

[9] J. L. P. Marciano, "Segurança da Informação - Uma abordagem social," Doutor em Ciência da Informação, Ciência da Informação e Documentação, Universidade de Brasília, 2006.

[10] C. B. Alves, *Segurança da Informação vs. Engenharia Social: Como se proteger para não ser mais uma vítima*: Clube de Autores, 2010, p. 128.

[11] I. G. Business, "IBM Global Business Security Index : Surge in Viruses and Worms Targeting Mobile Devices, Satellite Communications Anticipated," IBM Global Business, 2005, Available: https://www-03.ibm.com/press/us/en/pressrelease/7512.wss.

[12] I. G. Services, "Stopping insider attacks: how organizations can protect their sensitive information," IBM Global Services, 2006, Available: https://www-935.ibm.com/services/us/imc/pdf/gsw00316-usen-00-insider-threats-wp.pdf.

[13] J. Berti and M. Rogers, "Social engineering: The forgotten risk," in *Information Security Management Handbook*. vol. 3, H. F. Tipton and M. Krause, 4 ed, New York: Auerbach, 2004, pp. 51-53.

[14] O. Dictionaries. "Hacker". Internet: http://www.oxforddictionaries.com/definition/english/hacker. [Fev, 2015].

[15] K. Mitnick and W. Simon, *Mitnick: A arte de enganar*. Brasil: Pearson Education, 2002, p. 286.

[16] J. J. C. Cortela, "Engenharia Social Aplicada ao Facebook," Licenciado em Ciência da Computação, Departamento de Computação, Universidade Estadual de Londrina, Londrina, PR, 2013.

[17] E. E. d. Araujo, "A Vulnerabilidade Humana na Segurança da Informação," Licenciatura Sistemas de Informação, Faculdade de Ciências Aplicadas de Minas, Uberlândia-MG, 2005.

[18] C. Hadnagy, *Social engineering: The art of human hacking*. Indianapolis, IN: Wiley Publishing, Inc, 2011, p. 477.

[19] M. Zager, "Who are the hackers?," *Infosec News,* p. 3, 2002.

[20] A. Marcelo and M. Pereira, *A Arte de Hackear Pessoas*. Rio de Janeiro: Brasport, 2005.

[21] N. C. C. Corrêa, "O uso indevido da Engenharia Social na Informática," Licenciatura em Sistemas de Informação, Centro Universitário do Maranhão, São Luis, MA, 2006.

[22] B. Oosterloo, "Managing Social Engineering Risk," Master Industrial Engineering and Management, University of Twente, Enschede, Netherlands, 2008.

[23] Y. Lafrance, "Psychology: A Precious Security Tool," *SANS Institute,* p. 27, 2004.

[24] M. Allen, "Social Engineering: A Means To Violate A Computer System," *SANS Institute,* p. 13, 2006.

[25] C. Jones, "Social Engineering: Understanding and Auditing," *SANS Institute,* p. 22, 2003.

[26] K. C. Redmon, "Mitigation of Social Engineering Attacks in Corporate America " Graduate Student in Information Security, East Carolina University, Greenville, 2005.

[27] M. Corporation, "How to Protect Insiders from Social Engineering Threats: Midsize business security guidance.," *Microsoft Corporation,* p. 33, 2006.

[28] W. Arthurs, "A Proactive Defence to Social Engineering," *SANS Institute,* p. 6, 2001.

[29] R. Bearman. 2004, A guide to social engineering. 6. Available: http://obm.page4.me/_blog/2011/05/13/a-guide-to-social-engineering/

[30] Microsoft. "O que é o phishing?". Internet: https://www.microsoft.com/pt-pt/security/resources/phishing-whatis.aspx. [Fev, 2015].

[31] S. Granger, "Social Engineering Fundamentals, Part I: Hacker Tactics," *Infocus,* p. 3, 2001.

[32] A. Dolan, "Social Engineering," *SANS Institute,* p. 15, 2004.

[33] S. Granger, "Social engineering reloaded," *Infocus,* p. 5, 2006.

[34] Kaspersky. "O que é um Trojan?". Internet: http://www.kaspersky.com/pt/internet-security-center/threats/trojans. [Oct, 2015].

[35] A. Rohr. "G1 Explica: o que é um keylogger?". Internet: http://g1.globo.com/tecnologia/blog/seguranca-digital/post/g1-explica-o-que-e-um-keylogger.html. [Oct, 2015].

[36] D. Gragg, "A Multi-Level Defense Against Social Engineering," *SANS Institute,* p. 18, 2002.

[37] Vigilante. "Social Engineering". Internet: http://blackh4t.persiangig.com/document/S.E/VIGILANTe%20-%20Internet%20Security%20-%20Social%20Engineering.htm. [No date].

[38] J. J. RUSCH. "The Social Engineering of Internet Fraud". Internet: http://www.isoc.org/isoc/conferences/inet/99/proceedings/3g/3g_2.htm. [No date].

[39] C. Point. 2011, The Risk of Social Engineering on Information Security. 7. Available: http://www.greycastlesecurity.com/resources/documents/The_Risk_of_Social_Engineering_on_Information_Security_09-11.pdf

[40] Symantec, "Internet Security Threat Report," *Symantec Corporation,* vol. 19, p. 98, 2014.

[41] Microsoft. "O que é ransomware?". Internet: http://www.microsoft.com/pt-br/security/resources/ransomware-whatis.aspx. [Oct, 2015].

[42] G. Gusmão. "iCloud pode ter causado parte do vazamento de fotos íntimas". Internet: http://exame.abril.com.br/tecnologia/noticias/icloud-pode-ter-causado-parte-do-vazamento-de-fotos-intimas. [Aug, 2015].

[43] D. N. Portugal. "Predador sexual de 25 anos em prisão preventiva por abuso de duas crianças". Internet: http://www.dn.pt/portugal/interior/predador-sexual-de-25-anos-em-prisao-preventiva-por-abuso-de-duas-criancas-4224118.html. [Aug, 2015].

[44] W. Organisation. "Wikileaks". Internet: https://wikileaks.org/index.es.html. [Aug, 2015].

[45] F. Mariano. "Snowden ainda está na Rússia". Internet: http://www.jn.pt/PaginaInicial/Mundo/Interior.aspx?content_id=3290073.

[46] P. Uchoa. "Mercosul reforça na ONU indignação com espionagem dos EUA". Internet: http://www.bbc.com/portuguese/noticias/2013/08/130730_patriota_eua_mdb_pu. [Sept, 2015].

[47] M. F. Assunção, *Segredos do Hacker Ético*, 4 ed.: Visual Books, 2011.

[48] P. F. Fonseca, "Gestão de Segurança da Informação: O Fator Humano " Pós Graduação em Redes e Segurança de Computadores, Universidade Católica do Paraná Curitiva, PN, 2009.

[49] B. d. Costa, J. Schulte, and B. Singer. "SWIPE". Internet: http://archive.turbulence.org/Works/swipe/main.html. [Oct, 2015].

[50] TRENDMICRO. "A Global Black Market for Stolen Personal Data". Internet: http://www.trendmicro.com/vinfo/us/security/special-report/cybercriminal-underground-economy-series/global-black-market-for-stolen-data/#section-5. [Oct, 2015].

[51] R. Porphírio. "Homem que usou o Facebook para perseguir mulheres em 17 estados é condenado". Internet: http://www.techtudo.com.br/noticias/noticia/2011/07/homem-que-usou-o-facebook-para-perseguir-mulheres-em-17-estados-e-condenado.html. [Jul, 2015].

[52] I. C. C. Center, "Internet Crime Report," 2014, Available: https://www.fbi.gov/news/news_blog/2014-ic3-annual-report.

[53] Ofcom. "Adults Media Use and Attitudes Report 2013". Internet: http://media.ofcom.org.uk/news/2013/uk-adults-taking-online-password-security-risks/. [Oct, 2015].