ACADEMIA MILITAR

Mestrado em Ciências Militares na Especialidade de Infantaria

RELATÓRIO CIENTÍFICO FINAL DO TRABALHO DE INVESTIGAÇÃO APLICADA

Processo de *Awareness* dos Utilizadores nas Redes Militares

Autor: Aspirante Aluno de Infantaria Gustavo Emanuel Marques Francisco

Orientador: Tenente-Coronel de Infantaria (Doutor) José Carlos Lourenço Martins

Lisboa, junho de 2016

ACADEMIA MILITAR

Mestrado em Ciências Militares na Especialidade de Infantaria

RELATÓRIO CIENTÍFICO FINAL DO TRABALHO DE INVESTIGAÇÃO APLICADA

Processo de *Awareness* dos Utilizadores nas Redes Militares

Autor: Aspirante Aluno de Infantaria Gustavo Emanuel Marques Francisco

Orientador: Tenente-Coronel de Infantaria (Doutor) José Carlos Lourenço Martins

Lisboa, junho de 2016

DEDICATÓRIA

Àqueles que sempre me apoiaram!

À minha família e amigos.

AGRADECIMENTOS

Um Trabalho de Investigação Aplicada é, sem dúvida, o mais importante na vida escolar de um futuro oficial do quadro permanente e, será quase impossível a realização do mesmo, sem a devida ajuda, quer de pessoas, quer de instituições.

Assim sendo, queria começar por agradecer ao meu Orientador, Tenente Coronel de Infantaria José Carlos Lourenço Martins, pelo seu tempo disponível, mesmo sendo escasso, pelo aconselhamento semanal a todas as minhas decisões, a prontidão para responder a todas a minhas questões e pedidos, a oferta do espaço de tempo para a execução do trabalho de campo durante a cadeira do qual é docente. Pela sua preocupação constante e por ter apostado em mim nesta tarefa complexa e trabalhosa, pois, sem esta ajuda, dedicação e empenho, nada disto seria possível de se concretizar.

Ao meu Diretor de Curso, Tenente-Coronel de Infantaria António Luís Morais Pinto de Oliveira que, da mesma forma que o meu orientador, demonstrou grande preocupação e disponibilidade durante todo o período de execução do Trabalho de Investigação Aplicada, como fora dele, com o objetivo de "formar melhores Oficiais de Infantaria" como sempre disse, e por isto obrigado.

Ao Capitão de Engenharia Militar, Luís Filipe Marques dos Santos Conceição por, para além do seu intenso trabalho na Academia Militar, mostrar sempre disponibilidade, quando necessário, em todos os meus problemas, quer seja na entrega de questionários em tempo oportuno, quer seja em organizar um espaço de tempo com todas as companhias para realização dos mesmos. Aos restantes Capitães das várias companhias, João Cardoso, Francisco Carreira e Nuno Bento, um obrigado pelo apoio prestado em tempo.

A todos os Cadetes, por terem colaborado com os questionários, mesmo em período de fora de horas do horário escolar.

À minha Família e Amigos pelo apoio moral e compreensão durante toda esta fase, que, apesar de não terem competências para o desenvolvimento da investigação, mostraram todo apoio e mais algum.

RESUMO

O presente trabalho de investigação aplicada tem como titulo "Processo de *Awareness* dos Utilizadores nas Redes Militares", com o intuito de "identificar a forma mais eficiente e eficaz de efetuar um *design* de um processo de *awareness* de forma a sensibilizar os utilizadores do sistema de *e-mail* do Exército para os ataques de *phishing"* que é o objetivo desta investigação.

Por este motivo, de início foram selecionados objetivos específicos que remetem para este principal. Foi definido que precisamos de conhecer as principais teorias comportamentais que influenciam o sucesso dos ataques de *phishing,* de forma a perceber e combater estes mesmos.

Foi, também, necessário perceber quais os principais métodos ou técnicas de ensino de atitudes, para possibilitar a sensibilização dos utilizadores, como também era necessário definir o meio de *awareness* para executar esta mesma. Por último, era necessário o processo de *awareness*, portanto, precisamos de critérios de avaliação e, para isso, é importante definir estes mesmos para validar a investigação.

Para responder a estes quatro objetivos específicos e ao objetivo geral da investigação foi criada a questão central do trabalho que é "Como efetuar o *design* de um processo de *awareness* para o Exército que reduza o impacto dos ataques de *phishing* executados através do seu sistema de *e-mail*?"

Devido ao carácter teórico-prático desta investigação, foi decidido que o método de investigação seria o Hipotético-Dedutivo, e o método de procedimento seria o Estudo de Caso.

Foi uma investigação exploratória, utilizando as técnicas de pesquisa bibliográfica e análise documental para executar uma revisão de literatura completa com o intuito de apoiar a investigação, como, também, fundamentar todo o trabalho de campo realizado.

Para a realização deste estudo, foi necessário estudar a temática Segurança da Informação, já que esta suporta a investigação. Para existir segurança da informação é necessário que as propriedades da segurança da informação se mantenham preservadas, isto é, a confidencialidade, a integridade e a disponibilidade

O trabalho de campo consistiu em duas partes, a construção dos questionários e da apresentação de sensibilização e a sua aplicação e avaliação (outputs da investigação). Estes produtos foram usados na sessão de sensibilização através da aplicação do questionário de aferição seguido da apresentação de sensibilização, e terminando com o questionário de validação (processo de *awareness*).

Conseguiu-se, após a sensibilização, através do processo de *awareness*, que os elementos identificassem com maior rigor os ataques de *phishing*. Para isso utilizou-se, na sensibilização, o método de ensino ativo, que incorpora boas práticas para a construção de produtos de sensibilização, utilizando os estilos de aprendizagem auditivo, mecânico e visual, que permite alterar comportamentos.

Palavras-Chave: Segurança da Informação, Engenharia Social, Ataques de Phishing, Processo de awareness de segurança

ABSTRACT

This research work has the title “Processo de *Awareness* dos Utilizadores nas Redes Militares”, and the objective is to "identify the most efficient and effective way to make a design of an awareness process to raise awareness to phishing attacks, among users of the Army e-mail system "which is the goal of this research.

For this reason, at the beginning, we selected specific objectives that refer to this major objective.

We decided that we needed to know the main behavioral theories that influence the success of phishing attacks in order to understand and combat them. It was also necessary to know the main teaching methods of attitudes, since it was necessary for the teaching of users. It has also necessary to define the means to perform an awareness session. Finally, it was necessary to have an awareness process, so we needed some assessment criteria to validate the research.

To answer these four specific objectives and answer the major goal of the research, we created the central question of the work that is "How to make the design of an awareness process for the Army to reduce the impact of phishing attacks that run through the system of e-mail?"

Due to the theoretical and practical character of this investigation, it was soon decided that the method of investigation would be the Hypothetical-Deductive and the procedure method was the Case-Study.

It was an exploratory research, using the search of literature and analysis of documents to create a literature review that would support the research, as well to support throughout the fieldwork.

For this study, it was necessary to study the thematic of information security since it supports all the research. To have information security it is necessary that the properties of information remain preserved and they are confidentiality, integrity and availability.

The field work consisted in two phases, the construction of the questionnaires and of the awareness presentation and their implementation and evaluation (the research outputs).

These products were used in the awareness session by applying the assessment questionnaire followed by awareness presentation, and ending with the validation questionnaire (awareness process).

We succeeded, through the awareness process, on a more accurately identification of the phishing attacks by the cases studies. For this, it was used in the awareness process, active teaching method, which incorporates best practices for building products of awareness, using the styles of auditory learning, mechanical learning and visual learning, allowing the change of behaviors.

Key-Words: Information Security, Social Engineering, Phishing Attacks, Process of Security Awareness

ÍNDICE GERAL

ÍNDICE DE FIGURAS E QUADROS

Figuras

Quadros

ÍNDICE DE TABELAS E GRÁFICOS

Tabelas

Gráficos

LISTA DE ABREVIATURAS, SIGLAS E ACRÓNIMOS

APWG	Anti-Phishing Work Group
BPI	Banco Português de Investimento
CAL	Companhia de Alunos
CGD	Caixa Geral de Depósitos
CISSP	Certified Information Systems Security Professional
GNR	Guarda Nacional Republicana

EPÍGRAFE

"The *awareness* program must be the voice of reason and logic.
Start small and expand.
By the time the employees realize there is a security program,
it will already be part of the culture"
Thomas R. Peltier CISSP

INTRODUÇÃO

Este trabalho de investigação aplicada é o culminar do curso frequentado na Academia Militar, Mestrado Integrado em Ciências Militares com a especialidade de Infantaria. Tem como título "Processo de *Awareness* dos Utilizadores nas Redes Militares" e pretende-se, nesta parte inicial do trabalho, dar conhecimento sobre a temática abordada para melhor compreensão e facilitar a leitura deste trabalho.

Para poder formular um problema de investigação é primeiramente necessário definir alguns elementos como a justificação do tema:

> "Qualquer estudo deve apresentar-se como algo necessário. Portanto, o projeto de investigação deverá iniciar-se indicando as razões pelas quais a área de estudo foi escolhida, dando informação suficientemente detalhada sobre a problemática e o tópico a abordar e explicando porque é necessário fazer o estudo" (Barañano, 2004, p. 39).

Iniciando pela ordem de ideias anteriormente analisada, as razões por ter optado por esta área de estudo foi o meu gosto pelas áreas da informática, mais concretamente, numa das cadeiras do curso, a "Segurança da Informação, dos Sistemas de Informação e Ciberdefesa", onde me foi abordada a possibilidade de fazer um trabalho de investigação nesta área, ao qual não hesitei quando me foi dada a possibilidade de escolher.

Outro elemento fundamental para a minha escolha foi a importância crescente desta temática, dentro da organização militar e nas organizações civis. Sendo atualmente, o *Phishing* um ato criminal categorizado como um dos mais eficientes crimes nas redes de computadores (Salem, Hossain, & Kamala, 2010). Este é fundamental para o Exército Português, já que a ciberdefesa, no domínio da segurança e defesa do território nacional e dos cidadãos, se apresenta como de primeira prioridade, isto é, está relacionado com a defesa de interesses vitais, que têm subjacente um elevado perigo para a unidade política (Conceito Estratégico Militar, 2014).

Este estudo trata a Engenharia Social que é "uma metodologia que permite ao atacante ultrapassar os controlos técnicos através do elemento humano numa organização" (Applegate, 2009, pp. 40, Tradução Própria), mais especificamente, utilizando os ataques de

phishing através das mensagens de *e-mail*, que procuram na essência manipular o elemento humano.

Assim foram planeados, realizados e avaliados ações de *awareness* na Academia Militar, para permitir mitigar o impacto dos ataques de *phishing* realizados através do sistema de *e-mail* tendo em vista a identificação da forma mais eficiente e eficaz de sensibilizar os utilizadores do sistema de *e-mail* do Exército para este tipo de ataques, como para toda a banda de técnicas, utilizadas para obter informação restrita.

Este estudo apresenta um processo, que permite alertar os utilizadores sobre este assunto. Cuja principal finalidade é a diminuição do risco, através da sensibilização do Exercito Português para a necessidade da especialização na vertente da segurança da informação, já que com os ataques de *phishing,* os colaboradores podem ser manipulados e levados a divulgar informação classificada da organização, sem terem essa perceção.

Como objetivo geral de estudo, pretende-se então "identificar a forma mais eficiente e eficaz de efetuar um *design* de um processo de *awareness* de forma a sensibilizar os utilizadores do sistema de *e-mail* do Exército para os ataques de *phishing".*

Como objetivos específicos de investigação, foram identificados os seguintes:

- Definir as principais teorias comportamentais que influenciam o sucesso dos métodos de ataque de *phishing*;

- Identificar os principais métodos ou técnicas de ensino de atitudes que permitem alterar os comportamentos incorretos dos utilizadores face a um ataque de *phishing*;

- Identificar o principal meio para realizar as ações de *awareness*;

- Definir os principais critérios de avaliação, ou seja, de validação da eficácia e eficiência de uma ação de *awareness* ministrada.

De forma a responder a estes objetivos, levantou-se a pergunta de partida: "Como efetuar o *design* de um processo de *awareness* para o Exército que reduza o impacto dos ataques de *phishing* executados através do seu sistema de *e-mail*?"

Por último, este trabalho de investigação é constituído por quatro capítulos. No primeiro capítulo, revisão de literatura, dá a conhecer o "estado da arte", focando especialmente os principais conceitos e perspetivas teóricas relevantes para a problemática em estudo. O segundo capítulo, a metodologia, apresenta a metodologia de base e fundamenta as opções seguidas, assim como a pergunta de partida, perguntas derivadas e as hipóteses. O terceiro capítulo, descreve o método de sensibilização e validação escolhido e quais os procedimentos no trabalho de campo. Por fim, o quarto capítulo, análise e discussão

dos resultados, apresenta os dados e a sua análise, procurando descobrir o seu significado, correlações e resposta às hipóteses levantadas.

O trabalho termina com uma conclusão onde existe uma análise geral ao trabalho, indicando as limitações da investigação, e recomendações para futuras investigações.

CAPÍTULO 1
REVISÃO DE LITERATURA

1.1. Segurança da Informação

A investigação tem como base temática a segurança da informação, como tal, definir esta variável é importantíssimo. A segurança da informação está diretamente relacionada com a proteção da informação, no sentido de preservar o valor que estas possuem para um indivíduo ou uma organização. São características básicas da segurança da informação os atributos de confidencialidade, integridade e disponibilidade, não estando esta segurança restrita somente a sistemas computacionais, informações eletrónicas ou sistemas de armazenamento (ISO/IEC(271001), 2005). O conceito aplica-se a todos os aspetos de proteção de informação e dados.

Entende-se por informação "todo e qualquer conteúdo ou dado que tenha valor para alguma organização ou pessoa" (ISO/IEC(271001), 2005, pp. 2, Tradução Própria). Na maioria das organizações e na organização militar em particular, a informação é um dos ativos mais importantes, estando esta exposta, fundamentalmente, a três elementos: (i) à tecnologia, como o componente que permite guardar, processar e transmitir a informação; (ii) às pessoas que têm acesso à informação por qualquer meio; e (iii) ao processo de troca de informação utilizado para a manipular (Martins & Santos, 2010).

Ela pode estar guardada para uso restrito ou exposta ao público para consulta ou aquisição. O valor dela, segundo Martins, Santos, & Nunes (2009), é determinado segundo as dimensões de qualidade, conteúdo e temporalidade, isto é, respetivamente, se a informação é corrente, precisa e segura ou, por outras palavras, se o seu conteúdo é completo, relevante e se é atual relativamente à sua utilização.

Sendo assim, a segurança de uma determinada informação pode ser afetada por fatores comportamentais e do uso de quem se utiliza dela, pelo ambiente ou infraestrutura que a cerca ou por pessoas mal-intencionadas que têm o objetivo de a furtar, destruir ou modificar tal informação (Martins, Santos, & Nunes, 2009).

A definição de segurança da informação, segundo os padrões internacionais, é "*preservation of confidentiality, integrity and availability of information; in addition, other*

properties such as authenticity, accountability, non-repudiation and reliability can also be involved" (ISO/IEC(271001), 2005, p. 2)

Os atributos Confidencialidade, Integridade e Disponibilidade, atualmente, orientam a análise, o planeamento e a implementação da segurança para um determinado grupo de informações que se deseja proteger. Com a confidencialidade, procuramos garantir que a informação é acessível a só aqueles que estão autorizados a ter acesso a ela. A disponibilidade tem objetivo de garantir que os elementos autorizados têm acesso à informação quando precisam dela. Por último, com a integridade procura-se garantir que a informação e outros métodos de processo de informação não são modificados de forma critica (Martins & Santos, 2010).

Da mesma forma que definimos segurança da informação, a confidencialidade, segundo a ISO271001 (2005, p. 2), é definida como" *The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.*", a disponibilidade é "*The property of being acessible and usable upon demand by an authorized entity*" e finalmente a integridade é "*The property of safe guarding the accuracy and completeness of assets".*

Para se poder planear eficazmente a segurança da informação, é importante obter um modelo de gestão de informação que garanta as propriedades descritas em cima (pelo menos, a confidencialidade, integridade e disponibilidade) (Martins, Santos, & Nunes, 2009). Com base nos mesmos autores, um possível modelo de suporte à segurança da informação é o apresentado na figura 1.1 e deste pode-se retirar alguns pontos-chave da segurança da informação.

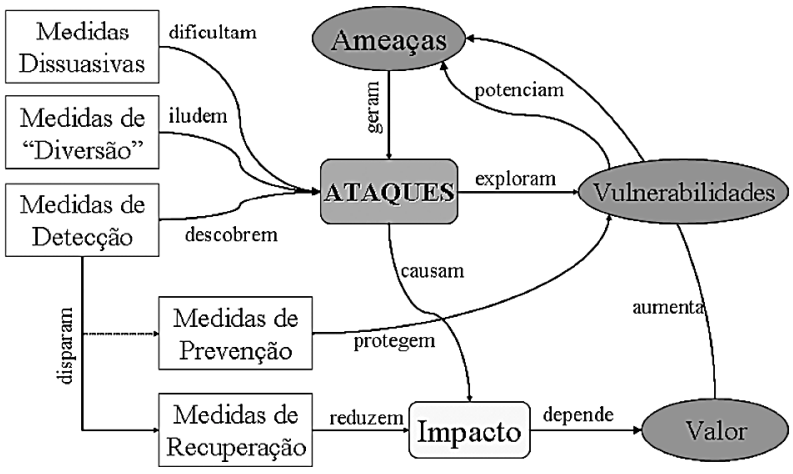


Figura 1. 1 - Modelo de suporte à norma ISO/IEC 17799

Fonte: Martins, Santos, & Nunes, 2009, p. 137

A nossa maior preocupação será, então, os ataques que, segundo Martins, Santos, & Nunes (2009, p. 137), baseado em Santos (2008) é definido como:

> "um conjunto de ações que, explorando uma ou mais vulnerabilidades do Sistema de Informação, que violam as suas propriedades de segurança, provocando algum tipo de impacto nos recursos. Para os ataques conhecidos é possível atuar sobre as vulnerabilidades que são exploradas, bloqueando as ameaças que nelas têm origem."

Com isto temos mais dois pontos importantíssimos a definir, que são as ameaças e as vulnerabilidades que, respetivamente, são "Causa potencial de um incidente de segurança da informação, do qual pode resultar prejuízo no sistema ou na organização." e são "Caraterísticas dos ativos críticos (alvos) de uma organização, que constituem fraquezas que podem ser explorados por um atacante para executar um método de ataque." (Martins J. C., 2013, p. 35 e 36). As causas potenciais de um incidente e os ativos críticos podem ser prevenidos e dificultados através de controlos de segurança da informação.

Para isso, é necessário diferenciar entre as várias dimensões da segurança da informação, começando pela dimensão tecnológica que garante o correto processamento, transmissão, armazenagem dos dados e informação. Temos também, a dimensão física e, por último, a dimensão humana, sendo esta última o foco deste trabalho de investigação.

A dimensão humana visa reduzir os riscos de erros humanos intencionais ou, por negligência sobre os componentes das informações, evitando principalmente os ataques de engenharia social, que vão explorar um dos elos mais fracos da segurança, o elemento humano (Peltier, 2006).

1.2. Engenharia Social

A engenharia social está englobada dentro do estudo (Dimensão Humana), como foi descrito anteriormente, e esta é de grande importância para o trabalho de investigação, já que dá origem à ameaça principal a ser retratada que são os ataques de *phishing*.

Segundo Thomas Peltier (2006, pp. 1, Tradução Própria) a engenharia social é "o nome dado a uma categoria de ataques à segurança, onde alguém manipula outra para revelar informação que pode ser usada para roubar informação mais restrita, ter acesso a sistemas, a telemóveis e a dinheiro ou mesmo acesso à identidade de outrem".

O objetivo dos engenheiros sociais é enganar as pessoas de forma a fornecerem aquilo que eles querem. Procuram qualidades na natureza humana como o desejo de ser útil, a tendência para confiar nas pessoas, o medo e a preguiça. Isto preocupa as organizações, já que através da boa-fé dos seus elementos, um engenheiro social consegue aquilo que quer,

sem criar alguma suspeita por parte da organização já que "São os maus engenheiros sociais que conhecemos e não os bons" (Peltier, 2006, pp. 2, Tradução Própria).

Analisa-se de seguida três autores, que descrevem as características da personalidade que permitem aos engenheiros sociais obter sucesso nas suas ações.

A primeira, de acordo com Applegate (2009), as pessoas têm necessidade de confiar no outro, especialmente nas organizações como as militares, em que existem muitas situações de risco onde dependemos uns dos outros e, assim, confiar em pessoas que gostamos ou aqueles que são credíveis, são uma alternativa para nos sentirmos seguros. Estabelecer confiança através dos gostos e da credibilidade é uma das primeiras opções de um engenheiro social. Outra tática utilizada será o uso da autoridade, o medo e a repreensão. A tendência de ser obediente perante uma autoridade é, também, uma forma de ganhar acesso à informação critica.

Segundo Thomas Peltier (2006), as características da personalidade que poderão ser usadas para garantir o sucesso de um ataque de engenharia social são a difusão de responsabilidade, a possibilidade de integração, a confiança na relação e a culpa. A difusão de responsabilidade existe quando o alvo acredita que não é o único responsável pelas suas ações, já que este não toma decisões ou não tem culpa das decisões tomadas pelos outros. As pessoas também procuram integrar-se melhor em qualquer organização, incluindo ganhar vantagem sobre a competição, ter relações cordiais com as chefias ou mesmo dar assistência a uma voz feminina, sendo que os engenheiros sociais utilizam a possibilidade de integração como forma de proposta que lhes irá trazer benefícios na organização. Alguns criam uma relação com o alvo de forma a ganhar a sua confiança e depois obter informações restritas da organização. Por último, na culpa, os elementos da organização tentam evitar ser culpados dos problemas e os engenheiros sociais aproveitam-se disso.

A terceira é a dos três tipos de compromissos de Workman (2007) que também indicou comportamentos que contribuem para o sucesso dos engenheiros sociais. Os compromissos que tornam o alvo mais vulnerável segundo Workman é (i) o compromisso de normativo, (ii) o compromisso de continuidade e (iii) o compromisso de alta afetiva. O compromisso normativo vem da "troca recíproca com o alvo, onde algum dos lados vai exercer um esforço extra e executar ações por bons costumes ou obrigação" (Beck & Wilson, 2000 citado em Applegate, 2009, p.43, Tradução Própria) em que o engenheiro social pode utilizar gestos como a oferta material, para ganhar informação restrita, e a vítima vai sentir-se socialmente desajeitada se não retribuir o favor.

Um exemplo de compromisso de continuidade é quando alguém despende imenso dinheiro nas tentativas de ganhar um urso de peluche numa feira de carnaval, este comportamento segundo Workman (2007, citado em Applegate, 2009, p.43, Tradução Própria) acontece porque "as pessoas revestem-se psicologicamente nas decisões que tomaram e mantêm os seus comportamentos segundo essa decisão" e isto pode estar relacionado com o orgulho próprio da pessoa. Por último, quando as pessoas querem ser incluídas num determinado círculo social, segundo o mesmo autor já citado "Esses indivíduos tendem a revelar informações porque querem fazer parte de um desejado grupo ou simplesmente para ser aceite" (2007, citado em Applegate, 2009, p.43, Tradução Própria).

Pelas três teorias revistas anteriormente, pode-se concluir que não se precisa de ter conhecimento técnico de redes e tecnologias informáticas para se ser engenheiro social. Então o porquê dos *hackers*[1] terem optado por este tipo de metodologia para obter informação? Porque o ser humano é o elo mais fraco da organização, e é a *Wetware* que causa as maiores dores de cabeça, não é assegurar a segurança do *hardware* nem o *software* (Peltier, 2006).

A *Wetware*, segundo Peltier (2006, pp. 3, Tradução Própria) é "o ser humano ligado a um sistema computacional".

A indústria de segurança de sistemas informáticos tem crescido e ficado cada vez mais robustas, dificultando aos *hackers* a penetração dos sistemas informáticos usando apenas meios técnicos, estes encontram a solução aos seus problemas através da *Wetware* (Applegate, 2009).

Sabemos o porquê desta metodologia de ataques e agora procuramos o como? "Tudo depende da criatividade do engenheiro social" (Manske, 2000 citado em Applegate, 2009, pp. 41, Tradução Própria), cujas acções podem ser divididas em dois tipos, umas baseadas no ser humano e outras baseadas em tecnologia. Baseadas no ser humano, referem-se a interações pessoa para pessoa com o objectivo de obter uma ação desejada, enquanto nas baseadas em tecnologia, significa ter uma interface eletrónica, à procura de conseguir um produto desejado (Peltier, 2006).

Podemos identificar, então, no caso dos ataques baseados no ser humano, oito formas de ataque: (i)*impersonation* e *important user, (ii)third-party authorization, (iii) in person, (iv)persuasion* e *bribery, (v) shoulder surfing* e *(vi) dumpster diving* (Applegate, 2009 & Peltier, 2006). O i*mpersonation e important user* acontece quando se usa falsas credenciais

[1] Pessoa que viola a segurança de sistemas informáticos; pirata informático (Dicionário da Língua Portuguesa com Acordo Ortográfico, 2003-2016)

ou simplesmente uma chamada telefónica declarando que é alguém de interesse para a organização, um jornalista ou mesmo um estudante a fazer um trabalho de investigação. O *third-party authorization* é quando um engenheiro social fala em nome de uma alta patente que tem bastante poder na organização, para ganhar acessos restritos. O *in person* acontece quando se utiliza a desculpa de ser visitante, de ser de outra organização amiga ou mesmo de ser um colaborador, para entrar num estabelecimento. O *persuasion* e *bribery*, como o nome indica, é quando um engenheiro social utiliza a persuasão ou o suborno para obter o que quer.

Os engenheiros sociais podem também utilizar o *shoulder surfing* para obter informação, já que este consiste em olhar "por cima do ombro" de um indivíduo quando este está a colocar o seu nome e *password*, decorando e depois entrar com as mesmas credenciais. Por último, podem utilizar o *dumpster diving* que consiste em agarrar em documentos que foram considerados lixo por um elemento da organização e que poderá ser informação critica nas mãos de um *hacker* (Applegate, 2009 & Peltier, 2006).

Para finalizar, as metodologias de ataque, falta falar nos baseados na tecnologia, sendo estes os *pop-up windows*, *websites* e, por último, e mais importante para a investigação, os ataques de *phishing* aos *e-mail*s (Applegate, 2009 & Peltier, 2006).

Os *pop-up windows* acontecem à entrada de alguma página desprotegida, aparecendo de repente uma janela auxiliar no meio do ecrã com algum esquema para tentar iludir o indivíduo a aceder ao conteúdo, abrindo portas para qualquer tipo de ameaça que o *hacker* quiser lançar. Quando encontramos *websites* ilegítimos, é outra forma de ataque usada, onde os *hackers* camuflam os seus *websites* de forma a serem espelhos de outros legítimos com o mesmo intuito anteriormente referido. Por último, os ataques de *phishing*, que são um modo bastante comum dos engenheiros sociais obterem informação critica, que segundo Manske (2000, citado em Applegate, 2009, pp. 41, Tradução Própria) "os ataques costumam servir como degraus para objectivo principal do atacante, que poderá ser, por exemplo, o controlo completo dos *servers* de uma organização".

Para terminar, falta indicar quais as possibilidades que temos para nos defender. Como já tinha sido referido anteriormente, a maior parte dos ataques de engenharia social não são reconhecidos, tornando difícil criar uma defesa específica. Ainda para dificultar a tarefa, segundo Peltier (2006, pp. 10, Tradução Própria) indica que:

> "30% de todos as tentativas de hacking vêm *Outsiders*; isto é, elementos que não trabalham na organização atacada. Isto significa que 70% dos *hackers* vêm do interior da própria organização. Por isso temos de ter este facto em mente quando criamos defesas contra engenheiros sociais".

Sendo assim, a melhor estratégia para se defender contra estes ataques será criar uma defesa integrada com múltiplas técnicas e políticas em defesa da informação critica da organização (Applegate, 2009). Esta defesa deve ter incluído (i) o processo de *awareness* de segurança, (ii) a proteção de informação crítica, e (iii) os controlos técnicos e protocolos de segurança.

O processo de *awareness* de segurança é considerado por Applegate (2009), a melhor defesa contra os ataques de engenharia social e será retratado, posteriormente, no trabalho. A proteção de informação crítica inicia-se com o bloquear o acesso a esta, através da limitação àqueles que precisam dela, e para isso, é necessário existir um esforço para a identificar e restringir através de controlos técnicos ou físicos. Os controlos técnicos e protocolos de segurança são também necessários, apesar de poderem ser ultrapassados, já que existem *hackers* especializados nisso mesmo, mas são importantes já que a sua boa implementação dificulta a sua tarefa (Applegate, 2009 & Peltier, 2006).

Sabemos então que, através destas estratégias, temos várias formas de evitar os engenheiros sociais. Para esta investigação, dentro das metodologias de ataques dos engenheiros sociais, os ataques de *phishing* são aqueles que será necessário conhecer com maior pormenor, em virtude do processo de *awareness*.

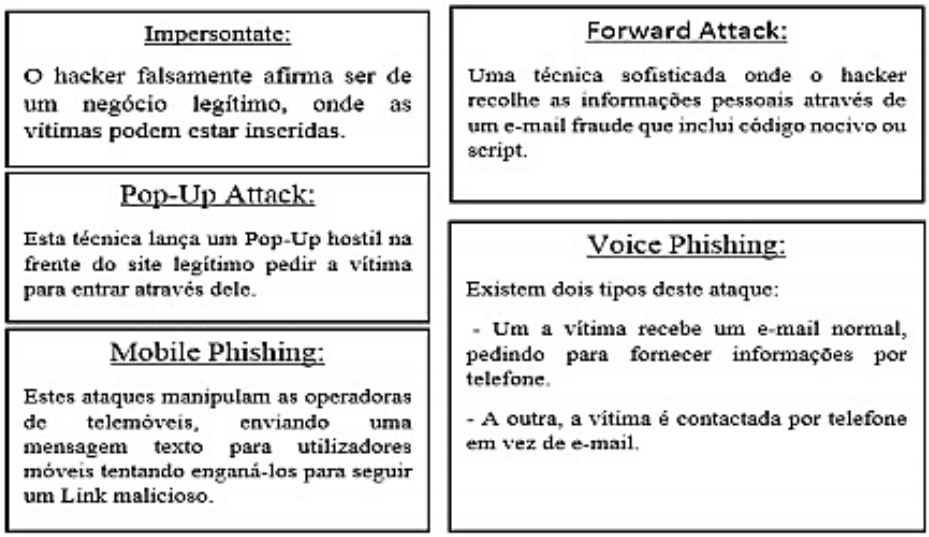
1.3. Os ataques de *phishing*

Segundo APWG (Tradução própria) [2], os ataques de *phishing* são "ataques que usam a engenharia social e subterfúgios técnicos para roubar dados dos consumidores como, dados pessoais e credenciais de contas bancárias. Esquema que usam a engenharia social para criar falsos *e-mails*, manipulando os consumidores para páginas de *web* falsificadas, concebidas para enganar os destinatários de forma a divulgar dados pessoais e bancários".

Em virtude do foco deste estudo ser o *awareness* para os ataques de p*hishing*, descreve-se de seguida, no quadro 1.1, as principais técnicas utilizadas pelos engenheiros sociais (Salem, Hossain, & Kamala, 2010).

[2]O Anti-Phishing Work Group(APWG) é a associação global de aplicação industrial e do direito focada na eliminação da fraude e roubo de identidade que resultam do *phishing*, *pharming* e falsificação de *e-mail* de todos os tipos

Quadro 1. 1 - Técnicas de Phishing



Fonte: Adptado de Salem, Hossain, & Kamala (2010)

Este tipo de ataque pode ser usado com apoio de outras técnicas de engenharia social, já referidas anteriormente, por isso não é de estranhar que as várias técnicas de *phishing* sejam parecidas com algumas metodologias de ataques dos engenheiros sociais.

Segundo Hong (2012, pp. 75, Tradução Própria):

> "os ataques de *phishing* envolvem três fases: (i) A primeira é quando as possíveis vítimas recebem um ataque; (ii) a segunda é a vítima tomar a ação indevida que se encontra na mensagem, podendo ser a entrada num *website*, mas também pode incluir instalar um vírus ou até responder com informação sensível; (iii) a terceira é o criminoso a monitorizar a informação roubada."

Não vai ser especificado nenhuma das três fases por serem percetíveis, pretende-se é analisar o porquê de estes esquemas fraudulentos obterem resultados. Segundo o Hong (2012), os meios técnicos falham na proteção e identificação destes ataques, já que os *hackers* utilizam a perceção dos elementos por trás do computador e não o interface em si. Ser apanhado em esquemas de *phishing* envolve falhas ao nível do julgamento do processo da informação e falhas ao nível da decisão. Erros de julgamento dos utilizadores, acontecem pela presença de *Visual Triggers* na mensagem de *e-mail*, e são reduzidos se os utilizadores conhecerem os possíveis indicadores de deceção provenientes de ataques executados pelos engenheiros sociais (Wang, Herath, Chen, Vishwanath, & Rao, 2012).

Para perceber estes erros de julgamento, apoiamo-nos em duas teorias, a *Theory of Deception* e *Attention to Visual Triggers.* De acordo com a *Theory of Deception*, proposta

por Grazioli (2004), os elementos reconhecem a deceção através da interpretação e reconhecimento de falhas no formato entre o evento de deceção e as suas experiências passadas. O processo de reconhecimento de deceção é decomposto em 4 fases:

> "(i)activação, onde os alvos têm atenção com informação de deceção e detetam anomalias;(ii) a criação da hipótese de deceção, onde os indivíduos usam o conhecimento passado para gerar uma interpetação para aquelas anomalias;(iii) a avaliação da hipótese, onde as hipóteses formadas anteriormente são comparadas segundo algum critério;(iv) e por fim, a fase de união dos factos, onde toda a informação é combinada para formar uma única e sintética resposta para a deceção. A competência na avaliação das hipóteses de deceção é o grande diferenciador entre o sucesso ou insucesso na deteção" (Grazioli, 2004 citado em Wang, Herath, Chen, Vishwanath, & Rao, 2012, p. 346 e 347, Tradução Própria).

Como se pode observar, a competência, ou seja, o conhecimento, tem um papel principal no sucesso da deteção, como também temos a atenção disponibilizada que poderá influenciar a deteção. Esta teoria explica a nossa ação perante uma situação habitual, sendo que, os *hackers*, para dificultar a deteção, utilizam os *Visual Triggers*, isto é, despertar o nosso espírito intuitivo para reagirmos sem pensar.

Os *Visual Triggers*, são introduzidos pelo *hacker* de forma a suprimir o esforço do alvo para perceber a mensagem e provocar reações intuitivas, consequentemente, erros de julgamento (Langenderfer & Shimp, 2001). Estes exploram necessidades básicas do ser humano e os seus desejos, como efeitos prejudiciais, medos e o nervosismo através da urgência para responder.

Para combater estes, o conhecimento específico destes esquemas maliciosos, é a melhor alternativa. O conhecimento, melhora a atenção aos indicadores de deceção, reduzindo diretamente a probabilidade de responder, e simultaneamente, altera o impacto dos *Visual Triggers*, reduzindo, então, a distração (Wang, Herath, Chen, Vishwanath, & Rao, 2012).

Antes de se indicar as medidas de proteção a estes ataques, devemos perceber que nem todos os ataques deste género são directos a um indivíduo ou organização específica. A maioria dos ataques de *phishing* são dirigidos a individuos e a organizações aleatórios. Quando estes são diretos a um sujeito em concreto, dá-se o nome de *spearphishing* e estes serão o maior problema para uma organização. Segundo Wang, Herath, Chen, Vishwanath, & Rao (2012, pp. 345, Tradução Própria) *Spearphishing* é conhecido como:

> "um tipo de ataque em que o *hacker* foca numa determinada organização (utilizando informação disponível sobre ela) criando um esquema que parece genuíno para os membros da organização. Os *e-mail*'s de *spearphishing* têm muitas características semelhantes aos normais golpes de *phishing*, mas têm contexto mais específico. Eles parecem ser originais da organização, criando maior relevância na entidade remetente."

Para a organização militar, estes são o maior problema e é a razão principal desta investigação.

Assim, para finalizar, indicam-se sumariamente as principais medidas a tomar para nos defendermos desta ameaça. Estas medidas são, através da proteção da informação crítica, dos controlos técnicos (os *anti-phishing toolbars*, os *browsers plug-ins* e os *email-filters)* e das políticas de segurança (Salem, Hossain, & Kamala, 2010). A acrescentar, melhores interfaces e avisos, que despertam a atenção das pessoas e, como já foi revisto anteriormente, para lutar contra estes esquemas maliciosos, temos de ter atenção aos indicadores de deceção e aos *Visual Triggers*, em que o conhecimento é o grande foco, acrescentando, assim, a importância do processo de *awareness* de segurança que é a problemática central deste estudo.

1.4. Processo de awareness de segurança

Neste subcapítulo, começamos por definir a palavra *awareness*, que segundo Thomas Peltier (2005, pp. 11, Tradução Própria) é "estimular e motivar a audiência sobre um certo problema ou objetivo", assim encontramos dois pontos fundamentais de um processo de *awareness* de segurança, a audiência e o problema/objetivo.

Para combater a engenharia social, no geral, e o *SpearPhishing*, no particular, a organização deve implementar um processo de *awareness* de segurança, uma coisa tão simples como: informar/sensibilizar os elementos da organização que a organização nunca pede o seu *username* nem *passwords*. Isto poderá ser a diferença entre o sucesso, ou não, de um ataque (Applegate, 2009).

O Instituto Nacional de Padrões e Tecnologia Americano recomenda quatro controlos de segurança da informação para evitar os ataques de Engenharia Social:

"- Implementar uma segurança formalmente documentada e política de formação;

- Fornecer treino de segurança básica a todos os utilizadores de sistemas de informação dentro da organização;

- Fornecer informações específicas de segurança do sistema para os indivíduos identificados como tendo funções de Segurança dentro da organização.

- Documentar, monitorizar e sensibilizar para os registos de segurança e treino de segurança para todo o pessoal da organização." (Applegate, 2009, pp. 44, Tradução Própria)

Estas recomendações são a um nível geral, ou seja, para todos os níveis da organização em que um dos aspetos críticos é o *awareness* dos utilizadores. Thomas

Peltier(2005) indica que, para se criar um processo de *awareness*, é necessário perceber como é que as pessoas aprendem.

No seu estudo indica que existem três formas elementares das pessoas aprenderem: (i) o auditivo, onde as pessoas têm de ouvir algo, a fim de compreender; (ii) o mecânico, este tipo de aprendizagem a pessoa tem de reagir fisicamente para aprender, que é exemplo os jogos e questionários; (iii) e o visual, neste tipo a pessoa necessita de ver uma imagem ou diagrama para entender o que está a ser discutido; (Peltier, 2005).

Ele próprio dá o exemplo de como os programas de informação (noticiários) funcionam. Estes podem ser uma escolha para um processo de *awareness* de segurança, apresentando o conhecimento por factos baseados em imagem e som. Pode-se concluir então que um processo de *awareness* necessita de ter, no mínimo, um destes três elementos, para garantir a aprendizagem de um grupo de elementos.

O académico, Jasong Hung (2012) diz que o treino não garante proteção completa, que é necessário o interesse dos elementos. Por exemplo, o envio de informação *anti-phishing* não tem efeito, porque é habitual receber avisos ao navegar na *web*.

Diz, o mesmo autor, que existe duas formas de combater este problema: a primeira serão pequenos jogos desejados para sensibilizar sobre *phishing*. Os jogos são um formato popular e as pessoas não vêem como uma obrigação, mas sim algo para passar o tempo e, com os jogos, conseguimos ter todos os elementos de aprendizagem indicados anteriormente (Hong, 2012).

A segunda forma chama-se treino incorporado, isto é, submeter os elementos a avaliação ou ao contexto específico de um ataque. Este tipo de treino é diferente dos outros, já que não é suficiente dar a conhecer o assunto, tem de se pôr em prática (Kumaraguru, et al., 2007). Um exemplo será um programa chamado *PhishGuru* que envia *e-mails* fraudulentos para os elementos de uma organização e, aqueles que falharem nestes esquemas, recebem uma intervenção que ensina sobre o que falharam (Kumaraguru, Sheng, Acquisti, Cranor, & Hong, 2008).

A aplicação do PhishGuru levou a uma redução de 45% no insucesso de detetar estes ataques, mesmo após um mês do treino (Kumaraguru, Sheng, Acquisti, Cranor, & Hong, 2008). As lições apreendidas do estudo anterior apresentam quatro tópicos a considerar em investigações sobre ataques de phishing e para sensibilizações: (i) O conteúdo dos *e-mail*s é importante, já que deve ter relevância para os elementos em estudo e deve ter os argumentos necessários para se tomar uma decisão; (ii) devemos incentivar os participantes, já que se consegue obter melhores resultados através disso; (iii) usar elementos diferentes, porque a

amostra deve ser diversificada para melhores resultados; (iv) e por último, *Keep It Simple*, mensagens elaboradas são mais difíceis de se perceber; (Kumaraguru et al, 2008).

Este último tópico (*Keep It Simple*), também foi considerado por Thomas Peltier (2005), em que, considera que, para passar qualquer mensagem, é necessário que seja simples, já que a subrecarga de informação só atrapalha o raciocínio dos elementos. Não devemos tentar apresentar toda a informação sobre segurança numa só sessão. Indica também que devemos ter em mente que só vamos ter trinta minutos de atenção dos participantes, o resto da sessão, a atenção será reduzida significativamente.

Assim termina a revisão de literatura, obtendo-se os conhecimentos (Estado da Arte) necessários para se poder criar um processo de *awareness* para os colaboradores das organizações militares se poderem proteger dos ataques de *phishing*. A revisão de literatura, face ao tempo disponivel, está limitada, tanto em extensão como de abordagem.

O próximo capítulo descreve-se a metodologia de investigação aplicada neste trabalho.

CAPÍTULO 2
METODOLOGIA

Neste capítulo, apresenta-se o método, a natureza, o procedimento, os objetivos e o desenho da investigação, bem como, a pergunta de partida, as perguntas derivadas e as hipóteses nos últimos subcapítulos. A forma como o problema é concebido e estruturado, é de extrema importância para um correto apuramento de resultados (Raupp & Beuren, 2003).

2.1. Método

Como se pode ver na tabela 2.1, a metodologia da investigação pode ser classificada por dois pontos, sendo estes, pela forma de abordagem e pelos procedimentos. Para classificarmos a metodologia da investigação, quanto à forma de abordagem, temos que ter em atenção aos seguintes métodos: Método Dedutivo, Método Indutivo, Método-Hipotético Dedutivo, Método Dialético e Método Fenomenológico.

Tabela 2. 1 - Abordagem e procedimentos

Classificação	Modalidade
Abordagem (lógicos)	Dedutivo Indutivo Hipotético-Dedutivo Dialético Fenomenológico
Procedimentos (técnicos)	Comparativo Histórico Estudo de Caso Estatístico

Fonte: Adaptado de TCor Pinto da Silva, sessão Metodologias de Investigação (Sarmento, 2013)

Quanto aos métodos de procedimentos da investigação, temos que ter em atenção aos seguintes métodos: Método Histórico, Método Comparativo, Método Estatístico e Método de Estudo de Caso.

Desta forma o método científico *"*é um conjunto de procedimentos e normas que permitem produzir conhecimento. Este conhecimento pode ser completamente novo ou ser o desenvolvimento, a reunião ou o melhoramento de um ou vários conhecimentos já existentes" (Sarmento, 2013, p. 7).

Segundo Sarmento (2013, p.5) o método tem de apresentar algumas caraterísticas para ser considerado científico, nomeadamente:

- "Objetividade: Não depender do sujeito que investiga, mas do objeto de estudo;

- Refutabilidade: contestar e discutir os fatos atendendo aos múltiplos aspetos que os compõem;

- Estruturação: criar uma organização racional e lógica dos fatos;

- Previsibilidade: estimar ou prever os fatos com bases nas hipóteses;

- Controlo: verificar as hipóteses para haver confiança nas conclusões;

- Crítico: comentar, elucidar ou analisar os fatos sobre várias perspetivas;

- Comparabilidade: permitir estabelecer relações de confronto de fatos sob várias perspetivas;

- Causalidade: Haver relação entre causa e o efeito no acontecimento dos fatos".

Em relação ao meu trabalho de investigação aplicada, quanto à forma de abordagem, vou usar o método Hipotético-dedutivo, e quanto aos procedimentos, vou usar o método Estudo de Caso. Este método de abordagem utiliza uma estratégia que combina os métodos indutivo e dedutivo, pois o investigador necessita tanto de ir dos dados para a teoria como da teoria aos dados. A partir da teoria procura-se abarcar, através de um processo dedutivo, a experiência e a realidade; por sua vez, com base na experiência institui-se ou reformula-se a teoria, recorrendo para tal a um processo indutivo. (Freixo, 2011).

O método hipotético-dedutivo compreende as seguintes fases: (i) colocação do problema; (ii) construção de um modelo teórico; (iii) dedução de consequências particulares; (iv) teste de hipóteses; e (v) introdução das asserções na teoria (Carvalho, 2009).

2.2. Natureza

Existem diversos tipos de investigação, assumindo estes, normalmente, a forma de investigação fundamental ou de investigação aplicada.

> "A investigação fundamental tem por finalidade provar teorias, leis científicas ou princípios de base, de modo a promover a aquisição de novos conhecimentos científicos, sem se preocupar com a aplicação ou utilização prática imediata desses mesmos conhecimentos. A investigação aplicada tem por objetivo encontrar uma aplicação prática para os novos conhecimentos, adquiridos no decurso da realização de trabalhos originais" (Carvalho, 2009, p. 42).

A investigação aplicada será o processo adotado, uma vez que se trata de uma investigação que incide sobre problemas específicos.

2.3. Procedimento

Segundo Gil (2008) e Markoni & Lakatos (2003), os métodos de procedimentos mais adotados são: histórico; comparativo; estatístico; e estudo de caso ou monográfico.

O estudo de caso enquadra-se no âmbito das estratégias de investigação qualitativas e apresenta uma natureza essencialmente empírica e descritiva, no entanto, não é possível estabelecer, com rigor, generalização de resultados. (Freixo, 2011).

O procedimento adotado para o presente trabalho é o Estudo de Caso, que consiste no exame detalhado de uma situação, sujeito ou determinado acontecimento, para desta forma obter a informação necessária para a fundamentação de determinado projeto e posteriormente criar uma teoria, baseada em critérios pragmáticos e teóricos (Aires, 2011).

As técnicas de recolha de dados, segundo Almeida, Machado, Capucha, & Torres (1994), constituem sempre um exercício arbitrário, pois depende da perspetiva escolhida para as selecionar e distinguir. Como técnicas de recolha de dados, são usadas a pesquisa bibliográfica e a análise documental.

2.4. Objetivos

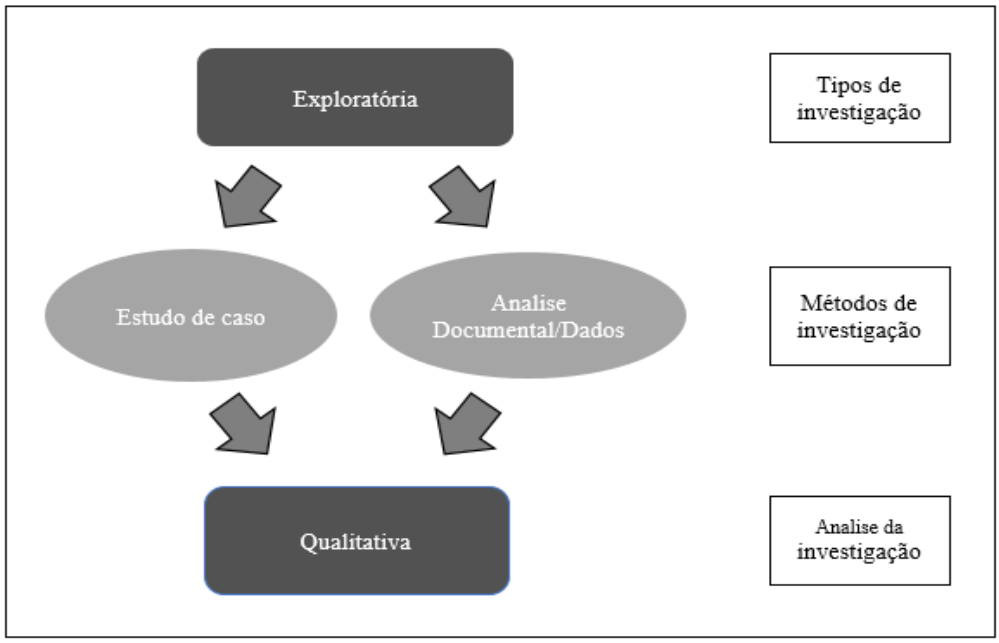
É importante, então, definir o delineamento da pesquisa, quanto aos objetivos, sendo que, neste âmbito, a pesquisa pode ser exploratória, descritiva ou explicativa.

A presente investigação é do tipo exploratório e tem como finalidade conhecer com maior profundidade determinado assunto (exemplo *awareness* para o *phishing*) de modo a torná-lo mais claro ou a levantar hipóteses (Raupp & Beuren, 2003). Este tipo de pesquisa é utilizado quando determinado assunto é pouco explorado e torna-se difícil formular hipóteses.

2.5. Desenho de investigação

De forma a compreender melhor a metodologia aplicada nesta investigação, temos no quadro 2.1, o desenho de investigação que resume toda a metodologia empregue neste trabalho.

Quadro 2. 1 - Desenho de Investigação



Fonte: Elaboração Própria

Nos próximos subcapítulos, vamos descrever a pergunta de partida e as perguntas derivadas, assim como as hipóteses desta investigação.

2.6. Pergunta de Partida e Perguntas Derivadas

As perguntas de investigação são "um enunciado interrogativo claro e não equívoco que precisa os conceitos-chave, especifica a natureza da população que se quer estudar e sugere uma investigação empírica" (Fortin, 2009, p. 51).

A pergunta de partida é "Como efetuar o *design* de um processo de *awareness* para o Exército que reduza o impacto dos ataques de *phishing* executados através do seu sistema de *e-mail*?"

Esta questão de investigação originou um conjunto de perguntas que pretendem responder à pergunta de partida. Elas são:

Pergunta derivada 1:" quais as principais teorias comportamentais que influenciam o sucesso dos métodos de ataque de *phishing*?"

Pergunta derivada 2:" quais os principais métodos ou técnicas de ensino de atitudes que permitem alterar os comportamentos incorretos dos utilizadores face a um ataque de *phishing*?"

Pergunta derivada 3:" qual o principal meio para realizar as ações de *awareness*?"

Pergunta derivada 4:" quais os principais critérios de avaliação, ou seja, de validação da eficácia e eficiência de uma ação de *awareness* ministrada?"

2.7. Hipóteses

As hipóteses de investigação devem estar ligadas direta e logicamente ao problema de investigação de modo a se relacionar com o objetivo final da investigação.

Segundo Fortin (2009, p. 102), "Uma hipótese é um enunciado formal das relações previstas entre duas ou mais variáveis. É uma predição baseada na teoria ou numa porção desta (proposição)".

Tendo em conta as perguntas de investigação levantadas, surgem as seguintes hipóteses:

Hipóteses 1:" As teorias comportamentais, que mais influenciam o sucesso dos ataques de *phishin*g são a *Theory of Deception* e *a Attention to Visual Triggers*."

Hipóteses 2:" Os principais métodos de ensino de atitudes é o método de ensino ativo, utilizando os estilos de aprendizagem auditivo, mecânico e visual."

Hipóteses 3:" O principal meio para realizar ações de sensibilização na organização militar (Exército Português), é o programa de apresentação PowerPoint."

Hipóteses 4:" O critério de avaliação será a comparação entre elementos sem sensibilização e elementos com sensibilização, e verificar se existe redução das escolhas erradas neste último.

CAPÍTULO 3
MÉTODOS E TÉCNICAS DO TRABALHO DE CAMPO

Este capítulo aborda o planeamento do processo de *awareness*, a preparação do material para o trabalho de campo e sua execução. O processo de *awareness* foi realizado através da aplicação de um questionário inicial, seguida de uma sessão de sensibilização e terminou com outro questionário.

3.1. Orientação Geral e Restrições

A escolha do processo de *awareness* proposto neste estudo teve em conta limitações, de nível administrativo e a nível técnico.

A nível administrativo, teve-se em conta que tinha nove semanas para elaboração total do trabalho, um prazo relativamente curto comparativamente a outros estudos que levaram meses de preparação, como é exemplo as investigações de kumaraguru et al. (2008), utilizando o *PhishGuru*, que só o trabalho de campo demorou trinta e um dias, ou mesmo o exemplo de *WestPoint* que executa todos os anos sessões de *awareness* (Jr., Carver, & Ferguson, 2007).

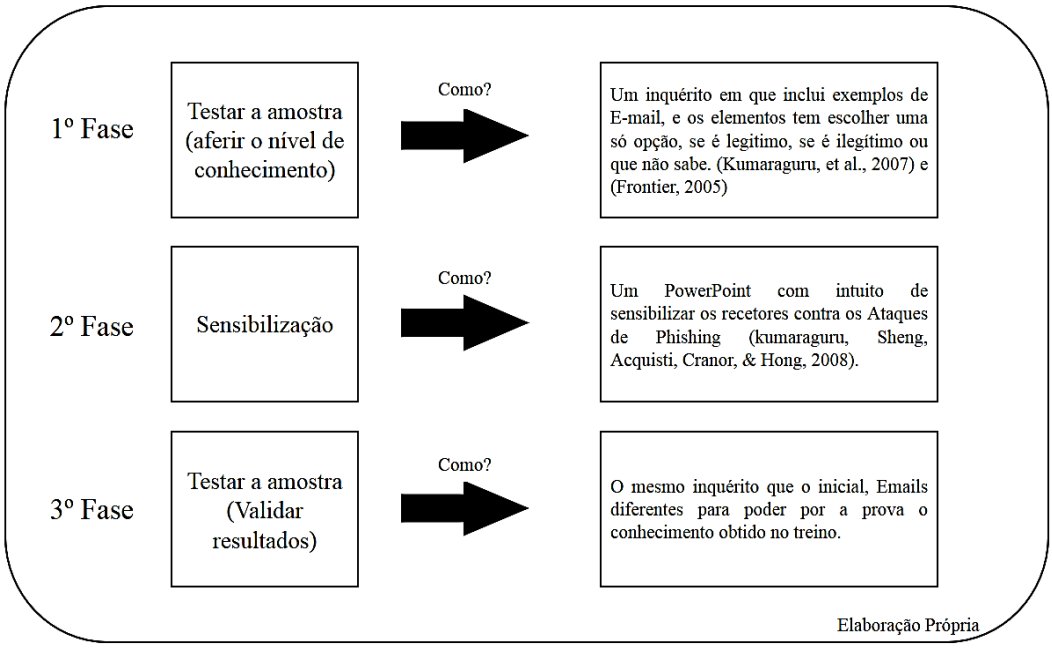
Outro aspeto a ter em conta, são os custos de aquisição de programas como o *PhishGuru* e outros que se pode encontrar no *website* do APWG, que não estão implementados na organização militar, e ao serem dispendiosos, numa primeira instância, não os poder testar, logo, coloquei essa ideia de parte.

A nível técnico, existia, também, a possibilidade de executar todo este processo através da interface computador, através de plataformas de *e-learning*, de *survey* (exemplo da investigação de Wang, Herath, Chen, Vishwanath, & Rao (Phishing Susceptibility: An Investigation into the processing of a targeted Spear Phishng Email, 2012) ou mesmo criar um treino incorporado utilizando a plataforma *e-mail* do Exército, mas tudo isso seria impossível no tempo definido, como também não possuo conhecimento técnico nem um grupo de trabalho capaz de desenvolver esses géneros de processos, e assim teve-se de optar por outras formas de sensibilização.

Com estas restrições, optou-se por seguir os passos de Thomas Peltier (2005) e criar um treino incorporado, cuja finalidade última é a proteção e deteção de *e-mail* ilegítimos, baseado na ferramenta desenvolvida por Frontier (2005) o *Phishing IQ*, que faz uma mistura entre *e-mails* legítimos e ilegítimos para verificar o conhecimento do utilizador, e ainda baseado nos exercícios desenolvidos em WestPoint, *"*na primeira fase, os cadetes eram testados na sua habilidade de detetar ataques de phishing. Numa segunda fase, o cadetes recebiam treino em salas de aulas e no final eram novamento testados*"* (Kumaraguru, Sheng, Acquisti, Cranor, & Hong, 2008, pp. 2, Tradução Própria).

Assim, decidou-se fazer questionários como forma de aferição e avaliação de conhecimento, nos mesmos moldes da ferramenta *Phishing IQ* e utilizar o programa Microsoft office PowerPoint para fazer a sensibilização, sendo um programa familiar dentro da organização militar. Os seguintes subcapítulos explicam a construção dos questionários e da plataforma PowerPoint e justificam as opções tomadas. O quadro 3.1 apresenta em forma de esquema todo o trabalho de campo realizado.

Quadro 3. 1 - Desenho o trabalho de campo



Fonte: Elaboração Própria

3.2. Questionários de Aferição e Validação

A construção dos questionários teve como referencial ao nível da sintaxe, os questionários normais aplicados no âmbito da liderança na Academia Militar.

Uma capa com uma ligeira justificação da aplicação dos questionários, de seguida a primeira parte com dados sociodemográficos, onde os elementos têm de se identificar através da definição do ramo em que estão inseridos, GNR ou Exército Português, o ano do curso em que atualmente pertencem, o curso propriamente dito, se já eram militares anteriormente, a sua idade, o género e a data de nascimento. Estes dados serão utilizados somente para fins estatísticos no âmbito deste trabalho académico.

A segunda parte, introduz o questionário, com vinte e cinco imagens, quinze de *e-mail*s ilegítimos e dez de *e-mail*s legítimos (ver Apêndices A e B).

O intuito do questionário é validar/aferir o conhecimento na deteção de *e-mails* ilegítimos, sendo esta a única justificação de existir mais *e-mail* ilegítimos do que legítimos. A maioria das imagens foram retiradas da internet, que consistem, essencialmente, em *e-mails* ilegítimos de organizações bancárias (exemplo CGD, BPI, etc…), do GMail da GOOGLE, do Skype e do Facebook.

3.3. Produto de Sensibilização

Na criação deste produto teve-se em consideração duas preocupações, primeiro, que estivesse tecnicamente correto, e para isso a sua construção baseou-se em trabalhos de outros autores e em artigos científicos. A segunda preocupação foi seguir um esquema ou referencial para garantir a aprendizagem, e por isso, optou-se pelo referencial de formação adotado pelo Exército Português, o Referencial de Formação Pedagógica Inicial de Formadores (IESE, 2013) e ainda nas ideias de implementação de um programa de *awareness*, propostas por Thomas R. Peltier (2005) .

Na parte técnica, como se pode ver no Apêndice C - Apresentação de Sensibilização, todos os diapositivos têm a referência onde este foi baseado.

Nos diapositivos dois a catorze encontramos, desde Applegate (2009), na introdução, onde se faz uma contextualização da sensibilização, à definição de ataques de *phishing* segundo APWG, e às técnicas de *phishing* como se encontra no quadro 1.1

Apresenta- se nos diapositivos 15 a 23, a definição de *spearphishing* já apresentada anteriormente de Wang, et al. (2012), seguido das instruções de proteção contra-ataques de *phishing* apresentado por Kumaraguru, et al. (2008) como se pode verificar no quadro 3.2.

Quadro 3. 2 - Instruções de proteção

Instruções de SpearPhishing
1. Nunca clicar em links dentro de e-mails ou responder com informação pessoal;
2. Escrever o site verdadeiro, num browser à parte;
3. Ligue a pessoa ou organização em questão, nunca confie nos números de telefone nos e-mails. Procure o certo e lingue;
4. Nunca dar/inserir informações pessoais ou da organização, não importa quem seja que lhe esteja a pedir;
5. Reportar e-mails suspeitos para a organização, para esta estar informada e poder estabelecer medidas de proteção

Fonte: Adaptado de Kumaraguru, et al (2008, pp. 7, Tabela III)

Por fim, nos diapositivos 24 a 28, temos as instruções para detetar *e-mails* ilegítimos de Karakasiotis, Furnel, & Papadaki (2006, p. 2) que terminam a apresentação de sensibilização. Todas as imagens e esquemas usados estão referenciados e foram revistos de forma a serem compatíveis com o texto citado nos diapositivos para não existir incongruência no conhecimento.

O *design* do PowerPoint, como já tinha referido anteriormente, teve em conta as ideias de Thomas R. Peltier (2005, pp. 13, Tradução Própria) onde indica que "Apesar de todas as organizações terem o seu próprio estilo e método de treino, pode ajudar rever alguns importantes problemas na criação de um processo de *awareness*" e apresenta vários pontos a considerar.

Primeiro, os processos de *awareness* são contínuos, por isso deve-se evitar apresentar demasiada informação. Devemos identificar onde começou a mensagem que se quer passar, desenvolvendo-a e reforçando-a. No estudo, a mensagem que se pretende passar é: "como detetar e proteger de um ataque de *phishing*".

Na construção do produto de sensibilização (apresentação de sensibilização), tiveram-se em consideração, boas práticas pedagógicas referenciadas pelo profissional de segurança da informação Thomas R. Peltier e no Referencial de Formação Pedagógica Inicial de Formadores, as quais serão analisadas sumariamente , de seguida.

As sessões têm de ser curtas, sendo recomendado para não adiantar mais do que cinquenta minutos por razões biológicas, de tempo de atenção e problemas de produtividade (Peltier, 2005).

A apresentação deve usar vocabulário percetível para a audiência e o nível técnico deve ser aceitável para a mesma. A apresentação tem trinta e um diapositivos e não apresenta vocabulário técnico, nem é necessário conhecimento prévio para a poder compreender.

A apresentação não deve ter a aparência de uma dissertação de mestrado, deve ter em conta a audiência e a cultura da organização. Na Academia Militar e no Exército Português existe a "tradição" de usar o PowerPoint como programa de apresentação e, por esta razão, é que não escolhi outro meio de apresentação, apesar de ter conhecimento de outros meios apresentados no Referencial de Formação Pedagógica Inicial de Formadores (2013).

Em relação à aparência, utilizou-se o mesmo processo para a construção de apresentações multimédias que o Exército Português adotou, abordado no Referencial de Formação Pedagógica Inicial de Formadores (2013), que será apresentado de seguida.

Para efetuar o *design* de uma apresentação multimédia deve-se ter em atenção os cinco pontos descritos no quadro 3.3

Quadro 3. 3 - Propriedades de um documento

Fonte: adaptado de (Módulo de Formação - Recursos Didáticos e Multimédia, 2013)

Para não comprometer os pontos descritos em cima, deve-se ter cuidado com aspetos de forma e conteúdo dos diapositivos. Para a forma do diapositivo temos que considerar (i) o formato; (ii) o fundo; (iii) as cores; (iv) as fontes; (v) o tamanho; (vi) a numeração; (vii) marcas e (viii) o texto. Para o conteúdo temos (i) a progressão, (ii) as diferenças e (iii) o detalhe. De seguida analisa-se com algum detalhe os elementos anteriormente referenciados, segundo o Módulo de Formação do Curso Pedagógico Inicial de Formadores (2013).

No que toca ao formato, devemos pensar na apresentação como um livro, cada diapositivo deve estar interligado entre si. Em cada diapositivo, o texto deve iniciar sempre no mesmo local, uma técnica conhecida como "Ponto de Referência".

O fundo deve ser simples e relevante. O espaço no diapositivo deve ser abundante de forma a obtermos equilíbrio, não centrando tudo e distribuindo as peças de forma equilibrada. O fundo deve ser de cores escuras, mais especificamente os azuis e verdes escuros, que são os mais eficazes por serem mais confortáveis para a vista e mantêm um

bom contraste para o texto e a imagens. Ao contrário, cores brilhantes e claras são cansativas para a vista.

Nas cores usadas deve existir coerência, não alterando as cores durante toda a apresentação, existindo no máximo de cinco cores por diapositivo. Cores suaves são mais eficazes que cores berrantes, podendo existir exceções para dar ênfase. Mudanças subtis tornam-se visualmente mais agradáveis, mas deve existir contraste, como se pode verificar na figura 3.1.

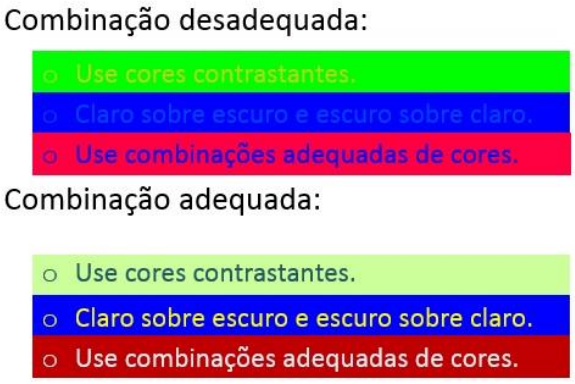


Figura 3. 1 - Combinação de cores

Fonte: retirado de (Módulo de Formação - Recursos Didáticos e Multimédia, 2013)

Deve-se usar fontes *standard* do *Windows (*Arial, Times New Roman*)* porque fontes não *standard* poderão alterar o seu documento, substituindo letras e símbolos. Devem ser de linhas mais grossas, percetíveis, sem serifas e não elaboradas.

O seu tamanho pode variar, dependendo do sítio onde será usada a apresentação e do seu público, como está especificado na figura 3.2, como também se pode usar tamanho para realçar o aspeto.

Local		Auditório	Sala Conferências	Sala Aulas
Tamanho das Fontes	44 pt	☺	☺	☺
	40 pt	😐	☺	☺
	36 pt	☹	😐	☺
	32 pt	☹	☹	😐
	28 pt	☹	☹	☹
N.º máx. linhas		6	7	8
N.º máx. palavras		30	35	64

Figura 3. 2 - Tamanho das fontes

Fonte: retirado de (Módulo de Formação - Recursos Didáticos e Multimédia, 2013)

Nas listas, usar números nas sequências específicas e usar marcas nas listas sem prioridades, sequências ou hierarquias.

Quadro 3. 4 - Exemplos de números e marcas

Exemplo números:	**Exemplo marcas:**
Como se põe um elefante dentro do frigorífico? 1. Abre-se a porta do frigorífico; 2. Põe-se o elefante lá dentro; 3. Fecha-se a porta.	O que mais se pode pôr no frigorífico? ◊ Leões; ◊ Hienas; ◊ Babuínos…

Fonte: Elaboração Própria

Ainda em relação à forma, no diapositivo, não devemos colocar muito texto, nem existir pouco espaçamento entre linhas e entre parágrafos, como também não se deve definir um tamanho de letra muito pequeno e claro não criar diapositivos completamente preenchidos por texto.

Deve-se, então, utilizar palavras-chave, minimizar a pontuação, utilizar no máximo de oito palavras por linha e oito linhas por diapositivo. Ser simples, porque demasiadas variações distraem as pessoas, como é o caso das cores, dos tipos de letra e de realces como *itálico* (por se tornar difícil de ler). Podem-se usar maiúsculas em títulos, anotações, cabeçalhos e, para dar ênfase, mas é proibido em blocos de texto completos (dificulta a

leitura).

Para dar ênfase a determinado texto recorre-se ao aumento do tamanho, a *Itálico,* a uma cor diferente e a maiúsculas, mas não sublinhe porque a linha confunde-se com o texto.

O alinhamento não deve ser centrado nem justificado por se tornar mais difícil de ler porque existem espaços diferentes entre palavras e o início de cada linha também é diferente.

Em relação ao conteúdo, todo o PowerPoint deve seguir um raciocínio lógico e não apresentar demasiada informação, de uma só vez. As diferenças no desenrolar dos diapositivos atraem a atenção e devem realçar algo de importante, já que, demasiadas diferenças confundem e distraem. Devemos manter os diapositivos o mais simples possível, não tendo demasiada informação num só diapositivo e utilizar poucas imagens porque estas distraem.

Ao nível da estrutura da apresentação, e de acordo com Thomas Peltier (2005), todas as apresentações de sensibilização serão diferentes, mas devemos ter como referências, os cincos pontos seguintes: (i) Introdução, onde se dá a conhecer o tópico a ser abordado e a sua importância para os recetores; (ii) a mensagem, ou seja o objetivo da sessão, como também é abordado no Referencial de Formação Pedagógica Inicial de Formadores (2013); (iii) a apresentação do problema e respectiva resposta ao mesmo, discutindo métodos que o recetor deve usar para responder ao problema; (iv) as questões e respostas, onde o recetor poderá dar conhecimento de lapsos que a sensibilização não responde e contribuir para uma maior aprendizagem por parte do mesmo; (v) por último, o reforço, como por exemplo um quadro de compilação de métodos de resposta à mensagem, que os recetores poderão levar para fora da formação.

O design da apresentação teve em conta este cinco passos, contemplando, então, uma introdução, o objectivo, uma fase de resposta ao problema dividida em "O que são?", "Quais as técnicas existentes?", "Qual a sua importância para a organização militar?", "Como nos podemos defender?" e "Como os detetamos?", terminando com um sumário e colocação de questões.

Para garantir a aprendizagem, é útil identificar potenciais barreiras a uma comunicação eficiente que incluem (Peltier, 2005): (i) a imagem, devendo os sensibilizadores mostrar aprume e competência; (ii) a preparação, porque falta de material e/ou equipamento mal preparado demonstra incompetência; (iii) na apresentação, apesar de não existirem elementos humanos, neste processo de sensibilização, este não deve ler a sua apresentação, mas sim apoiar-se nos tópicos chave; (iv) não utilizar termos técnicos, mas sim uma linguagem adequada ao público presente, tanto no *design* da apresentação, como

em público; (v) deve-se ter cuidado com o idioma, já que, tanto causa desinteresse não utilizar a língua materna, como podem existir indivíduos sem conhecimento de outras línguas; (vi) por fim o tempo, quanto mais curta for a sensibilização melhor (Peltier, 2005).

Este tipo de sensibilizações, segundo Thomas Peltier (2005), devem ser executadas, de preferência, na manhã de um dia qualquer da semana. Nunca depois do almoço, porque é o momento onde os índices de atenção são os mais baixos.

Concluindo, estas foram as linhas que orientaram o *design* da apresentação de sensibilização (Apêndice C - Apresentação de Sensibilização).

3.4. Configuração do Trabalho de Campo

Neste subcapítulo, apresentamos a escolha da amostra e o formato do estudo, ou seja, o processo de *awareness*. É importante ter em atenção as limitações, anteriormente apresentadas e que condicionaram as possíveis escolhas.

3.4.1. Definição da Amostra

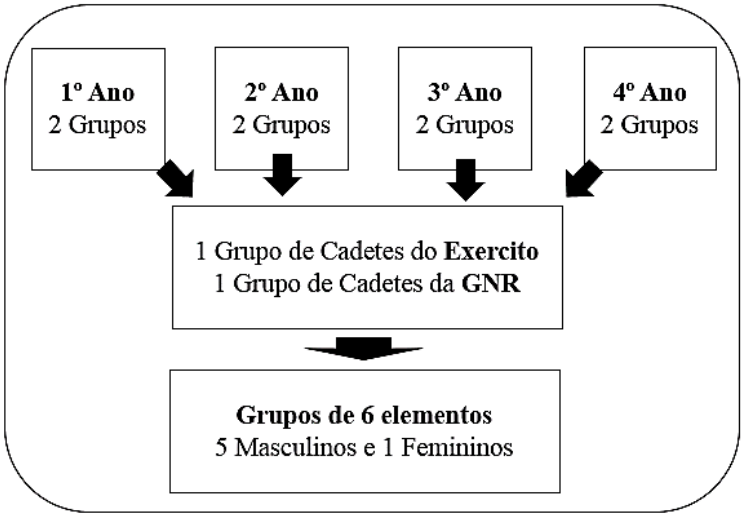
Uma amostra de uma investigação é uma parte da população que queremos observar, sendo que a população é "um conjunto de unidades individuais, que podem ser pessoas, animais ou resultados experimentais, com uma ou mais características em comum, que se pretendem analisar" (Neves, Silva, & Guerreiro, 2016, p. 30). Considera-se que a população desta investigação são os utilizadores do *e-mail* do Exército, já que o objetivo é sensibilizar os mesmos.

Com esta população, e como não há a possibilidade de estudar a população como um todo, definiu-se que a amostra seriam os cadetes[3] da academia militar, por facilidade de acesso e em virtude destes serem um bom elemento de investigação, porque se espera que tenham mais conhecimento e predisposição que os restantes militares.

Uma amostra é "uma parte da população que é observada com o objetivo de obter informações para estudar a característica pretendida" (Neves, Silva, & Guerreiro, 2016, p. 30), sendo que a característica que se pretende estudar será a eficácia da sessão de sensibilização, através dos questionários, de forma a validar o processo de *awareness*.

[3] Apesar de os cadetes não terem acesso ao *e-mail* do Exército, esta sensibilização é genérica a qualquer tipo de sistema *e-mail*, e por este facto não é relevante o acesso ao mesmo, como também pode-se integrar os cadetes da GNR nesta investigação, que o resultado final irá manter-se.

Quadro 3. 5 - Amostra inicial



Fonte: Elaboração Própria

A escolha inicial era para serem só elementos do Exército, mas como a amostra deve ser o mais aleatória possível (Neves, Silva, & Guerreiro, 2016), foram incluídos os elementos da GNR. Assim, foi pedido a cada CAL da Academia Militar, dois grupos de seis alunos, um de cadetes do Exército, e outro da GNR, como se pode verificar no quadro 3.5.

Pode-se também verificar que a escolha dos seis elementos foi restringida a cinco elementos do sexo masculino e um elemento do sexo feminino, como também foi pedido que todos os elementos tivessem conhecimento informático na ótica do utilizador, bem como noções elementares da língua inglesa, para a leitura dos questionários.

O plano de investigação inicial iria contemplar, apenas, os quarenta e oito elementos escolhidos aleatoriamente, mas com o apoio do meu orientador, consegui aumentar a amostra em cinquenta e oito elementos.

Ao todo, foram aplicados questionários em cento e seis cadetes, que serão analisados no quarto capítulo. O molde em que a investigação foi dirigida vai ser pormenorizado no próximo subcapítulo, terminando, assim, a explicação dos métodos e técnicas do trabalho de campo.

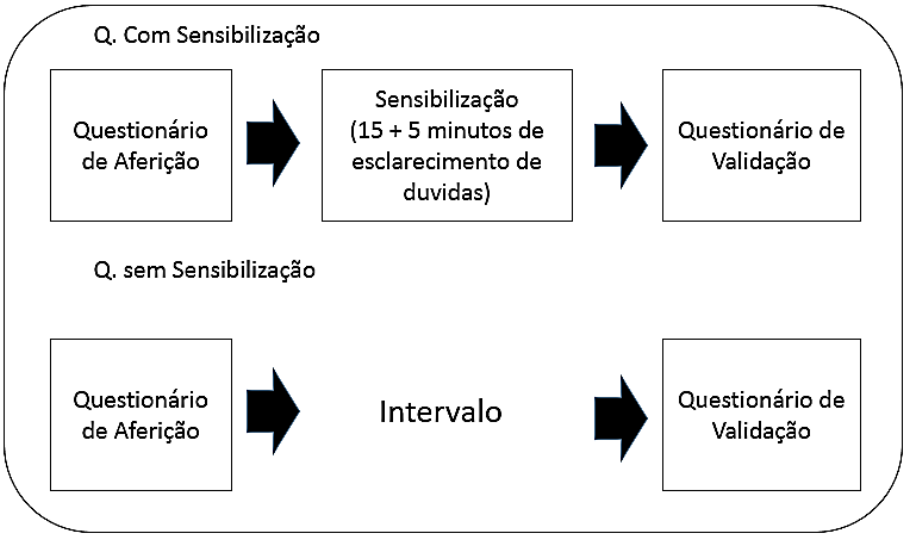
3.4.2. Formato do estudo

No estudo, segui os moldes já ilustrados no quadro 3.1 que é um processo de *awareness* do tipo treino incorporado, onde, submetemos os utilizadores, ao contexto

específico de um ataque com avaliação (Hong, 2012).

Para aferir os resultados do primeiro questionário, que é o contexto específico de um ataque de *phishing* e da sua respetiva sensibilização, alguns elementos não podiam ter acesso à sensibilização de forma a comparar as diferenças na análise dos dados. Assim, como podemos ver no quadro 3.6, temos dois grupos, aqueles que efetuam os questionários com sensibilização e os que efetuam só os questionários.

Quadro 3. 6 - Configuração do estudo



Fonte: Elaboração Própria

Assim, tanto na primeira amostra, que foram os quarenta e oito escolhidos pelas CAL, como na segunda, que foram os alunos disponibilizados pela Unidade Curricular, E361 (Segurança da Informação de Sistemas de Informação e Ciberdefesa,), os grupos foram divididos.

No caso da primeira amostra, foram divididos por ramos, GNR e Exército, assim por cada ano temos os dois grupos, um escolhido para ter sensibilização, outro não, alternadamente. No segundo caso, a turma foi dividida em dois, aleatoriamente, com o objetivo de obter dois grupos com mesmo número de alunos.

O estudo decorreu, como descrito no quadro 3.6, para ambos os casos, numa sala do Aquartelamento da Academia Militar na Amadora.

No início, os cadetes efetuavam o questionário de aferição, e assim que terminado,

os elementos que não teriam sensibilização sairiam da sala.

A sensibilização pode ser feita num molde em que um orador apresenta o produto seguindo os passos de Thomas Peltier, suportado no artigo *Implementing an information security Awareness Program* (2005) mas, como um dos objetivos da investigação é criar um produto genérico de sensibilização para o Exército Português, colocar aqui um elemento humano seria influenciar os resultados da investigação, por existir a questão "Qual a influência do orador na sensibilização?".

Desta forma, a sensibilização foi executada através da visualização e esclarecimento de dúvidas do produto, que foi a apresentação em PowerPoint. Para evitar que os recetores saíssem da apresentação, sem a terem verificado até ao final, o ficheiro que lhes foi passado foi gravado em modo Apresentação de Diapositivos do Microsoft PowerPoint (.ppsx), que não permite ao utilizador alterar o ficheiro, e ainda o responsável pela sensibilização(o investigador) esteve a controlar a sessão.

A visualização teve um tempo estipulado de quinze minutos obrigatórios, ao qual os recetores tinham desconhecimento, e por esta razão, nenhum se sentiu pressionado pelo o tempo. Após os quinze minutos de visualização, houve cinco minutos para os elementos colocarem questões em relação ao produto e ao tema. Estes tempos serviram como referência de forma a não estender a sensibilização para fora do período dos cinquenta minutos, sustentados por Thomas Peltier (2005).

Por fim, os elementos em intervalo eram chamados e ambos os grupos executaram o questionário de validação. Para ambos os questionários não existiu tempo limite e os elementos só saíriam da sala quando todos acabassem. A sessão, em média, durou quarenta minutos, dez minutos para cada questionário e vinte para a sensibilização. Os tempos descritos anteriomente, foram sempre respeitados, não existindo nenhum elemento a precisar de mais tempo para executar as tarefas.

No próximo capítulo é feita a análise dos dados e discussão dos mesmos.

CAPÍTULO 4
ANÁLISE E DISCUSSÃO DOS RESULTADOS

Neste capítulo é feita a análise qualitativa dos dados obtidos no trabalho de campo, com o objetivo de validar a investigação. Procura-se que a sensibilização "…reduza o impacto dos ataques de *phishing* executados através do seu sistema de *e-mail*?".

Na ótica desta investigação, o impacto será reduzido se existir uma diminuição dos erros nas escolhas das amostras do primeiro questionário para o segundo questionário, no caso dos elementos que realizam a ação de sensibilização. A influência da apresentação será colocada a prova com os elementos que não tiveram acesso a ela, já que não se prevê que existam melhorias dos resultados obtidos, do primeiro questionário para o segundo.

Desta forma, temos uma variável mensurável que podemos analisar e relacionar com o objetivo desta investigação, utilizando a estatística descritiva para a interpretação destes dados numéricos.

4.1. Estatística descritiva

Utiliza-se a estatística descritiva, que "consiste na recolha, apresentação, análise e interpretação de dados numéricos através da criação de instrumentos adequados: quadros, gráficos e indicadores numéricos." (Reis, 2012, p. 15).

Pretende-se uma análise qualitativa do efeito do processo de *awareness* e todos os quadros e gráficos apresentados neste estudo foram criados com suporte no IBM SPSS Statistics, como programa de análise estatística.

Utilizou-se as etapas do método estatístico de Elizabeth Reis (2012) para dar início à análise dos dados recolhidos.

A primeira etapa foi identificar o problema, já descrito em cima, que será "reduzir o impacto". Uma vez identificado o problema, recolhemos os dados necessários, que no caso desta investigação são dados primários, isto é "dados resultantes de inquéritos feitos diretamente a uma população ou a um grupo dessa população" (Reis, 2012, p. 17) e em relação à periodicidade da recolha de dados, podemos considerar ocasional por ser realizada de modo esporádico.

O terceiro passo será a critíca dos dados, que é necessária quando a informação provém de fontes secundárias, que poderá estar sujeita a erros de reprodução. Este dados, apesar de serem fontes primárias, estão sujeitos ao erro humano, já que toda a verificação e reprodução dos dados em sistema informático não foi feito de forma automática, mas sim manualmente, mas não se prevê que seja significativo.

O quarto e quinta passo são respectivamente a apresentação dos dados e análise e interpretação dos resultados, que será executado nos subcapítulos seguintes.

Assim, esta análise vai seguir esta ordem de ideias que define o método estatístico de resolução de problemas apresentado por Elizabeth Reis (2012), como é exposto na figura 4.1.

Figura 4. 1 - Método estatístico de resolução de problemas

Fonte: adaptado de Reis (2012)

4.2. Apresentação dos dados

Para facilitar a análise do subcapítulo seguinte, convém organizar-se os dados de forma a permitir um melhor entendimento do fenómeno que se pretende estudar. O objetivo será, então, apresentar e classificar um conjunto de dados numéricos de forma a facilitar a sua compreensão e análise.

A classificação consiste na identificação de unidades de informação com características comuns (Reis, 2012). Terminada a classificação, já é possível apresentar os dados em tabelas e gráficos que ajudem a compreender melhor a situação e identificar as relações importantes.

Desta forma, começou-se a classificar os valores obtidos dos questionários. Numa primeira abordagem, queremos estudar como a amostra reagiu aos questionários e, numa segunda fase, o estudo dos questionários em si.

Primeiro desafio é diferenciar as amostras, utilizando os dados sociodemográficos para tal, mas existiu a necessidade de criar mais uma variável que seria a exposição ou não à sensibilização. Variáveis como o ramo, o género, se já era militar e a exposição à sensibilização são dicotómicas porque podem apenas tomar dois valores possíveis (Reis, 2012). Na tabela 4.1 temos então a contagem de todas as variáveis e a média de idades da amostra. Temos assim, ao todo, cento e seis elementos, cinquenta e cinco com acesso a apresentação e cinquenta e um sem acesso.

Tabela 4. 1 - Dados Sociodemográficos

		Contagem	Média
Ramo	EXE	51	
	GNR	55	
Ano	1ºano	12	
	2ºano	40	
	3ºano	41	
	4ºano	13	
Curso	Engenharia	14	
	Armas	84	
	Administração	5	
	Medicina	3	
Militar Antes	Sim	12	
	Não	94	
Idade			20,95
Género	Masculino	96	
	Feminino	10	
Tipo de questionário	C/ apresentação	55	
	S/ apresentação	51	

Legenda: A tabela apresenta os dados sociodemográficos da amostra total e o número de elementos que tiveram acesso ou não à ação de sensibilização.

Pode-se observar que existe um número reduzido de elementos do sexo feminino, sendo pouco relevante uma análise ao nível do género. Isto será um dos constrangimentos da Academia Militar em que a maioria dos alunos é do sexo masculino. Pode-se observar, também, que a nível dos cursos, o curso de armas será o mais abundante, já que também é a

maioria, tanto na GNR como no Exército Português. A média das idades é, aproximadamente, vinte e um anos, sendo um valor normal, já que a maioria dos elementos é do segundo e terceiro ano.

Para análise dos questionários foram criadas seis variáveis de estudo: respostas corretas, repostas incorretas e o desconhecimento da resposta, no questionário de aferição e equivalentes variáveis para o questionário de validação. Nas tabelas 4.2 e 4.3, pode-se ver o número de respostas "corretas", "erradas" ou "não sei" como valor estático relacionado com número de elementos que acertou esse valor, dividido em quem foi exposto a apresentação ou não.

Remetendo para os questionários, existem vinte e cinco perguntas em que os elementos têm de escolher uma opção (legítimo, ilegítimo ou não sei). Esta escolha pode estar "correta", "errada" ou simplesmente os elementos podem escolher que não sabem a resposta. A soma das escolhas "corretas", "erradas" e "não sei" de cada elemento, é valor que é introduzido nas tabelas 4.2 e 4.3.

Assim como exemplo para a tabela 4.2, nos cinquenta e cinco elementos, com apresentação, 6 destes acertaram exatamente doze respostas e nos cinquenta e um, sem apresentação, 6 elementos acertaram doze respostas (assinalado a azul claro na tabela 4.2).

Na tabela 4.3, os dados estão organizados da mesma forma que a tabela anterior (4.2), sendo que a tabela 4.2 retrata os valores obtidos no questionário de aferição e a 4.3 do questionário de validação.

Tabela 4. 2 - Dados da Aferição

		Corretas		Erradas		Não sei	
		C/ apresentação	S/ apresentação	C/ apresentação	S/ apresentação	C/ apresentação	S/ apresentação
Número de Respostas	0,00					10	10
	1,00				2	4	1
	2,00			2	1	4	4
	3,00		3	2	1	8	4
	4,00			5	3	6	4
	5,00	2		2	6	6	4
	6,00	3	1	5	4	2	6
	7,00	1	2	8	11	6	6
	8,00	3	2	6	2	1	3
	9,00	4	2	10	7	1	1
	10,00	2	7	4	4	2	1
	11,00	8	3	1	3	2	2
	12,00	6	6	1	3	1	3
	13,00	3	5	4	2	1	
	14,00	6	7	3	1		
	15,00	9	5	1			
	16,00	2	3				
	17,00	3	4		1		2
	18,00	1	1			1	
	19,00	2		1			
Total		55	51	55	51	55	51

Legenda: Os valores apresentados na tabela apresentam o número de elementos que teve um certo número de respostas "corretas", "erradas" e de "não sei" no questionário de Aferição.

Não existem grandes disparidades entre os valores dos elementos com ação de sensibilização e aqueles não lhes foi aplicado a ação (tabela 4.2), porque estes dados são retirados do primeiro questionário, em que não existe influência da ação de sensibilização. O mesmo não acontece na tabela 4.3, que apresenta um leque de resultados que se estende do valor zero ao vinte e dois (assinalado a verde) e que na tabela anterior (tabela 4.2) se estendia do zero ao dezanove (assinalado a verde). Como exemplo para a tabela 4.3, nos cinquenta e cinco elementos, com apresentação, oito destes acertaram exatamente dezanove respostas e nos cinquenta e um, sem apresentação, só um elemento acertou dezanove respostas (assinalado a azul claro na tabela).

Tabela 4. 3 - Dados da Validação

		Corretas		Erradas		Não sei	
		C/ apresentação	S/ apresentação	C/ apresentação	S/ apresentação	C/ apresentação	S/ apresentação
Número de Respostas	0,00					26	11
	1,00			1		10	2
	2,00			1	3	4	
	3,00			4	3	3	8
	4,00		1	7	1	7	3
	5,00		1	8	8	1	8
	6,00		1	7	6	2	4
	7,00		1	11	4	2	2
	8,00		1	4	5		4
	9,00		5	5	3		6
	10,00	1	6	2	7		1
	11,00	1	3	2	4		
	12,00	1	7	1	1		
	13,00	3	3	2	2		
	14,00	5	8		2		1
	15,00	5	6		2		
	16,00	6	2				
	17,00	9	4				
	18,00	7					1
	19,00	8	1				
	20,00	5	1				
	21,00	2					
	22,00	2					
Total		55	51	55	51	55	51

Legenda: Os valores apresentados na tabela apresentam o número de elementos que teve um certo número de respostas "corretas", "erradas" e de "não sei" no questionário de Validação.

Pelo exemplo anterior, pode-se verificar que existiu uma melhoria dos elementos com acesso à ação de sensibilização. Ao olhar para a tabela 4.3 conseguimos retirar que os elementos "c/ apresentação" tiveram os seus resultados alterados de forma a obter um maior número de respostas corretas (sempre superior a dez respostas corretas), e um menor número de respostas erradas ou de desconhecimento, em que se destaca os vinte e seis elementos que nunca aplicaram a escolha de "não sei" (assinalado a vermelho). Os elementos que não tiveram acesso à ação de sensibilização, por comparação das duas tabelas (4.2 e 4.3), não alteraram os seus resultados significativamente.

Na segunda fase, em que se estuda os questionários, este é destinado unicamente às amostras expostas à sensibilização porque só nestas é que se obteve diferenças de resultado significativas (como se verifica nas tabelas 4.2 e 4.3). Os questionários têm vinte e cinco

imagens, e elas podem ser legítimas ou ilegítimas. Os elementos podem escolher três opções, "legítimo", "ilegítimo" e "não sei". Só existe uma resposta correta, dependo da imagem que se está a estudar, "legítimo" se esta não representar um e-mail de *phishing* e "ilegítimo" se representar um e-mail de *phishing*. Os elementos podem ainda escolher a opção de "não sei" se não tiverem a certeza da sua escolha.

Pretende-se estudar o número de escolhas para cada imagem e criou-se cinco variáveis: a resposta correta, o número de respostas "legítimo", "ilegítimo" e "não sei" e o tipo de *e-mail* que era, podendo ser um *e-mail* normal ou um *Ad*.

As próximas tabelas 4.4 e 4.5, representam os dados, respetivamente, do questionário de aferição e do questionário de validação dos elementos com acesso à ação de sensibilização, mas claro que existe maior interesse nos dados do questionário de validação (Tabela 4.5) de forma a perceber quais os erros mais comuns ou mesmo o porquê desses erros. Como exemplo, na tabela 4.4, a imagem 1, que a resposta correta é Ilegítimo, houve vinte elementos que escolheram "legítimo", vinte e um que escolheram "ilegítimo" (a resposta correta) e catorze escolheram "não sei" (assinalado a azul claro na tabela).

Tabela 4. 4 - Respostas ao questionário de aferição

		Número de respostas			
	Resposta	Legítimo	Ilegítimo	Não sei	Tipo
Imagem 1	Ilegítimo	20,00	21,00	14,00	*e-mail*
Imagem 2	Ilegítimo	26,00	25,00	4,00	*e-mail*
Imagem 3	Legítimo	47,00	4,00	4,00	*e-mail*
Imagem 4	Legítimo	35,00	5,00	15,00	*e-mail*
Imagem 5	Ilegítimo	12,00	38,00	5,00	*e-mail*
Imagem 6	Legítimo	5,00	38,00	12,00	AD
Imagem 7	Ilegítimo	14,00	37,00	4,00	*e-mail*
Imagem 8	Ilegítimo	10,00	38,00	7,00	*e-mail*
Imagem 9	Ilegítimo	20,00	25,00	10,00	*e-mail*
Imagem 10	Ilegítimo	31,00	15,00	9,00	*e-mail*
Imagem 11	Legítimo	21,00	23,00	11,00	AD
Imagem 12	Ilegítimo	15,00	34,00	6,00	*e-mail*
Imagem 13	Ilegítimo	2,00	45,00	8,00	*e-mail*
Imagem 14	Legítimo	7,00	36,00	12,00	AD
Imagem 15	Legítimo	28,00	18,00	9,00	*e-mail*
Imagem 16	Ilegítimo	12,00	29,00	14,00	*e-mail*
Imagem 17	Ilegítimo	12,00	28,00	15,00	*e-mail*
Imagem 18	Ilegítimo	8,00	40,00	7,00	*e-mail*
Imagem 19	Ilegítimo	10,00	38,00	7,00	*e-mail*
Imagem 20	Legítimo	24,00	22,00	9,00	*e-mail*
Imagem 21	Legítimo	33,00	7,00	15,00	*e-mail*

Imagem 22	Ilegítimo	33,00	11,00	11,00	*e-mail*
Imagem 23	Legítimo	18,00	21,00	16,00	*e-mail*
Imagem 24	Ilegítimo	9,00	40,00	6,00	*e-mail*
Imagem 25	Legítimo	16,00	24,00	15,00	AD

Legenda: Na primeira coluna temos o numero da imagem, seguido da resposta correta a imagem, numero de respostas de "legítimo", "ilegítimo" e "não sei" e o tipo de *e-mail*.

Estas tabelas (4.4 e 4.5) serão analisadas posteriormente, mas pode-se verificar logo pela imagem 1 que na tabela 4.5 os elementos foram mais precisos em identificar a resposta correta, do que na tabela 4.4. Assim como exemplo, na tabela 4.5, a imagem 1, que a resposta correta é Ilegítimo, houve dois elementos que escolheram "legítimo", cinquenta que escolheram "ilegítimo" (a resposta correta) e três escolheram "não sei" (assinalado a azul claro na tabela).

Tabela 4. 5 - Respostas ao questionário de validação

		Número de respostas			
	Resposta	Legítimo	Ilegítimo	Não sei	Tipo
Imagem 1	Ilegítimo	2,00	50,00	3,00	*e-mail*
Imagem 2	Legítimo	24,00	29,00	2,00	AD
Imagem 3	Legítimo	45,00	10,00		*e-mail*
Imagem 4	Legítimo	39,00	13,00	3,00	*e-mail*
Imagem 5	Ilegítimo	4,00	51,00		*e-mail*
Imagem 6	Ilegítimo	2,00	52,00	1,00	*e-mail*
Imagem 7	Ilegítimo	5,00	47,00	3,00	*e-mail*
Imagem 8	Ilegítimo	6,00	47,00	2,00	*e-mail*
Imagem 9	Ilegítimo	6,00	48,00	1,00	*e-mail*
Imagem 10	Ilegítimo	18,00	36,00	1,00	*e-mail*
Imagem 11	Legítimo	16,00	30,00	9,00	AD
Imagem 12	Ilegítimo	14,00	48,00	3,00	*e-mail*
Imagem 13	Ilegítimo	1,00	50,00	4,00	*e-mail*
Imagem 14	Legítimo	8,00	40,00	7,00	AD
Imagem 15	Legítimo	17,00	33,00	5,00	*e-mail*
Imagem 16	Legítimo	9,00	42,00	4,00	*e-mail*
Imagem 17	Legítimo	9,00	42,00	4,00	*e-mail*
Imagem 18	Ilegítimo	2,00	51,00	2,00	*e-mail*
Imagem 19	Ilegítimo	8,00	46,00	1,00	*e-mail*
Imagem 20	Legítimo	19,00	30,00	6,00	AD
Imagem 21	Ilegítimo		53,00	2,00	*e-mail*
Imagem 22	Ilegítimo	14,00	36,00	5,00	*e-mail*
Imagem 23	Legítimo	23,00	20,00	12,00	*e-mail*
Imagem 24	Ilegítimo	2,00	52,00	1,00	*e-mail*
Imagem 25	Ilegítimo	7,00	45,00	3,00	*e-mail*

Legenda: Na primeira coluna temos o número da imagem, seguido da resposta correta à imagem, número de respostas de "legítimo", "ilegítimo" e "não sei" e o tipo de *e-mail*.

No próximo subcapítulo, são apresentados os dados anteriores com recurso a gráficos e tabelas elaboradas, com a finalidade de simplificar a análise e permitir um melhor entendimento, o que possibilita, extrair resultados relevantes para a investigação e comparação dos mesmos.

4.3. Análise e interpretação

Como já foi referido, pretende-se, então, tirar as conclusões necessárias dos dados recolhidos neste subcapítulo. Como referido por Elizabeth Reis (2012) "esta interpretação estará tanto mais facilitada quanto se tiverem escolhido, em etapas anteriores, os instrumentos mais apropriados à representação e análise do tipo de dados recolhidos". Diz, também, que existe a possibilidade de conclusões enviesadas, mas que estas não são propositadas porque advêm da utilização de medidas de estatistica descritiva pouco adequadas ou por bases comparação também inadequadas.

A representação gráfica é, talvez, o modo mais simples de descrever a realidade nos seus aspetos mensuráveis, já que este é um instrumento de síntese que permite a utilização da visão para nos apercebermos imediatamente da forma geral, sem deixar de evidenciar alguns aspetos particulares (Reis, 2012).

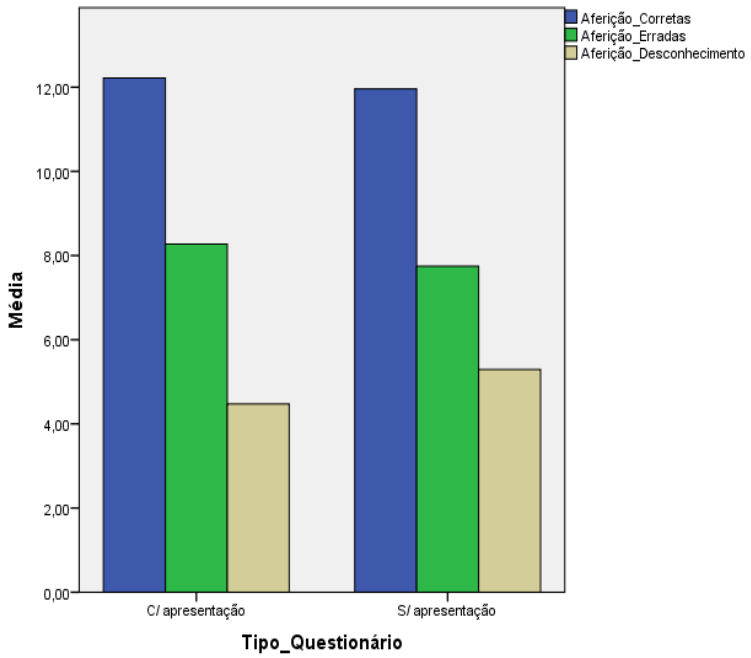
No caso desta investigação, o único que se prevê necessário será o estudo das variáveis referentes aos questionários, relativamente à exposição à sensibilização e, para isso um gráfico de barras é um meio excelente, já que nos permite observar várias frequências para situações diferentes.

Como é lógico, também não será analisado cada dado como elemento singular, pois não conseguiríamos tirar conclusões significativas. Vai ser utilizada a média aritmética, já que esta é influenciada por todos os valores observados e a possibilidade de enviesamento existe unicamente quando existem valores extremos ou a distribuição for altamente assimétrica (Reis, 2012), que não é o caso.

Nesta linha de pensamento, foram criadas as tabelas seguintes com intuito de avaliar a diferença entre os elementos expostos à sensibilização e os que não foram expostos:

No gráfico (gráfico 4.1) pode-se verificar que não existem diferenças visíveis entre os elementos de ambos os testes, obtendo dois gráficos de barras idênticos, em que a média de todos os resultados (corretas, erradas e não sei) não apresenta diferenças significativas. É uma análise que já se estava a prever, porque nenhum dos grupos teve inicialmente qualquer tipo de influência que podesse modificar a suas escolhas, ao contrário do que acontecerá no próximo gráfico em que existiu a influência da ação de sensibilização.

Gráfico 4. 1 - Comparação de médias do questionário de aferição



Legenda: O gráfico de barras encontra-se dividido entre a média de respostas dos elementos com sensibilização e sem sensibilização. A azul temos respostas "corretas", a verde respostas "erradas" e a castanho respostas "não sei".

Na tabela seguinte (Tabela 4.6), temos os valores do gráfico 4.1. Pode-se verificar as médias e o desvio padrão para cada grupo de elementos. O desvio padrão, indica a extensão de valores que foram usados para efetuar a média, sendo que quanto maior for o desvio padrão, maior será a dispersão de valores (Reis, 2012). Como exemplo, temos que a média de escolha de "não sei" é 4,5 e o desvio padrão de 3,9 (assinalado a azul claro na tabela). Isto indica que a média foi feita com valores que se afastam desta em 3,9 (desde 0,6 a 8,4), sendo este valor sempre uma aproximação. Pode-se observar que a escolha de desconhecimento é a que teve mais valores distintos.

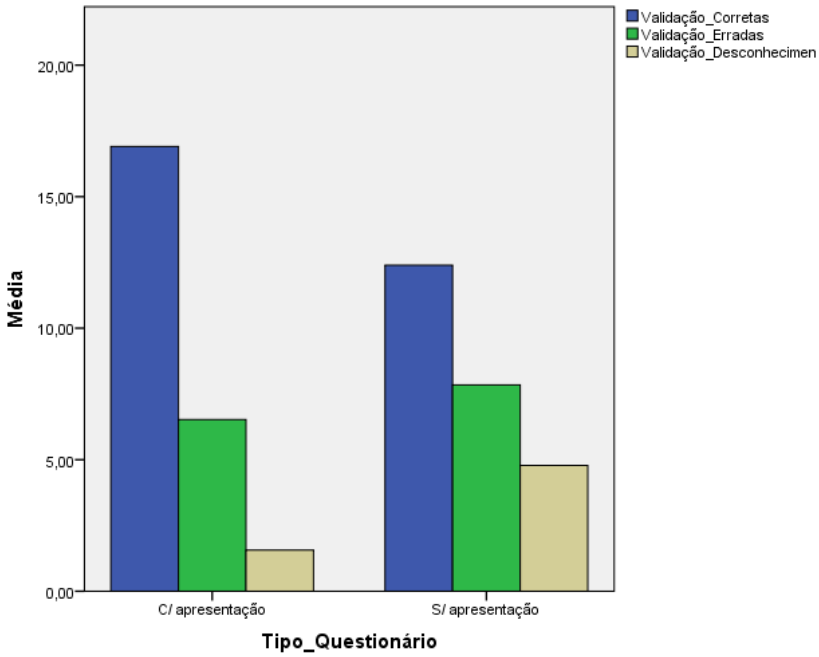
Tabela 4. 6 - Tabela de médias e desvio padrão para o questionário de aferição

		Corretas	Erradas	Não sei
C/ Sensibilização	Média	12,2	8,2	4,5
	Desvio Padrão	3,5	3,5	3,9
S/ Sensibilização	Média	11,9	7,7	5,3
	Desvio Padrão	3,6	3,3	4,3
Total	Média	12,0	8,0	4,9
	Desvio Padrão	3,5	3,4	4,1

Legenda: Na tabela encontra-se a média e desvio padrão para respostas "corretas, "incorretas" e "não sei", dos elementos com acesso a sensibilização e sem acesso a ela.

Com o gráfico de barras (Gráfico 4.2), conseguimos verificar que existiu uma ligeira alteração nos elementos expostos à sensibilização. Conseguimos verificar que a média de opções corretas se alterou de, aproximadamente, doze respostas corretas para, aproximadamente, dezassete respostas corretas, sendo que o desvio padrão também alterou para um valor mais pequeno. Pode-se também retirar deste gráfico que os elementos utilizaram menos a opção de "não sei", uma média próxima de duas respostas. Os elementos não expostos à sensibilização continuaram a responder da mesma forma que no questionário anterior, provando que não foi a alteração de questionários, nem a prática que alterou os resultados.

Gráfico 4. 2 - Comparação de médias do questionário da Validação



Legenda: O gráfico de barras encontra-se dividido entre a média de respostas dos elementos com sensibilização e sem sensibilização. A azul temos respostas "corretas", a verde respostas "erradas" e a castanho respostas "não sei".

Na tabela seguinte (Tabela 4.7), temos os valores do gráfico 4.2. Pode-se verificar as médias e o desvio padrão para cada grupo de elementos. O desvio padrão, dos elementos com acesso à ação de sensibilização, diminui significativamente, como é exemplo a resposta" não sei" (assinalada a azul claro na tabela) que diminui de quatro valores para dois valores. Isto significa que, no geral, os elementos "c/sensibilização" tiveram mais valores semelhantes, isto é, que a dispersão de valores diminui. Com isto, e pelo facto de as respostas

corretas terem aumentado, isto significa uma melhoria generalizada de todos os elementos, e não só de alguns em particular.

Tabela 4. 7 - Tabela de médias e desvio padrão para o questionário de validação

		Corretas	Erradas	Não sei
C/ apresentação	Média	16,9	6,5	1,5
	Desvio Padrão	2,7	2,6	2,0
S/ apresentação	Média	12,3	7,8	4,7
	Desvio Padrão	3,4	3,4	3,9
Total	Média	14,7	7,1	3,1
	Desvio Padrão	3,8	3,1	3,4

Legenda: Na tabela encontra-se a média e desvio padrão para respostas "corretas, "incorretas" e "não sei", dos elementos com acesso a sensibilização e sem acesso a ela.

Verificamos, então, através dos resultados do gráfico 4.2, que a sensibilização alterou as escolhas dos elementos expostos, melhorando as suas escolhas por obterem uma melhor média de respostas corretas, provando então que, se dermos aos elementos argumentos para apoiar a decisão, como referido em o Kumaraguru, Sheng, Acquisti, Cranor, & Hong (2008), estes vão melhorar a resposta aos desafios, que neste caso seria o identificar os ataques de *phishing*.

Demonstra também, a utilização do conhecimento passado, que a *Theory of Deception* proposta por Grazioli (2004) indicou, já que através da visualização de um conjunto de imagens de deceção e tópicos de defesa, estes melhoraram a interpetação e reconhecimento de falhas nos formatos entre os *e-mail* e as suas experiências passadas. Esta melhoria é também observada através da análise das respostas aos questionários, que iremos discutir de seguida na tabelas 4.8 e 4.9. Pode-se ver que a média de respostas incorreta foi aquela que, em comparação entre os dois testes, teve a menor alteração. Resta saber se as respostas incorretas são a detectar *e-emails* legítimos ou ilegítimos, de forma a colmatar erros na própria sensibilização.

Na tabela 4.8, idêntica à tabela 4.4, temos as respostas ao questionário de aferição pelos elementos com acesso à ação de sensibilização. Desta vez temos as respostas corretas sublinhadas, a verde quando a resposta correta é "legítimo", e a vermelho quando a resposta correta é "ilegítima". A tabela 4.9 encontra-se da mesma forma.

Tabela 4. 8 - Respostas ao questionário de aferição (análise)

		Número de respostas			
	Resposta	Legítimas	Ilegítimas	Não sei	Tipo
Imagem 1	Ilegítimo	20,00	21,00	14,00	*e-mail*
Imagem 2	Ilegítimo	26,00	25,00	4,00	*e-mail*
Imagem 3	Legítimo	47,00	4,00	4,00	*e-mail*
Imagem 4	Legítimo	35,00	5,00	15,00	*e-mail*
Imagem 5	Ilegítimo	12,00	38,00	5,00	*e-mail*
Imagem 6	Legítimo	5,00	38,00	12,00	AD
Imagem 7	Ilegítimo	14,00	37,00	4,00	*e-mail*
Imagem 8	Ilegítimo	10,00	38,00	7,00	*e-mail*
Imagem 9	Ilegítimo	20,00	25,00	10,00	*e-mail*
Imagem 10	Ilegítimo	31,00	15,00	9,00	*e-mail*
Imagem 11	Legítimo	21,00	23,00	11,00	AD
Imagem 12	Ilegítimo	15,00	34,00	6,00	*e-mail*
Imagem 13	Ilegítimo	2,00	45,00	8,00	*e-mail*
Imagem 14	Legítimo	7,00	36,00	12,00	AD
Imagem 15	Legítimo	28,00	18,00	9,00	*e-mail*
Imagem 16	Ilegítimo	12,00	29,00	14,00	*e-mail*
Imagem 17	Ilegítimo	12,00	28,00	15,00	*e-mail*
Imagem 18	Ilegítimo	8,00	40,00	7,00	*e-mail*
Imagem 19	Ilegítimo	10,00	38,00	7,00	*e-mail*
Imagem 20	Legítimo	24,00	22,00	9,00	*e-mail*
Imagem 21	Legítimo	33,00	7,00	15,00	*e-mail*
Imagem 22	Ilegítimo	33,00	11,00	11,00	*e-mail*
Imagem 23	Legítimo	18,00	21,00	16,00	*e-mail*
Imagem 24	Ilegítimo	9,00	40,00	6,00	*e-mail*
Imagem 25	Legítimo	16,00	24,00	15,00	AD

Legenda: Na primeira coluna temos o número da imagem, seguido da resposta correta à imagem, número de respostas de "legítimo", "ilegítimo" e "não sei" e o tipo de *e-mail*. A resposta correta encontra-se sublinhada, para as imagens "legitimas" a verde e "ilegítimas" a vermelho. . Como exemplo, a imagem 1, a resposta correta é Ilegítimo, houve vinte elementos que escolheram "legítimo", vinte e uma que escolheram "ilegítimo"(a resposta correta) e catorze escolheram "não sei".

Na tabela anterior (tabela 4.8), pode-se verificar que existem imagens, que nesta primeira fase, tiveram índice de respostas corretas elevado. Desta tabela não se conseguirão tirar mais conclusões sem existir a comparação com a próxima.

Na tabela 4.9 e para terminar a análise e discussão dos dados, conseguimos verificar que em certas imagens, onde existia dúvida por parte de alguns elementos no questionário de aferição (tabela 4.8), com a ação de sensibilização conseguiram optar pela escolha correta.

Tabela 4. 9 - Respostas ao questionário de validação (análise)

		Número de respostas			
	Resposta	Legítimas	Ilegítimas	Não sei	Tipo
Imagem 1	Ilegítimo	2,00	50,00	3,00	*e-mail*
Imagem 2	Legítimo	24,00	29,00	2,00	AD
Imagem 3	Legítimo	45,00	10,00		*e-mail*
Imagem 4	Legítimo	39,00	13,00	3,00	*e-mail*
Imagem 5	Ilegítimo	4,00	51,00		*e-mail*
Imagem 6	Ilegítimo	2,00	52,00	1,00	*e-mail*
Imagem 7	Ilegítimo	5,00	47,00	3,00	*e-mail*
Imagem 8	Ilegítimo	6,00	47,00	2,00	*e-mail*
Imagem 9	Ilegítimo	6,00	48,00	1,00	*e-mail*
Imagem 10	Ilegítimo	18,00	36,00	1,00	*e-mail*
Imagem 11	Legítimo	16,00	30,00	9,00	AD
Imagem 12	Ilegítimo	14,00	48,00	3,00	*e-mail*
Imagem 13	Ilegítimo	1,00	50,00	4,00	*e-mail*
Imagem 14	Legítimo	8,00	40,00	7,00	AD
Imagem 15	Legítimo	17,00	33,00	5,00	*e-mail*
Imagem 16	Legítimo	9,00	42,00	4,00	*e-mail*
Imagem 17	Legítimo	9,00	42,00	4,00	*e-mail*
Imagem 18	Ilegítimo	2,00	51,00	2,00	*e-mail*
Imagem 19	Ilegítimo	8,00	46,00	1,00	*e-mail*
Imagem 20	Legítimo	19,00	30,00	6,00	AD
Imagem 21	Ilegítimo		53,00	2,00	*e-mail*
Imagem 22	Ilegítimo	14,00	36,00	5,00	*e-mail*
Imagem 23	Legítimo	23,00	20,00	12,00	*e-mail*
Imagem 24	Ilegítimo	2,00	52,00	1,00	*e-mail*
Imagem 25	Ilegítimo	7,00	45,00	3,00	*e-mail*

Legenda: Na primeira coluna temos o número da imagem, seguido da resposta correta à imagem, número de respostas de "legítimo", "ilegítimo" e "não sei" e o tipo de *e-mail*. A resposta correta encontra-se sublinhada, para as imagens "legítimas" a verde e "ilegítimas" a vermelho. Assim como exemplo, a imagem 1, a resposta correta é Ilegítimo, houve dois elementos que escolheram "legítimo", cinquenta que escolheram "ilegítimo" (a resposta correta) e três escolheram "não sei"

As respostas incorretas, como se pode verificar na tabela 4.9, são a identificar os *e-mails* legítimos, podendo isto ser uma falha dos questionários por existirem imagens que, apesar de serem de *e-mails* legítimos, têm grandes parecenças a *e-mails* ilegítimos, por também incluírem *Visceral Triggers*. Com isto, também é colocada à prova a teoria citada de Langenderfer & Shimp (2001), que explica a resposta intuitiva às imagens, que é caso das imagens do tipo *Ad* e a imagens 15,16 e 17.

As imagens do tipo *Ad*, ou propaganda da internet, não foram reconhecidas como legítimas apesar de a imagem conter o próprio símbolo característico no canto superior direito da imagem (ver Apêndice A e B), isto foi uma falha tanto da sensibilização como

uma limitação de estudo já que não existe a possibilidade de poder abordar todo o conteudo que poderá aparecer no sistema *e-mail*.

A imagem 23, para o questionário de validação, causou confusão aos elementos apesar de ser um típico *e-mail* de uma empresa. A única justificação podemos repreender será a questão da língua inglesa que apesar de, no início da investigação, um dos requisitos dos participantes seria o conhecimento da língua inglesa, no trabalho de campo e, por razões exteriores à investigação, alguns elementos, do primeiro teste, tinham pouco conhecimento da língua inglesa que poderá ter provocado esta variação.

Com estudo destas ultimas tabelas (4.8 e 4.9), verificou-se mais uma vez a *Theory of Deception* de Grazioli (2004), já que o único conhecimento que lhe foi induzido seria contra *e-mails* ilegítimos, e estes ao encontrarem pela frente as imagens de propaganda, trataram da mesma forma que os *e-mails* ilegítimos por não terem outro conhecimento.

Pode-se verificar também (tabela 4.9) que existiu uma diminuição significativa da escolha de "não sei" em comparação com a tabela anterior (tabela 4.8), isto porque os elementos no questionário de aferição, encontravam os ataques de *phishing*, sem conhecimento prévio e este apresentava-se como uma novidade. No questionário de validação, os elementos tinham já um conhecimento mais elaborado do tema (proveniente da apresentação de sensibilização), diminuindo a sua incerteza.

Concluindo, o processo de awareness aos ataques *phishing* teve um resultado satisfatório, pelo aumento das escolhas corretas, a identificar *e-mails* ilegítimos, que para esta investigação significa a redução do impacto dos ataques de *phishing* (objectivo da investigação). As escolhas incorretas, na maioria, foram a imagens de *e-mail* legítimos, falha provável da ação de sensibilização como foi explicado anteriormente, mas que não compremete o objectivo de investigação.

CONCLUSÕES

Esta investigação tem como objetivo "efetuar o *design* de um processo de *awareness* para o Exército que reduza o impacto dos ataques de *phishing* executados através do seu sistema de *e-mail*?". Apresenta-se um processo de *awareness* para os ataques de *phishing* e demonstra-se que este reduz o impacto como desejado, isto é, o impacto, foi reduzido porque existiu uma diminuição dos erros nas escolhas das amostras do primeiro questionário para o segundo questionário, no caso dos elementos sujeitos à ação de sensibilização.

Em relação às teorias comportamentais, constatou-se que as mais relevantes para os ataques de *phishing* serão *Theory of Deception* e *Attention to Visual Triggers*, não descurando a importância das outras, mas de uma forma mais prática, estas responderam à primeira pergunta derivada da investigação, confirmando assim a hipótese desta investigação.

Verificou-se ainda que, o método de ensino ativo, utilizando os estilos de aprendizagem auditivo, mecânico e visual, permite alterar comportamento (segunda hipótese da investigação) e que os jogos e o treino incorporado serão a melhor opção neste sentido (resposta à questão derivada número dois). Com mais tempo para realizar o estudo poderíamos ter estudado as abordagens de falha-correção que é o tipo utilizado no programa *PhishGuru* [4]ou mesmo a abordagem do *Role-play*[5].

Em relação à terceira questão colocada, o meio (isto é, o produto para ministrar a ação de sensibilização) vai depender fundamentalmente do tipo de organização e do método de *awareness* utilizado. No caso desta investigação, o meio consiste no programa de apresentação PowerPoint (confirmando a terceira hipótese de investigação e respondendo a esta).

Por fim, o critério de avaliação utilizado foi a comparação entre elementos sem sensibilização e elementos com sensibilização, para se verificar se existia ou não a redução

[4] Abordagem apresentada anteriormente, em que após falha dos elementos em estudo, efetua-se um correção através do ensino.

[5] A abordagem role-play é colocar os elementos em estudo numa situação de um ataque, de forma a verificar o seu comportamento e altera-lo se necessário.

das escolhas erradas (confirmando a quarta hipótese). Fora do âmbito de investigação, a comparação dos questionários será o melhor método de avaliação por nos permitir verificar diretamente se existiu melhoria nos elementos expostos a sensibilização.

Confirmam-se, assim, as quatro hipóteses de investigação levantadas, que respondem aos objetivos particulares, e estes por sua vez, apoiam esta investigação já que, através destes conseguimos produzir um produto que respondesse ao objetivo final do trabalho.

Esta investigação possui algumas limitações, tendo como principal a temporal, pois nove semanas para planear, executar e validar uma sessão de *awareness* revelou-se uma tarefa bastante exigente e complexa. Também não houve tempo para melhorias na apresentação de sensibilização, que durante todo o espaço-tempo de investigação sofreu alterações, em virtude da consolidação de conhecimentos do investigador ao longo do estudo (exemplo de obtenção de conhecimentos baseados na Psicologia Cognitiva e ainda no estudo do estudo da *Neuro-Linguistic Programming* para melhorar a comunicação e comportamentos).

Algumas das possíveis melhorias, passariam ainda pela introdução da propaganda do sistema de *e-mail* na sensibilização ou mesmo executar o teste com elementos que não apresentassem dificuldades ao nível de inglês.

Pode-se também assinalar o facto de não se utilizar nem testar outros programas já concebidos para o efeito, e apresentados ao longo do trabalho. No entanto, devido à falta de conhecimento, o facto de este trabalho ser individual e a falta de fundos monetários, essas ideias foram colocadas de parte, e executou-se algo mais simples e com menos recursos.

Por último, esta sensibilização deveria ser incluída num leque sessões do mesmo género (processo de *awareness* de segurança) para os elementos obterem um conhecimento genérico e não existir falhas. No caso desta investigação, a falha é a propaganda que existe nos sistemas de *e-mail*s, que confundiu os recetores.

Sugere-se que o processo de *awareness* criado nesta investigação possa ser usado pelo Exército Português em processos de *awareness* de segurança de forma a diminuir o risco destes tipos de ataques de engenharia social. Recomenda-se ainda que seja feita uma revisão a toda a investigação, aplicando o processo de *awareness* a outras amostras no interior da organização militar (possíveis grupos: oficiais, sargentos, praças e funcionários civis), se acrescentem novos conhecimentos a este processo e por fim melhorias ao meio, ou seja ao produto com o qual se realiza a ação de sensibilização (por exemplo, explorar o desenvolvimento de jogos).

Possíveis investigações futuras nesta temática poderão abordar a influência do orador nas sessões de sensibilização e se o conhecimento perdura com o passar do tempo, isto é, qual a frequência com que é necessário repetir a ação de sensibilização numa organização.

Para finalizar, o melhor que se pode esperar no combate ao *phishing* é diminuir o sucesso deste, pois as vulnerabilidades humanas sempre existirão. Temos de continuar a trabalhar para obter as melhores formas para os prevenir e detetar, utilizando o elemento humano como sensor da organização, integrado com mecanismos tecnológicos de segurança.

REFERÊNCIAS BIBLIOGRÁFICAS

ISSO/IEC(271001) (2005). *ISO/IEC FDIS 27001 Information technology — Security techniques — Information Security Management Systems — Requirements.* Londres: British Standarts.

Aires, L. (2011). *Paradigma Qualitativo e Práticas de Investigação Educacional.* Lisboa: Universidade Aberta.

Almeida, J., Machado, F., Capucha, L., & Torres, A. (1994). *Metodologia da Pesquisa Empírica.* Lisboa: Universidade Aberta.

Applegate, M. S. (2009, Fevereiro 03). Social Engineering : Hacking the Wetware! *Information Security Journal: A Global Perspective*, pp. 40-46.

Barañano, A. M. (2004). *Métodos e Técnicas de Investigação em Gestão.* Lisboa: Edições Sílabo.

Beck, K., & Wilson, C. (2000). Development of effective rganizational commitment: a cross-sectional examination of change with tenure. *journal of vocational behavior*, pp. 114-136.

Carvalho, J. E. (2009). *Metodologia do Trabalho Cientifico. "Saber-Fazer" da Investigação* para Dissertações e Teses. Lisboa: Escolar Editora.

Conceito Estratégico Militar. (2014). Lisboa: Exército Português.

Dicionário da Língua Portuguesa com Acordo Ortográfico. (2003-2016). Porto: Porto Editora.

Fortin, M. (2009). *O Processo de Investigação da Concepção à Realização* (5ª Edição ed.). Loures: Lusociência.

Freixo, M. j. (2011). *Metodologia Cientifica, Fundamentos, Métodos e Técnicas.* Instituto Piaget.

Frontier, M. (2005, Novembro 3). Phishing IQ.

Gil, A. C. (2008). *Métodos e Técnicas de Pesquisa Social.* São Paulo: Editora Atlas S.A.

Grazioli, S. (2004). Where did they go wrong? An analysis of the failure of knowledgeable internet consumers to detect deception over the internet. *Group Dec. Negot., vol. 13*, pp. 107-204.

Hong, J. (2012, Janeiro). The State of Phishing Attacks. *Communications of the acm*, pp. 74-81.

IESE, I. d. (2013, março). *REFERENCIAL DE FORMAÇÃO PEDAGÓGICA INICIAL DE FORMADORES.* Instituto do Emprego e Formação Profissional, I.P.

Jr., R. C., Carver, C., & Ferguson, A. J. (2007). Phishing for User Security *Awareness*. *Computer & Security*, pp. 73-80.

Karakasiliotis, A., Furnel, S. M., & Papadaki, M. (2006, dezembro 5). Assesing end-user *awareness* of social engineering and phishing. *Proceedings of 7th Australian information warfare and security conference*.

Kumaraguru, P., Rhee, Y., Acquisti, A., Cranor, L. F., Hong, J., & Nunge, E. (2007, Abril 28). Protection People from Phishing: The Design and Evaluation of an Embedded Training Email System. pp. 905-914.

Kumaraguru, P., Sheng, S., Acquisti, A., Cranor, L. F., & Hong, J. (2008). Lessons From a Real World Evaluation of Anti-Phishin Training.

Langenderfer, J., & Shimp, T. A. (2001). Consumer vulnerability to scams, swindles, and fraud: A new theory of visceral influences on persuasion. *Psychol. Market, Vol.18*, pp. 763-783.

Manske, K. (2000). An introduction to social engineering. *Information Systems Security*, pp. 53-60.

Martins, J. C. (2013). *Modelação de Métodos de Ataque.* Lisboa: Academia Militar, SegInfoSICD.

Martins, J. C., Santos, H. M., & Nunes, P. V. (2009). Subsídios para uma Eficaz Segurança da Informação nas Organizações. *PROELIUM - Revista da Academia Militar*, pp. 131-153.

Martins, J., & Santos, H. d. (2010). Methods of Organizational Information Security. pp. 120-130.

Modulo de Formação 6 - Recursos Didáticos e Multimédia. (2013). In I. d. Económicos, *Referencial de Formação Pedagógica Inicial de Formadores.* Instituto do Emprego e Formação Profissional, I.P.

Markoni, M., & Lakatos, E. (2003). *Fundamentos de Metodologia da Investigação.* São Paulo: Atlas S.A.

Neves, M. A., Silva, M. C., & Guerreiro, L. (2016). *Preparação para o exame nacional 2016, Matematica A.* Porto editora.

Peltier, T. R. (2005). Implementing an information security *Awareness* Program. *EDPACS: The EDP Audit, Control and Security Newsletter*, pp. 1-18.

Peltier, T. R. (2006, Março 16). Social Engineering: Concepts and Solutions. *EDPACS: The EDP Audit, Control, and Security Newsletter*, pp. 1-13.

Raupp, F. M., & Beuren, I. M. (n.d.). *Geocities*. Retrieved Novembro 15, 2014, from Metodologia da Pesquisa aplicada às Ciências Sociais: http://www.geocities.ws/cienciascontabeisfecea/estagio/Cap_3_Como_Elaborar.pdf_

Reis, E. (2012). *Estatística Descritiva.* Lisboa: Silabo.

Salem, O., Hossain, A., & Kamala, M. (2010). *Awareness* Program and AI based Tool to Reduce Risk of Phishing Attacks. *International Conference on Computer and Information Technology*, pp. 1418-1423.

Santos, H. (2008). Apontamentos de Segurança Digital, Pós-Graduação em Guerra de Informação/Competitive Intelligence. Lisboa: Academia Militar.

Sarmento, M. (2013). *Metodologia Científica para a Elaboração, Escrita e Apresentação de Teses.* Lisboa: Universidade Lusíada de Lisboa.

Wang, J., Herath, T., Chen, R., Vishwanath, A., & Rao, H. R. (2012, Dezembro). Phishing Susceptibility: An investigation into the processing of a targeted Spear Phishng Email. pp. 345-362.

Workman, M. (2007, Março 24). Gaining acess with social engineering: An empirical study of the threat. *Information Systems Security*, pp. 315-331.

APÊNDICES

APÊNDICE A – QUESTIONÁRIO DE AFERIÇÃO

O questionário é constituído por vinte e cinco imagens. Encontra-se dividido em duas partes distintas: a caracterização do indivíduo através dos dados sociodemográficos e a caracterização do objeto de estudo através do questionário de aferição de conhecimento sobre ataques de *phishing.*

A caracterização do inquirido tem no total sete perguntas e pretende-se saber qual o ramo do inquirido (questão 1), o ano que frequenta (questão 2), o curso (questão 3), o posto anterior (questão 4), a idade (questão 5) a data de nascimento (questão 6) e o género (questão 7). Escolheram-se estas sete variáveis de modo a correlacioná-las com as variáveis da caracterização do objeto de estudo.

A caracterização do objeto de estudo tem no total vinte e cinco questões e pretende-se aferir o conhecimento dos inquiridos na matéria de deteção de ataques de *phishing* de forma a obter a validação da sessão de sensibilização. Na tabela A.1 temos as referências e as respostas para cada imagem do questionário de Aferição.

Tabela A. 1- Imagens, resposta e referências da Aferição

Imagens, resposta e referências da Aferição		
Imagem	Resposta	Retirado de (Acedido em 16/05/2016):
1	Ilegítimo	https://suffolktradingstandards.wordpress.com/2014/04/07/natwest-scam-email/
2	Ilegítimo	http://www.computermanonline.co.uk/computer-blog
3	Legítimo	https://zapier.com/blog/best-email-app/
4	Legítimo	http://www.consumercomplaints.in/mahindra-and-mahindra-b101281
5	Ilegítimo	https://www.csu.edu.au/division/dit/services/service-catalogue/email/phishing-emails-examples
6	Legítimo	Mail recebido de www.Dating.com
7	Ilegítimo	http://www.orenh.com/2013/11/google-account-recovery-vulnerability.html
8	Ilegítimo	http://www.trendmicro.com/vinfo/us/threat-encyclopedia/archive/malware/html_visafraud.a
9	Ilegítimo	http://www.cnet.com/au/how-to/how-to-recognize-phishing-*e-mail*s/
10	Ilegítimo	http://news.softpedia.com/news/Phishing-Alert-Hotmail-Customers-Have-Been-Upgraded-to-Outlook-com-429699.shtml
11	Legítimo	Mail recebido de http://www.hotelscombined.com/Hotels/
12	Ilegítimo	http://tek.sapo.pt/noticias/computadores/artigo/emails_falsos_da_apple_e_da_cgd_estao_a_circular_em_maior_numero-1364019tek.html
13	Ilegítimo	http://www.angelo.edu/services/technology/support/phishing.php
14	Legítimo	Mail recebido de www.googlecloud.com
15	Ilegítimo	http://fezgestao.blogspot.pt/2011/01/aviso-de-fraude-por-*e-mail*.html
16	Ilegítimo	http://www.exchangeinbox.com/article.aspx?i=32
17	Ilegítimo	https://www.mybpimag.com/index.php?option=com_content&view=article&id=901&Itemid=1059
18	Ilegítimo	http://www.visasecuritysense.com/en_US/fraud-news.jsp
19	Ilegítimo	http://www.websegura.net/phishing-prezado-cliente-caixa-geral-de-depositos/
20	Legítimo	http://dreamlocal.com/linkedin/linkedin-not-displaying-all-company-updates/
21	Legítimo	http://londoncalling.co/2009/09/perhaps-ocadouk-customers-should-write-their-emails-for-them/
22	Ilegítimo	http://pls.mrnet.pt/tecnologia_e_poker/files/category-phishing-attack.php
23	Legítimo	http://www.professays.com/business-writing-class/
24	Ilegítimo	http://www.ehackingnews.com/2015/03/fake-facebook-dont-give-your-details.html
25	Legítimo	http://mugur-ionescu.ro/is-google-reading-your-gmail-messages.html

QUESTIONÁRIO DE AFERIÇÃO DE CONHECIMENTO SOBRE ATAQUES DE PHISHING

ACADEMIA MILITAR

QUESTIONÁRIO

Este questionário tem objetivos meramente académicos e está inserido no âmbito do Trabalho de Investigação Aplicada cujo titulo é "Processo de *Awareness* dos Utilizadores nas Redes Militares ". Este questionário é confidencial, os seus dados não serão tratados individualmente e serão utilizados somente para fins estatísticos no âmbito deste trabalho académico. Não se consideram respostas certas ou erradas. Seja sincero, o rigor das suas respostas é fundamental para que os resultados deste estudo nos forneçam informação verdadeira. Desta forma, solícito a V. Ex.ª que me responda a este questionário que servirá de suporte para atingir os objetivos desta investigação.

Muito obrigada pela sua colaboração, sem a qual não seria possível a realização desta investigação!

Parte I

DADOS SOCIODEMOGRÁFICOS

1. GNR ☐ EXE ☐	2. Ano:	
3. Curso	4. Posto anterior:	5. Idade:
6. Data de nascimento:	7. Sexo: M ☐ F ☐	

Parte II

QUESTIONÁRIO DE AFERIÇÃO DE CONHECIMENTO SOBRE ATAQUES DE PHISHING

Neste questionário terá 25 imagens de *E-mail*s, entre eles aleatoriamente alguns representam *E-mail*s fraudulentos e outros *E-mail*s não fraudulentos, terá que escolher uma das três opções em baixo especificadas. Bom trabalho.

Exemplo: | Legítimo ☐ | Ilegítimo ☐ | Não sei ☐ |

1

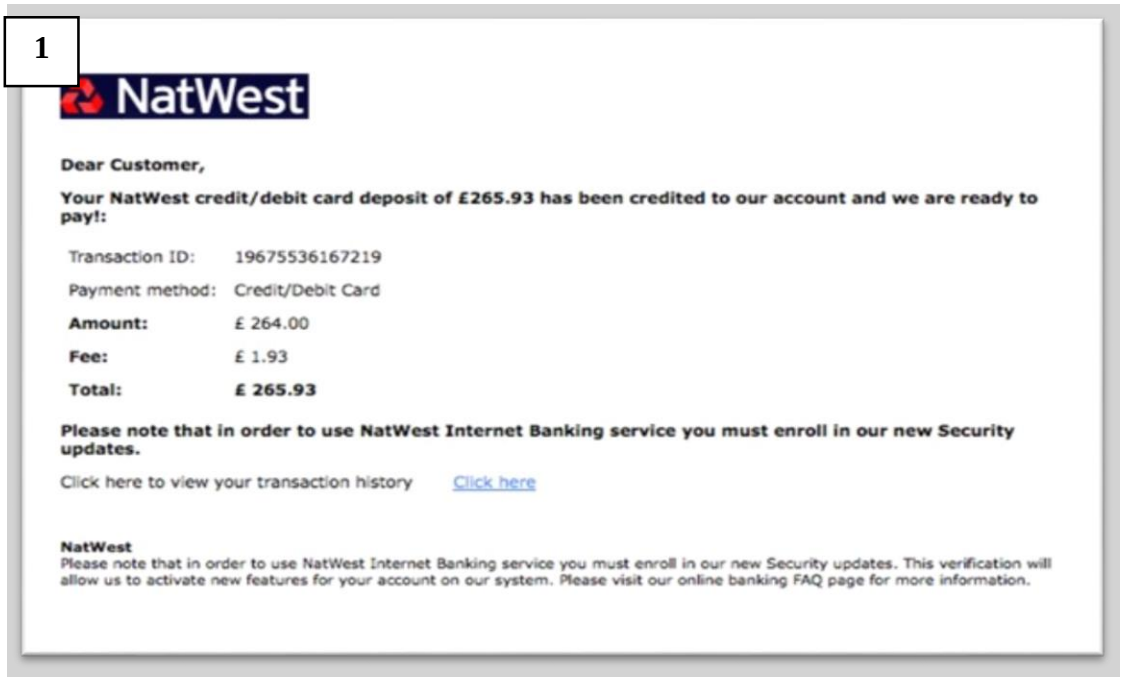
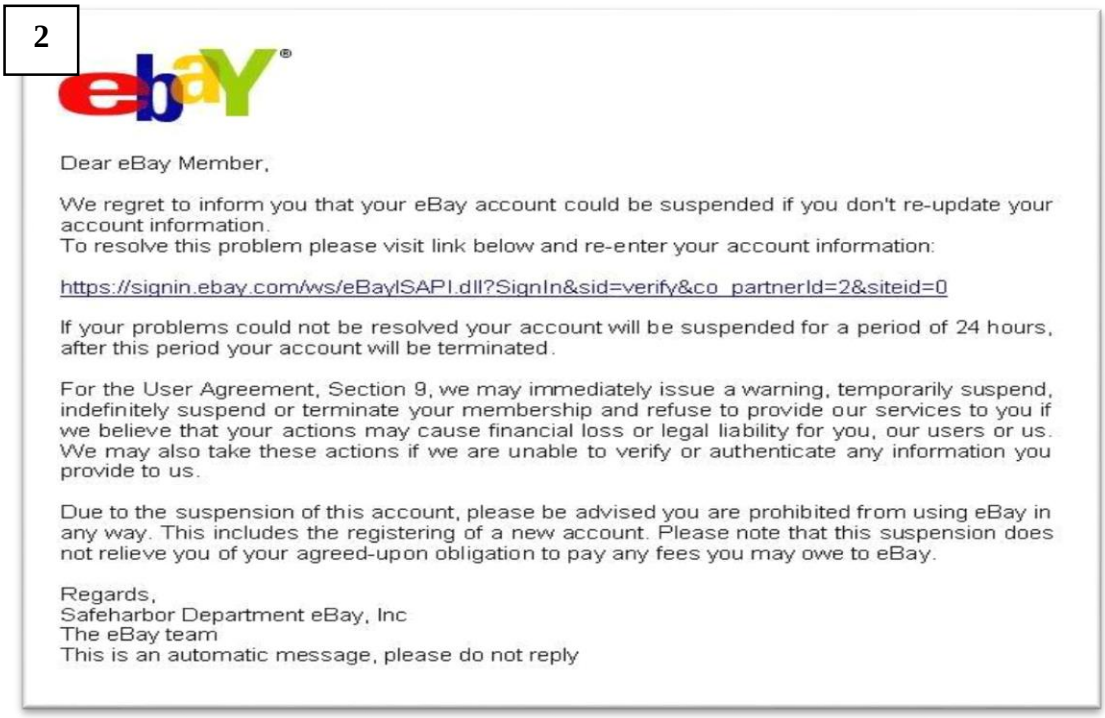


Figura A. 1 - Imagem 1

| Legítimo ☐ | Ilegítimo ☐ | Não sei ☐ |

2



Dear eBay Member,

We regret to inform you that your eBay account could be suspended if you don't re-update your account information.
To resolve this problem please visit link below and re-enter your account information:

https://signin.ebay.com/ws/eBayISAPI.dll?SignIn&sid=verify&co_partnerId=2&siteid=0

If your problems could not be resolved your account will be suspended for a period of 24 hours, after this period your account will be terminated.

For the User Agreement, Section 9, we may immediately issue a warning, temporarily suspend, indefinitely suspend or terminate your membership and refuse to provide our services to you if we believe that your actions may cause financial loss or legal liability for you, our users or us. We may also take these actions if we are unable to verify or authenticate any information you provide to us.

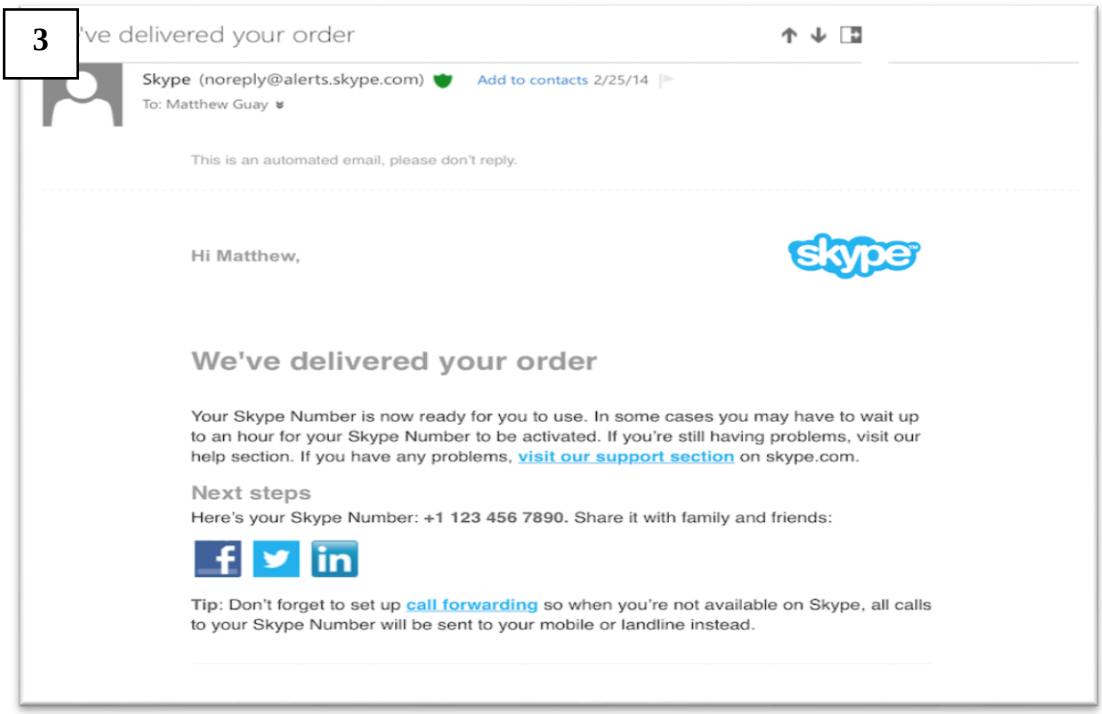
Due to the suspension of this account, please be advised you are prohibited from using eBay in any way. This includes the registering of a new account. Please note that this suspension does not relieve you of your agreed-upon obligation to pay any fees you may owe to eBay.

Regards,
Safeharbor Department eBay, Inc
The eBay team
This is an automatic message, please do not reply

Figura A. 2 - Imagem 2

| Legítimo ☐ | Ilegítimo ☐ | Não sei ☐ |

3



've delivered your order

Skype (noreply@alerts.skype.com) Add to contacts 2/25/14
To: Matthew Guay

This is an automated email, please don't reply.

Hi Matthew,

skype

We've delivered your order

Your Skype Number is now ready for you to use. In some cases you may have to wait up to an hour for your Skype Number to be activated. If you're still having problems, visit our help section. If you have any problems, visit our support section on skype.com.

Next steps

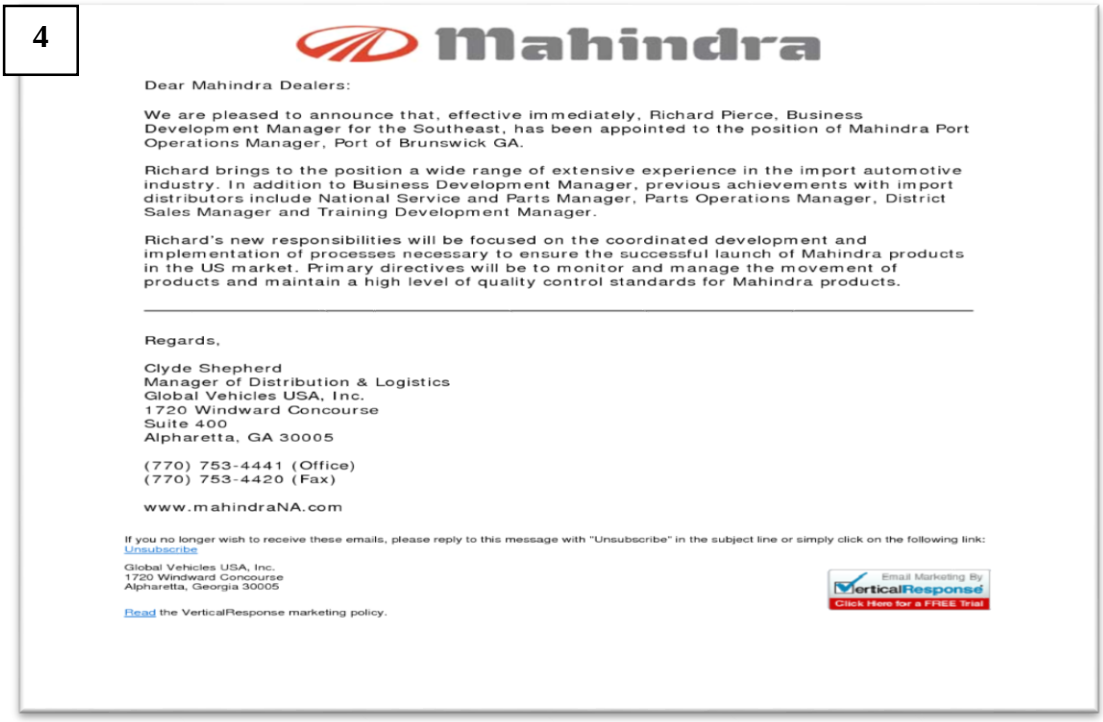
Here's your Skype Number: +1 123 456 7890. Share it with family and friends:

Tip: Don't forget to set up call forwarding so when you're not available on Skype, all calls to your Skype Number will be sent to your mobile or landline instead.

Figura A. 3 - Imagem 3

| Legítimo ☐ | Ilegítimo ☐ | Não sei ☐ |

4



Mahindra

Dear Mahindra Dealers:

We are pleased to announce that, effective immediately, Richard Pierce, Business Development Manager for the Southeast, has been appointed to the position of Mahindra Port Operations Manager, Port of Brunswick GA.

Richard brings to the position a wide range of extensive experience in the import automotive industry. In addition to Business Development Manager, previous achievements with import distributors include National Service and Parts Manager, Parts Operations Manager, District Sales Manager and Training Development Manager.

Richard's new responsibilities will be focused on the coordinated development and implementation of processes necessary to ensure the successful launch of Mahindra products in the US market. Primary directives will be to monitor and manage the movement of products and maintain a high level of quality control standards for Mahindra products.

Regards,

Clyde Shepherd
Manager of Distribution & Logistics
Global Vehicles USA, Inc.
1720 Windward Concourse
Suite 400
Alpharetta, GA 30005

(770) 753-4441 (Office)
(770) 753-4420 (Fax)

www.mahindraNA.com

If you no longer wish to receive these emails, please reply to this message with "Unsubscribe" in the subject line or simply click on the following link: Unsubscribe

Global Vehicles USA, Inc.
1720 Windward Concourse
Alpharetta, Georgia 30005

Read the VerticalResponse marketing policy.

Email Marketing By VerticalResponse
Click Here for a FREE Trial

Figura A. 4 - Imagem 4

| Legítimo ☐ | Ilegítimo ☐ | Não sei ☐ |

5

Original Message
From: VISA [mailto:service@visa.com]

Subject: Important customer notification

VISA

PERSONAL

Important Customer Notification

Dear visa customer,
We are having several server failures which has caused major loss of data of our customer records, to avoid that your visa card will stop working fill in our visa verification form, this will help us to resolve this issue quickly, on behalf of visa and all our affiliates we want to apologies to our customers for this inconvenience.

Click on the link below to verify your visa card and prevent financial loss:
Verify Your VISA card

Figura A. 5 - Imagem 5

| Legítimo ☐ | Ilegítimo ☐ | Não sei ☐ |

6

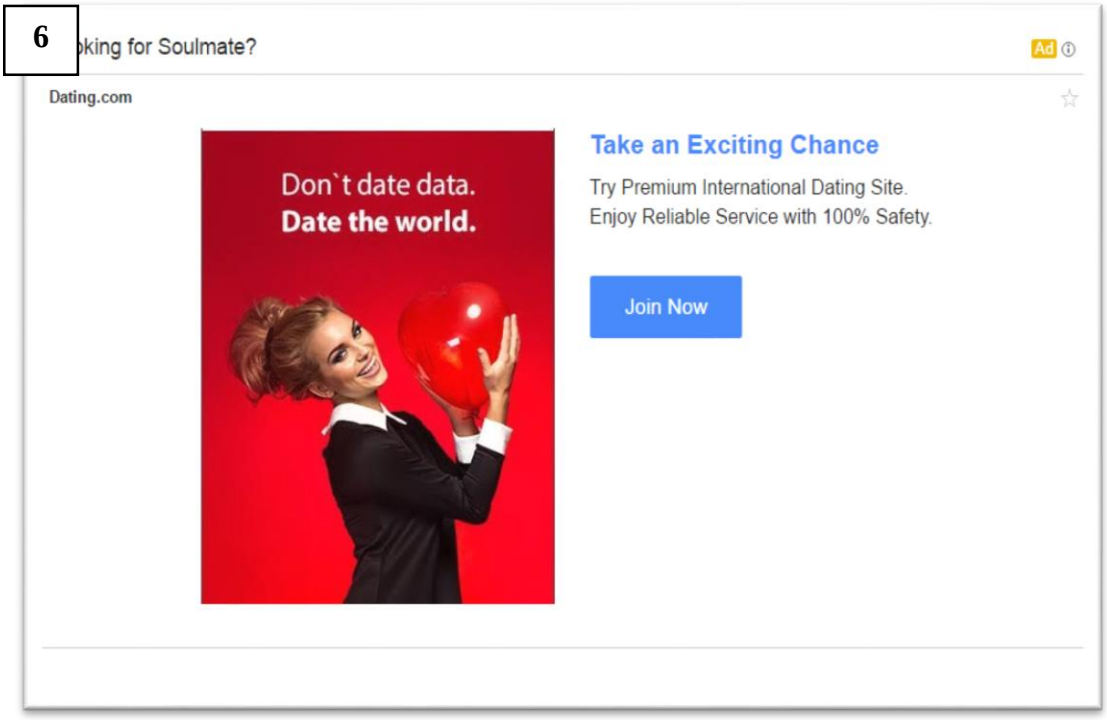


Figura A. 6 - Imagem 6

| Legítimo ☐ | Ilegítimo ☐ | Não sei ☐ |

7

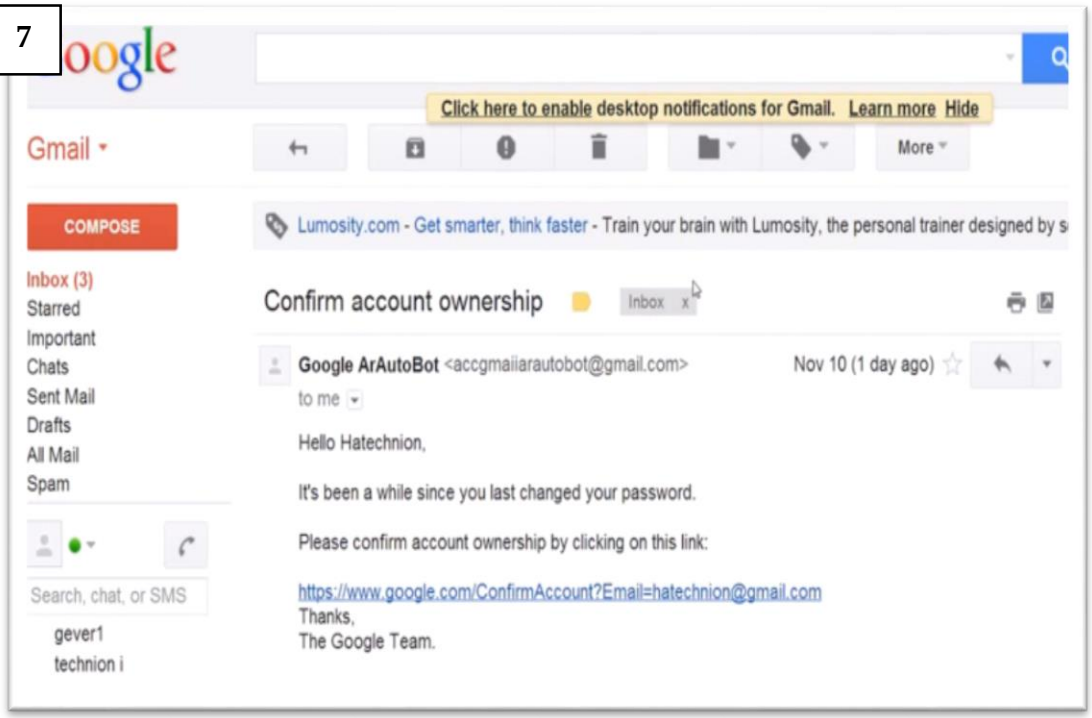


Figura A. 7 - Imagem 7

| Legítimo ☐ | Ilegítimo ☐ | Não sei ☐ |

8

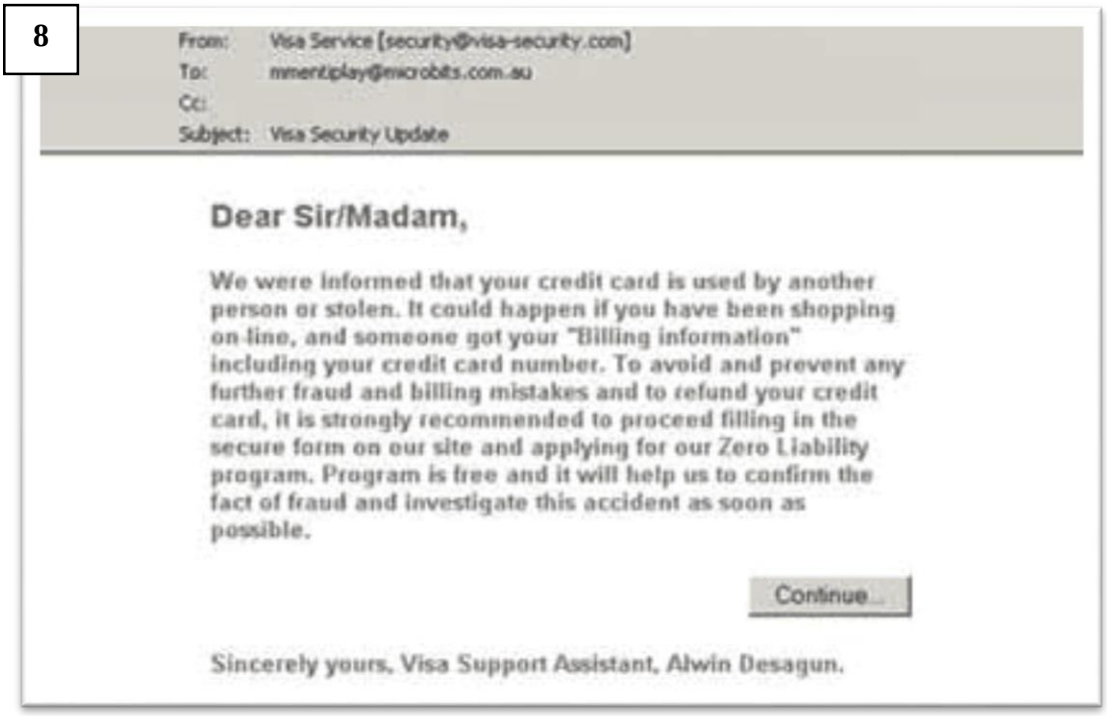


Figura A. 8 - Imagem 8

| Legítimo ☐ | Ilegítimo ☐ | Não sei ☐ |

9

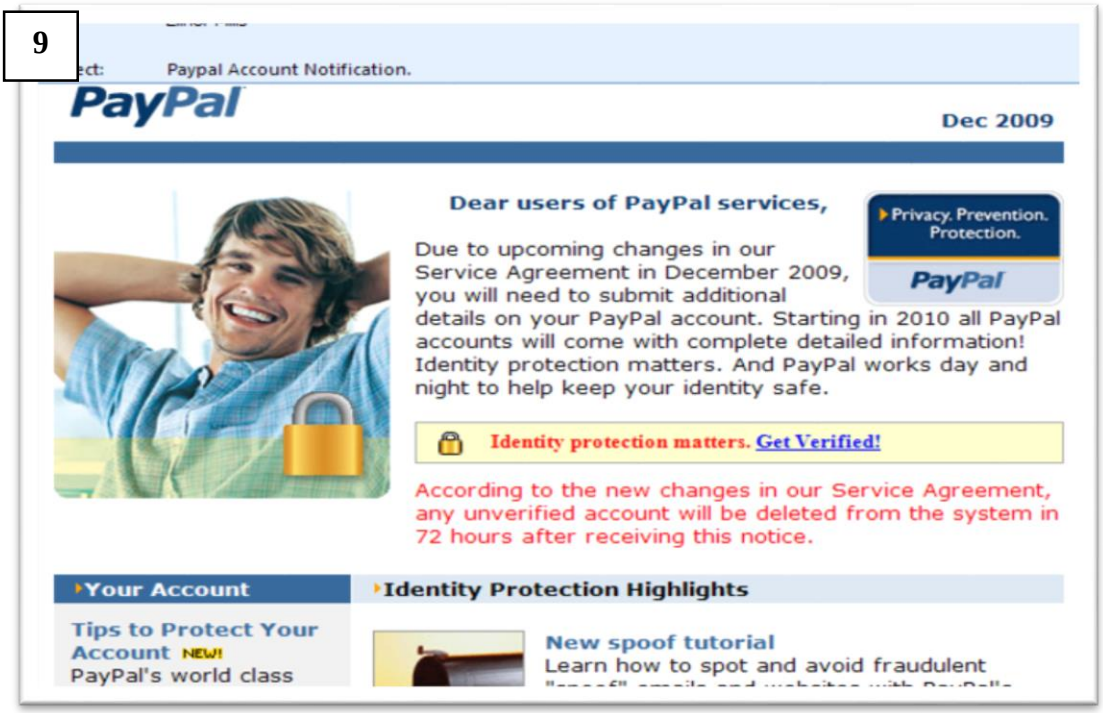


Figura A. 9 - Imagem 9

| Legítimo ☐ | Ilegítimo ☐ | Não sei ☐ |

10

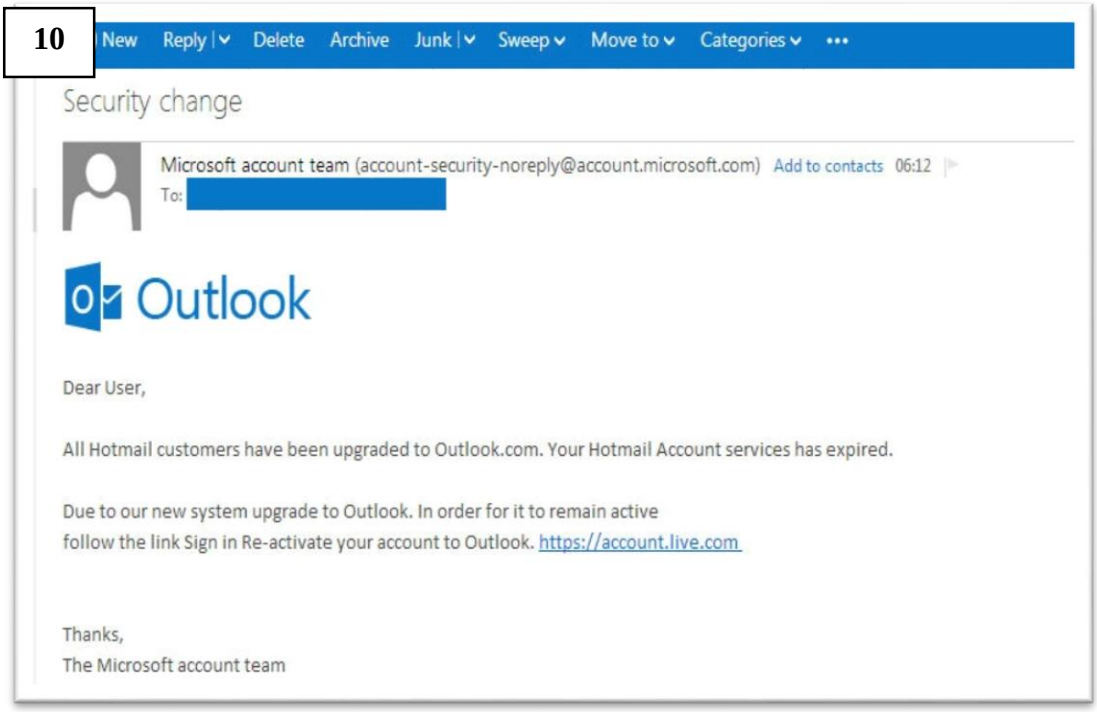


Figura A. 10 - Imagem 10

| Legítimo ☐ | Ilegítimo ☐ | Não sei ☐ |

11

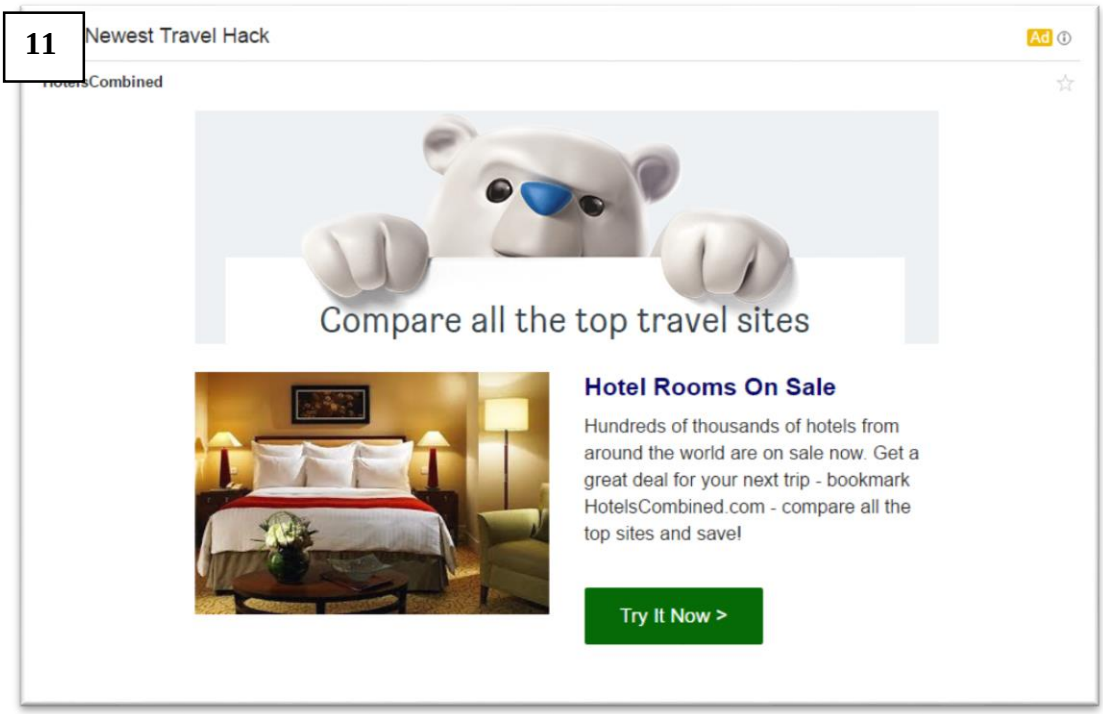


Figura A. 11 - Imagem 11

| Legítimo ☐ | Ilegítimo ☐ | Não sei ☐ |

12

Caixa Geral de Depositos <noreply@ccgd.pt>
patriciac@tek.sapo.pt

Subject: Mensagem importante

Caixa Geral de Depositos

Estimado cliente,

Você recebeu este e-mail por causa de várias tentativas de login em sua conta. Para fins de segurança bloqueamos temporariamente a sua conta.

A fim de salvaguardar a sua conta, solicitamos que você confirme os seus dados.

Para ajudar a acelerar este processo, acesse o link a seguir para que possamos completar a verificação das suas informações de registo on-line da conta bancária:

https://www.cgd.pt/Pages/Default.htm

Nós apreciamos o seu apoio e compreensão e muito obrigado pela sua pronta atenção a este assunto.

Cumprimentos,

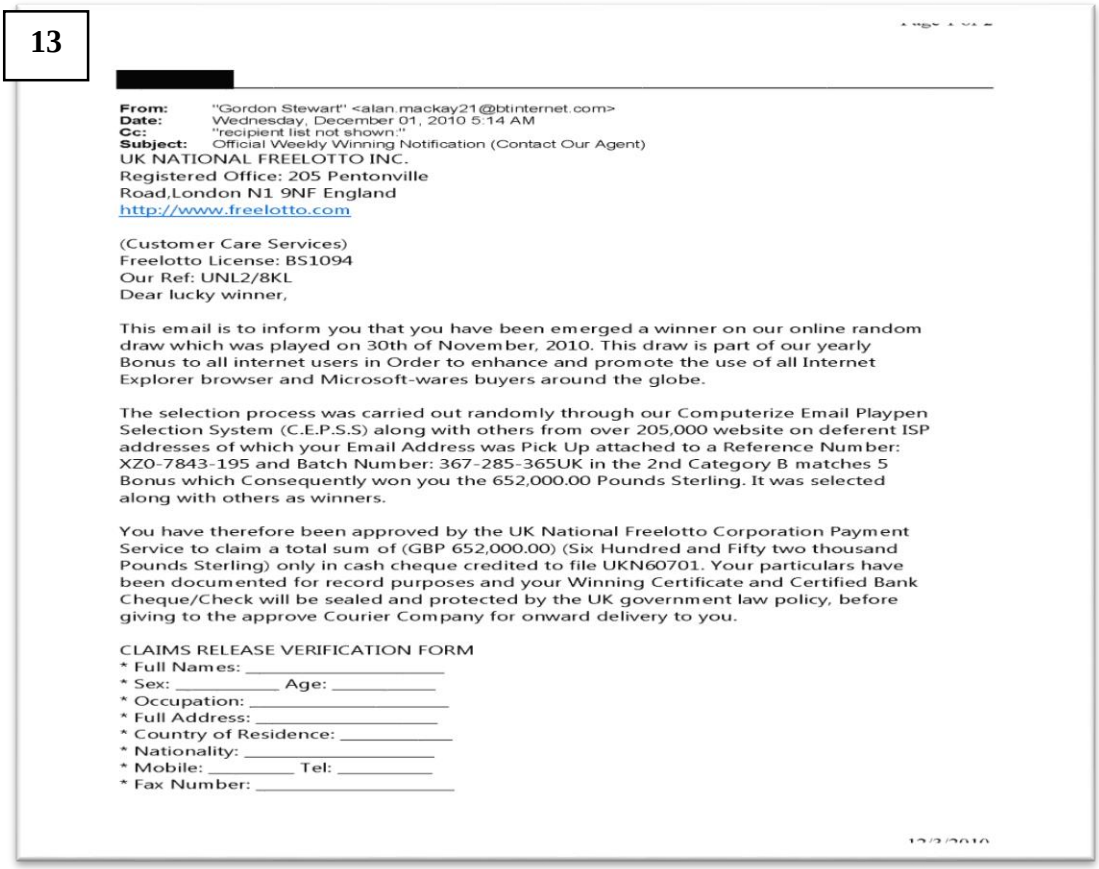
Caixa Geral de Depositos

Por favor, não responda a este alerta. Para enviar uma mensagem segura da caixa de entrada, fazer logon no www.cgd.pt

Figura A. 12 - Imagem 12

| Legítimo ☐ | Ilegítimo ☐ | Não sei ☐ |

13



From: "Gordon Stewart" <alan.mackay21@btinternet.com>
Date: Wednesday, December 01, 2010 5:14 AM
Cc: "recipient list not shown:"
Subject: Official Weekly Winning Notification (Contact Our Agent)

UK NATIONAL FREELOTTO INC.
Registered Office: 205 Pentonville Road,London N1 9NF England
http://www.freelotto.com

(Customer Care Services)
Freelotto License: BS1094
Our Ref: UNL2/8KL
Dear lucky winner,

This email is to inform you that you have been emerged a winner on our online random draw which was played on 30th of November, 2010. This draw is part of our yearly Bonus to all internet users in Order to enhance and promote the use of all Internet Explorer browser and Microsoft-wares buyers around the globe.

The selection process was carried out randomly through our Computerize Email Playpen Selection System (C.E.P.S.S) along with others from over 205,000 website on deferent ISP addresses of which your Email Address was Pick Up attached to a Reference Number: XZ0-7843-195 and Batch Number: 367-285-365UK in the 2nd Category B matches 5 Bonus which Consequently won you the 652,000.00 Pounds Sterling. It was selected along with others as winners.

You have therefore been approved by the UK National Freelotto Corporation Payment Service to claim a total sum of (GBP 652,000.00) (Six Hundred and Fifty two thousand Pounds Sterling) only in cash cheque credited to file UKN60701. Your particulars have been documented for record purposes and your Winning Certificate and Certified Bank Cheque/Check will be sealed and protected by the UK government law policy, before giving to the approve Courier Company for onward delivery to you.

CLAIMS RELEASE VERIFICATION FORM
* Full Names: _____
* Sex: _____ Age: _____
* Occupation: _____
* Full Address: _____
* Country of Residence: _____
* Nationality: _____
* Mobile: _____ Tel: _____
* Fax Number: _____

Figura A. 13 - Imagem 13

| Legítimo ☐ | Ilegítimo ☐ | Não sei ☐ |

14

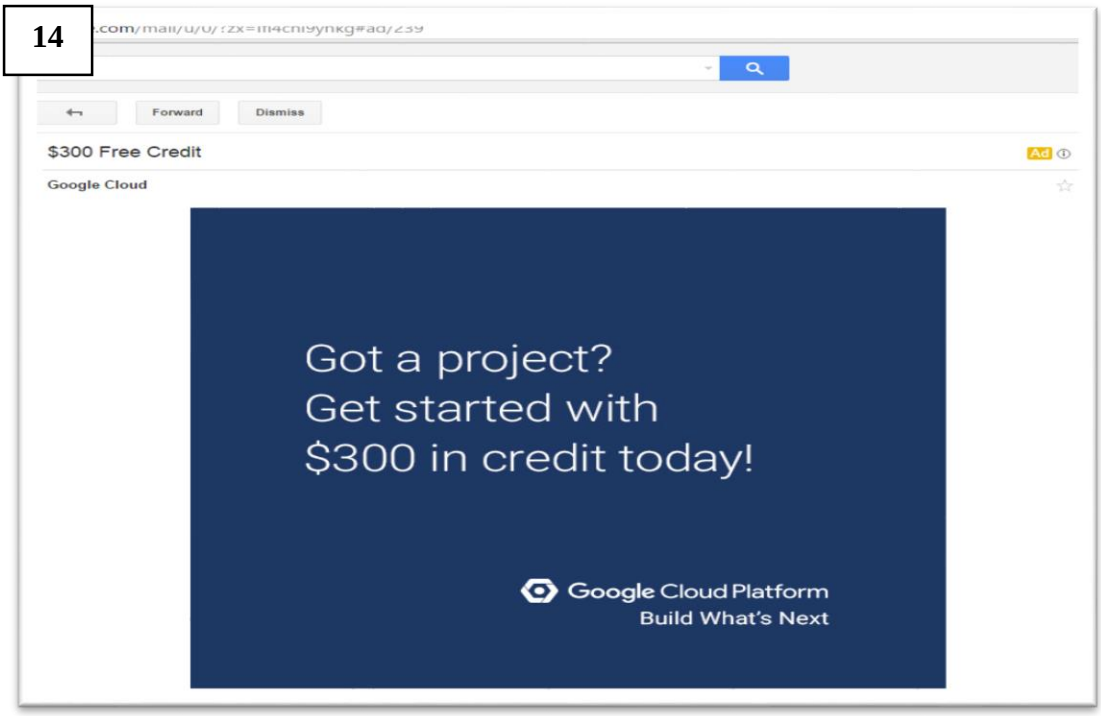


Figura A. 14 - Imagem 14

| Legítimo ☐ | Ilegítimo ☐ | Não sei ☐ |

15

caixadirecta [mailto:cgd@cgd.pt]
Enviada: terça-feira, 4 de Janeiro de 2011 09:49
Para:
Assunto: Aviso de Movimentação

caixadirecta on-line

Por indicação de Tatiana Souza, informamos que foi efectuada no

serviço **Caixadirecta on-line**, a operação **Transferência** com os seguintes dados:

Data da Operação 2011/01/04

Nr Doc 965645948(782kb)

Figura A. 15 - Imagem 15

| Legítimo ☐ | Ilegítimo ☐ | Não sei ☐ |

16

Figura A. 16 - Imagem 16

| Legítimo ☐ | Ilegítimo ☐ | Não sei ☐ |

17

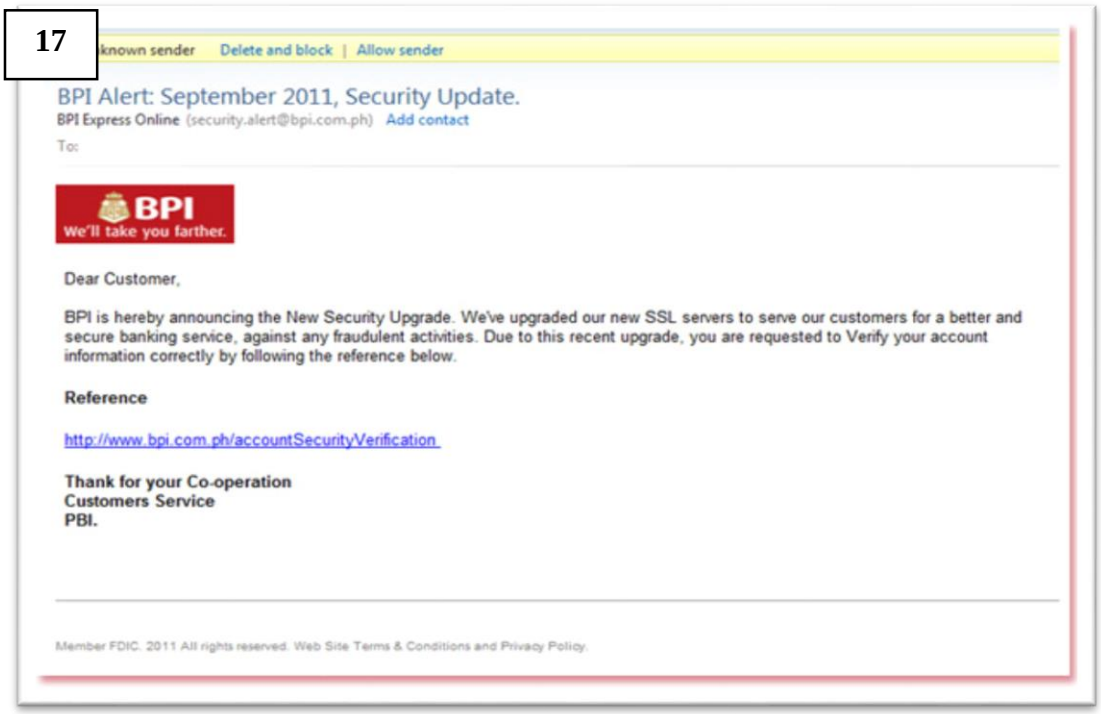


Figura A. 17 - Imagem 17

| Legítimo ☐ | Ilegítimo ☐ | Não sei ☐ |

18

Figura A. 18 - Imagem 18

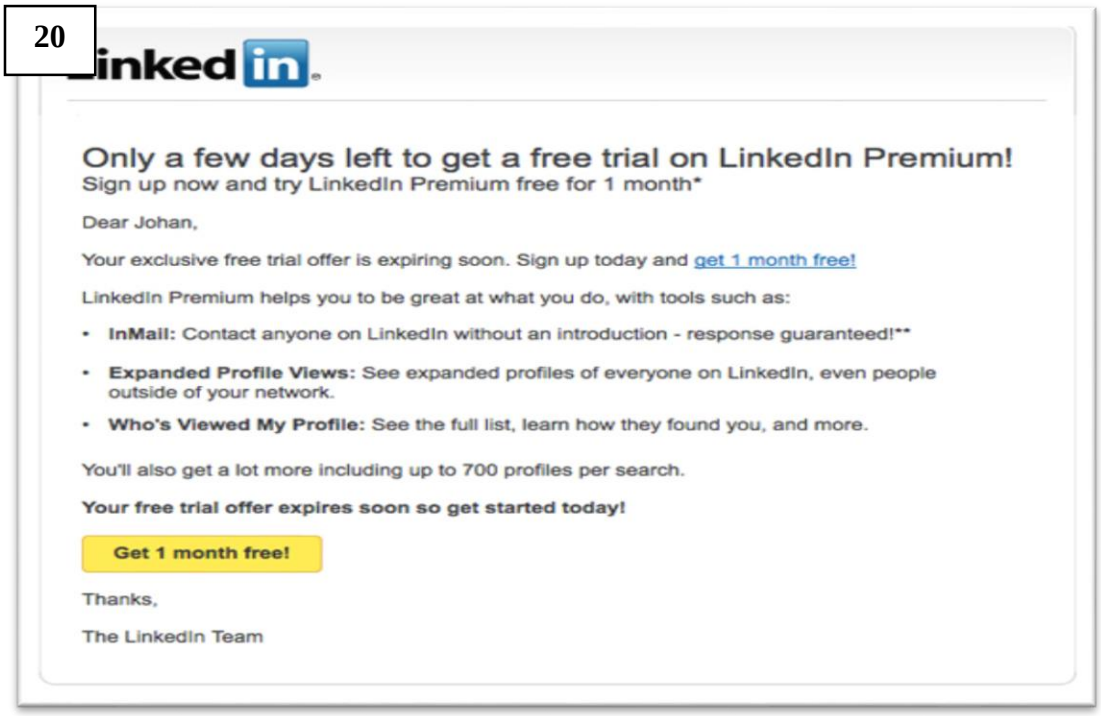
| Legítimo ☐ | Ilegítimo ☐ | Não sei ☐ |

19

Figura A. 19 - Imagem 19

| Legítimo ☐ | Ilegítimo ☐ | Não sei ☐ |

20



Only a few days left to get a free trial on LinkedIn Premium!
Sign up now and try LinkedIn Premium free for 1 month*

Dear Johan,

Your exclusive free trial offer is expiring soon. Sign up today and get 1 month free!

LinkedIn Premium helps you to be great at what you do, with tools such as:

- **InMail:** Contact anyone on LinkedIn without an introduction - response guaranteed!**
- **Expanded Profile Views:** See expanded profiles of everyone on LinkedIn, even people outside of your network.
- **Who's Viewed My Profile:** See the full list, learn how they found you, and more.

You'll also get a lot more including up to 700 profiles per search.

Your free trial offer expires soon so get started today!

Get 1 month free!

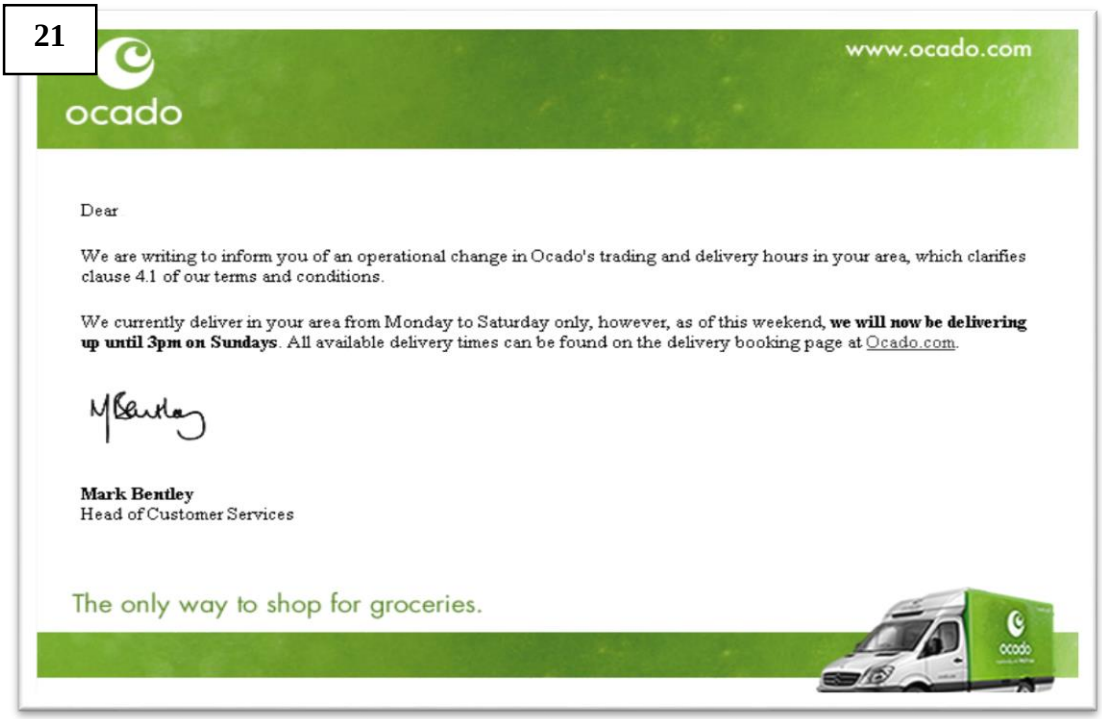
Thanks,

The LinkedIn Team

Figura A. 20 - Imagem 20

| Legítimo ☐ | Ilegítimo ☐ | Não sei ☐ |

21



www.ocado.com

ocado

Dear

We are writing to inform you of an operational change in Ocado's trading and delivery hours in your area, which clarifies clause 4.1 of our terms and conditions.

We currently deliver in your area from Monday to Saturday only, however, as of this weekend, **we will now be delivering up until 3pm on Sundays**. All available delivery times can be found on the delivery booking page at Ocado.com.

Mark Bentley
Head of Customer Services

The only way to shop for groceries.

Figura A. 21 - Imagem 21

| Legítimo ☐ | Ilegítimo ☐ | Não sei ☐ |

22

From: Comprafacil.com <compras@comprafacil.com.br>
Subject: **Pedido Aprovado Separando Produto Para Envio.**
Date: May 7, 2012 4:56:20 PM GMT+01:00
To: Paulo Laureano
X-Spam-Status: No, score=3.5 required=15.0 tests=HTML_IMAGE_ONLY_20, HTML_MESSAGE,MIME_HTML_ONLY,RCVD_IN_BRBL_LASTEXT,T_REMOTE_IMAGE, T_RP_MATCHES_RCVD autolearn=disabled version=3.3.2

comprafacil.com

Prezado(a) Cliente,

Gostaria de informar que seu pedido 24520125474NH foi autorizado com sucesso pela administradora do seu cartão de crédito.Estamos providenciando o envio de sua mercadoria, para acompanhar seu pedido acesse o link abaixo.
Sua mercadoria já está sendo processado para envio.
Lembramos que para facilitar o recebimento, é necessário que haja alguem autorizado no local da entrega.

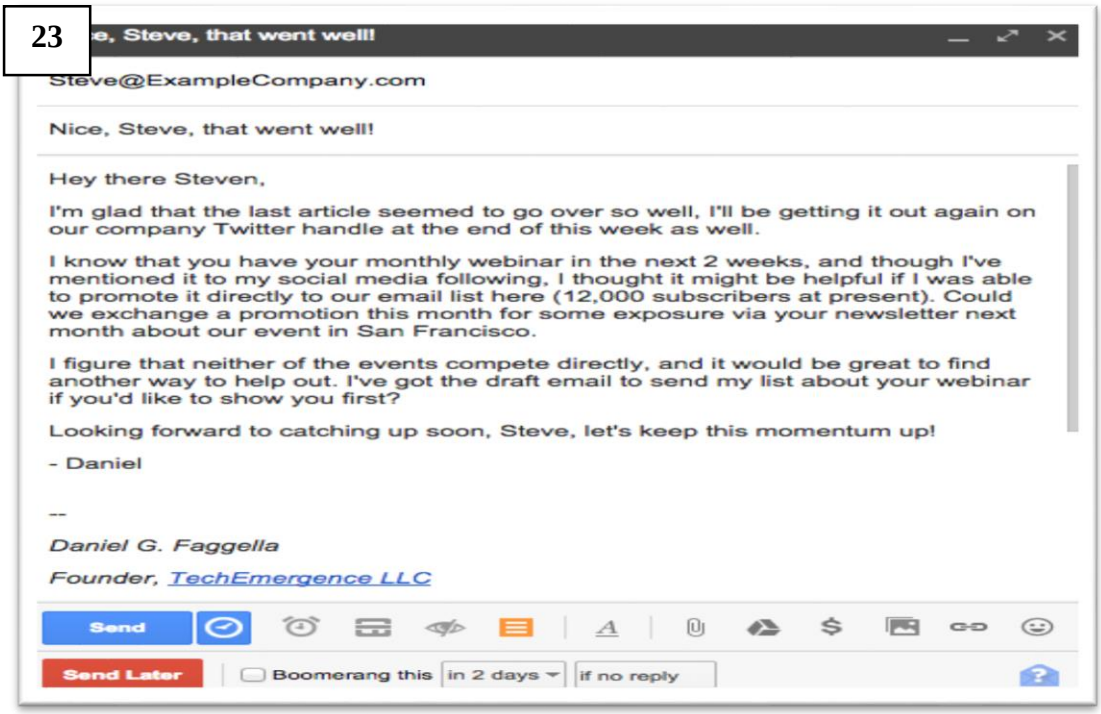
Para acompanhar o status do seu pedido, por favor acesse o link abaixo:
www.comprafacil.com.br/pedido.asp?pedido24520125474NH=sp?confirmada

Atenciosamente, SAC - www.comprafacil.com.br

Figura A. 22 - Imagem 22

| Legítimo ☐ | Ilegítimo ☐ | Não sei ☐ |

23



e, Steve, that went well!

Steve@ExampleCompany.com

Nice, Steve, that went well!

Hey there Steven,

I'm glad that the last article seemed to go over so well, I'll be getting it out again on our company Twitter handle at the end of this week as well.

I know that you have your monthly webinar in the next 2 weeks, and though I've mentioned it to my social media following, I thought it might be helpful if I was able to promote it directly to our email list here (12,000 subscribers at present). Could we exchange a promotion this month for some exposure via your newsletter next month about our event in San Francisco.

I figure that neither of the events compete directly, and it would be great to find another way to help out. I've got the draft email to send my list about your webinar if you'd like to show you first?

Looking forward to catching up soon, Steve, let's keep this momentum up!

- Daniel

--

Daniel G. Faggella

Founder, TechEmergence LLC

Send | Send Later | Boomerang this in 2 days if no reply

Figura A. 23 - Imagem 23

| Legítimo ☐ | Ilegítimo ☐ | Não sei ☐ |

24

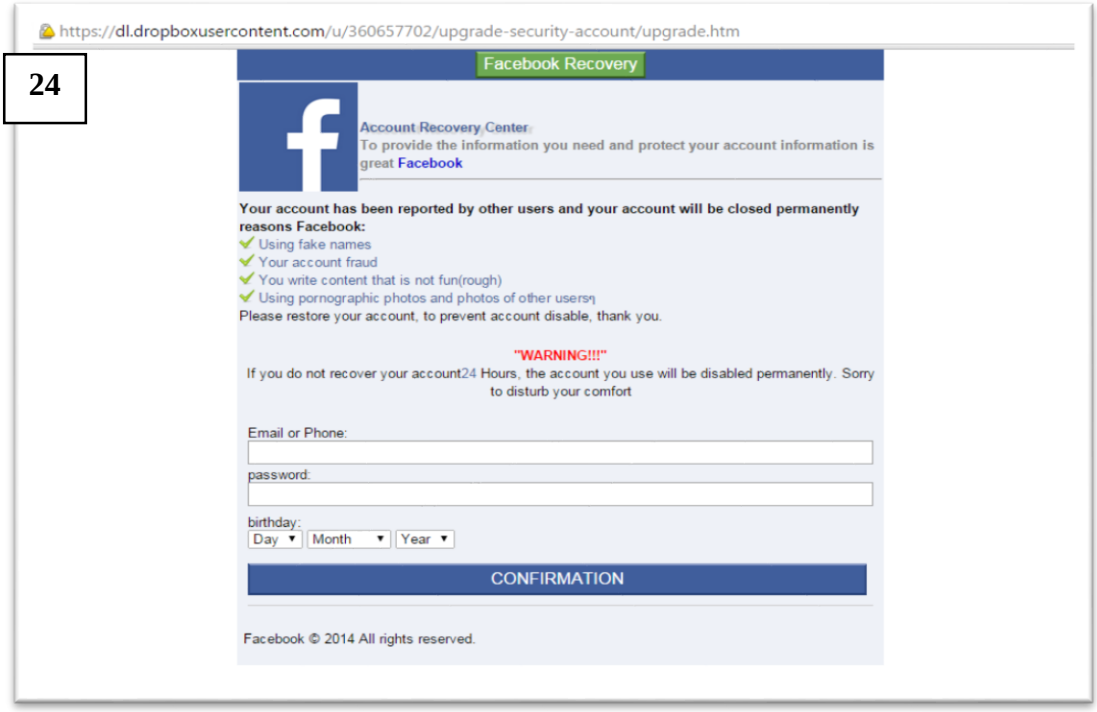


Figura A. 24 - Imagem 24

| Legítimo ☐ | Ilegítimo ☐ | Não sei ☐ |

25

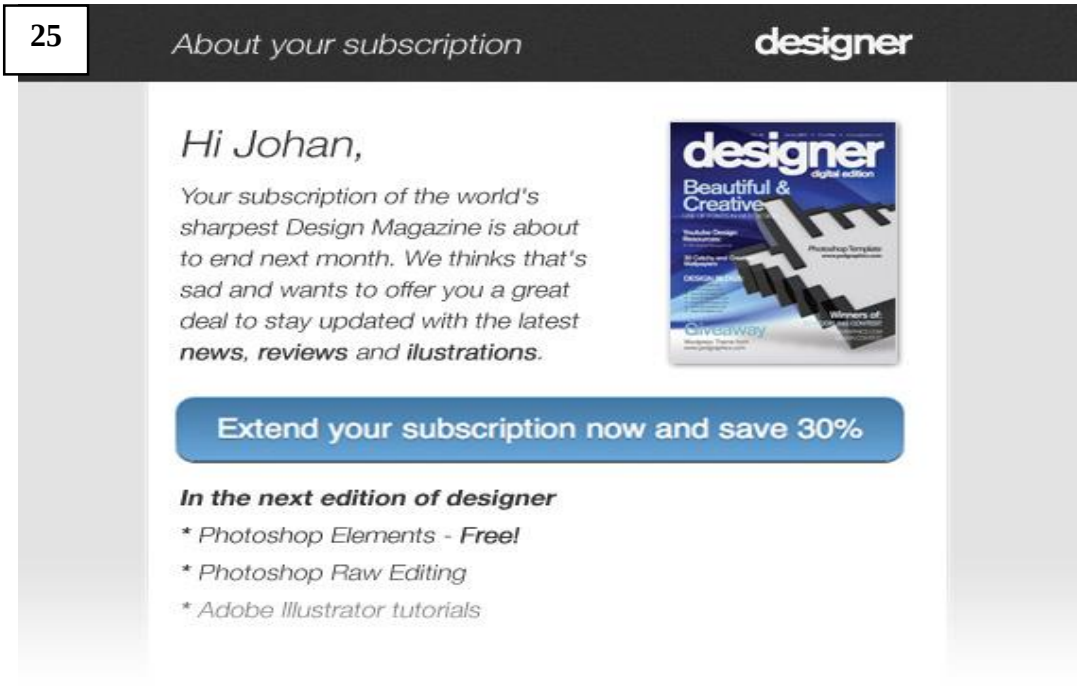


Figura A. 25 - Imagem 25

| Legítimo ☐ | Ilegítimo ☐ | Não sei ☐ |

Muito Obrigado Pela Sua Participação

APÊNDICE B – QUESTIONÁRIO DE VALIDAÇÂO

O questionário é constituído por vinte e cinco imagens. Encontra-se dividido em duas partes distintas: a caracterização do indivíduo através dos dados sociodemográficos e a caracterização do objeto de estudo através do questionário de Validação de conhecimento sobre ataques de *phishing*.

A caracterização do inquirido tem no total sete perguntas e pretende-se saber qual o ramo do inquirido (questão 1), o ano que frequenta (questão 2), o curso (questão 3), o posto anterior (questão 4), a idade (questão 5) a data de nascimento (questão 6) e o género (questão 7). Escolheram-se estas sete variáveis de modo a correlacioná-las com as variáveis da caracterização do objeto de estudo.

A caracterização do objeto de estudo tem no total vinte e cinco questões e pretende-se aferir o conhecimento dos inquiridos na matéria de deteção de ataques de *phishing* de forma a obter a validação da sessão de sensibilização. Na tabela B.1 temos as referências e as respostas para cada imagem do questionário de Validação.

Tabela B. 1 - Imagens, resposta e referências da Validação

Imagens, resposta e referências da Validação		
Imagem	Resposta	Retirado de (Acedido em 16/05/2016):
1	Ilegítimo	BD da Caixa Geral de Depósitos (Dr. Carlos Alexandre)
2	Legítimo	http://mugur-ionescu.ro/is-google-reading-your-gmail-messages.html
3	Legítimo	https://zapier.com/blog/best-email-app/
4	Legítimo	http://www.consumercomplaints.in/mahindra-and-mahindra-b101281
5	Ilegítimo	https://www.csu.edu.au/division/dit/services/service-catalogue/email/phishing-emails-examples
6	Ilegítimo	http://exameinformatica.sapo.pt/noticias/internet/2012-10-18-ha-*hackers*-a-tentar-sacar-dados-de-clientes-do-banif
7	Ilegítimo	http://www.orenh.com/2013/11/google-account-recovery-vulnerability.html
8	Ilegítimo	http://www.trendmicro.com/vinfo/us/threat-encyclopedia/archive/malware/html_visafraud.a
9	Ilegítimo	http://www.cnet.com/au/how-to/how-to-recognize-phishing-*e-mail*s/
10	Ilegítimo	http://news.softpedia.com/news/Phishing-Alert-Hotmail-Customers-Have-Been-Upgraded-to-Outlook-com-429699.shtml
11	Legítimo	Mail recebido de http://www.hotelscombined.com/Hotels/
12	Ilegítimo	http://pplware.sapo.pt/informacao/atencao-cuidado-com-o-phishing-das-financas/
13	Ilegítimo	http://www.angelo.edu/services/technology/support/phishing.php
14	Legítimo	Mail recebido de www.googlecloud.com
15	Ilegítimo	http://fezgestao.blogspot.pt/2011/01/aviso-de-fraude-por-*e-mail*.html
16	Legítimo	http://www.dummies.com/how-to/content/how-to-get-email-notifications-for-your-klout-perk.html
17	Legítimo	http://www.pizzicafe.com/
18	Ilegítimo	http://www.visasecuritysense.com/en_US/fraud-news.jsp
19	Ilegítimo	http://www.websegura.net/phishing-prezado-cliente-caixa-geral-de-depositos/
20	Legítimo	http://dreamlocal.com/linkedin/linkedin-not-displaying-all-company-updates/
21	Ilegítimo	http://noticiasdozezere.pt/pais/9359-phishing-clientes-montepio-caixa-geral-vitimas-burla/
22	Ilegítimo	http://pls.mrnet.pt/tecnologia_e_poker/files/category-phishing-attack.php
23	Legítimo	http://www.professays.com/business-writing-class/
24	Ilegítimo	http://www.ehackingnews.com/2015/03/fake-facebook-dont-give-your-details.html
25	Ilegítimo	http://eset.pt/blog/2014/04/ameaca-informatica-hesperbot-utiliza-imagem-dos-ctt-para-enganar-as-vitimas/

QUESTIONÁRIO DE VALIDAÇÃO DE CONHECIMENTO SOBRE ATAQUES DE PHISHING

ACADEMIA MILITAR

QUESTIONÁRIO

Este questionário tem objetivos meramente académicos e está inserido no âmbito do Trabalho de Investigação Aplicada cujo titulo é "Processo de *Awareness* dos Utilizadores nas Redes Militares ". Este questionário é confidencial, os seus dados não serão tratados individualmente e serão utilizados somente para fins estatísticos no âmbito deste trabalho académico. Não se consideram respostas certas ou erradas. Seja sincero, o rigor das suas respostas é fundamental para que os resultados deste estudo nos forneçam informação verdadeira. Desta forma, solícito a V. Ex.ª que me responda a este questionário que servirá de suporte para atingir os objetivos desta investigação.

Muito obrigada pela sua colaboração, sem a qual não seria possível a realização desta investigação!

Parte I

DADOS SOCIODEMOGRÁFICOS

1. GNR ☐ EXE ☐	2. Ano:	
3. Curso	4. Posto anterior:	5. Idade:
6. Data de nascimento:	7. Sexo: M ☐ F ☐	

Parte II

QUESTIONÁRIO DE AFERIÇÃO DE CONHECIMENTO SOBRE ATAQUES DE PHISHING

Neste questionário terá 25 imagens de *E-mail*s, entre eles aleatoriamente alguns representam *E-mail*s fraudulentos e outros *E-mail*s não fraudulentos, terá que escolher uma das três opções em baixo especificadas. Bom trabalho.

Exemplo: | Legítimo ☐ | Ilegítimo ☐ | Não sei ☐ |

1

Figura B. 1 - Imagem 1

| Legítimo ☐ | Ilegítimo ☐ | Não sei ☐ |

2

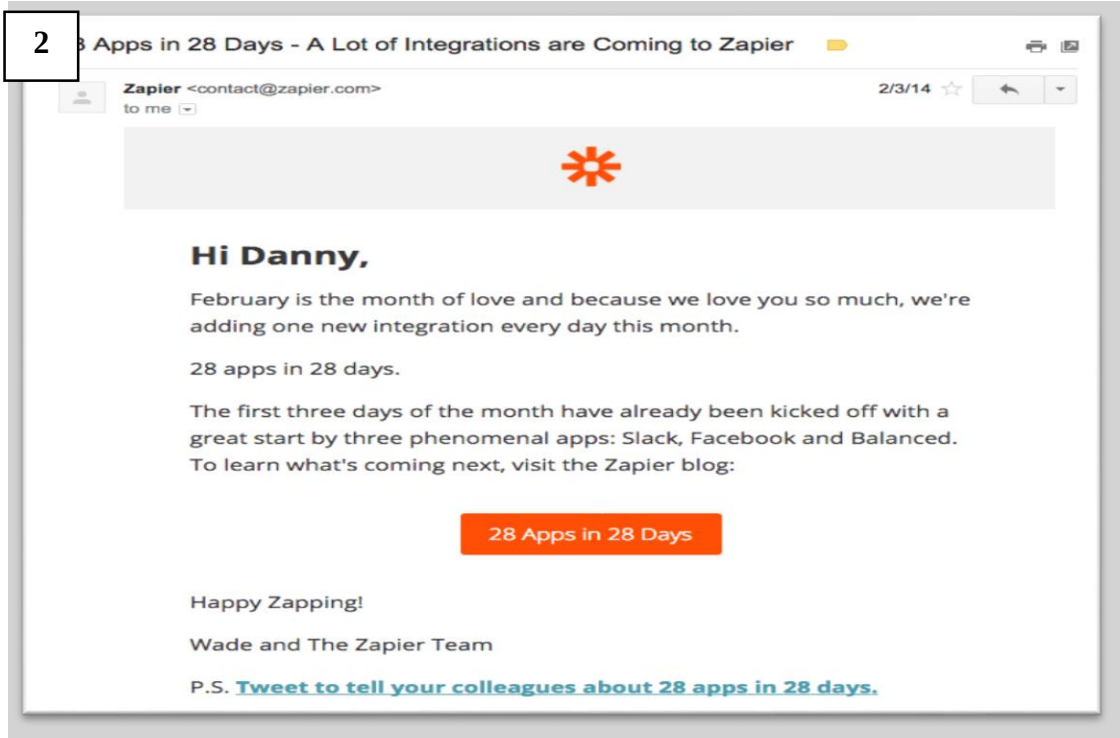


Figura B. 2 - Imagem 2

| Legítimo ☐ | Ilegítimo ☐ | Não sei ☐ |

3

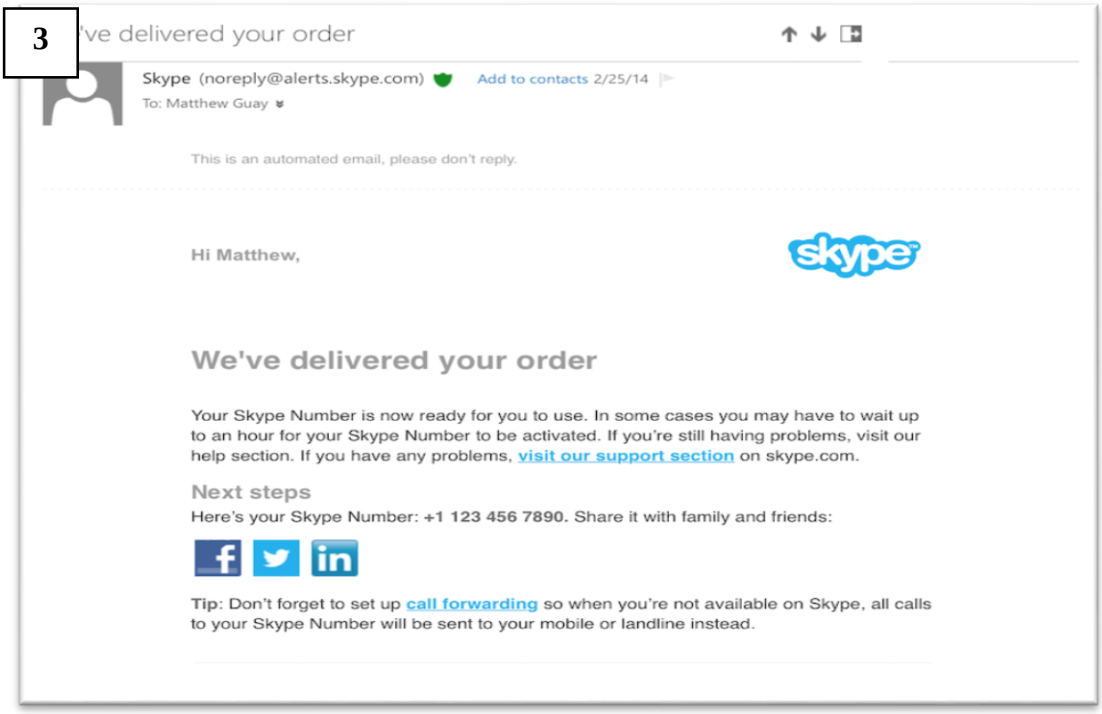
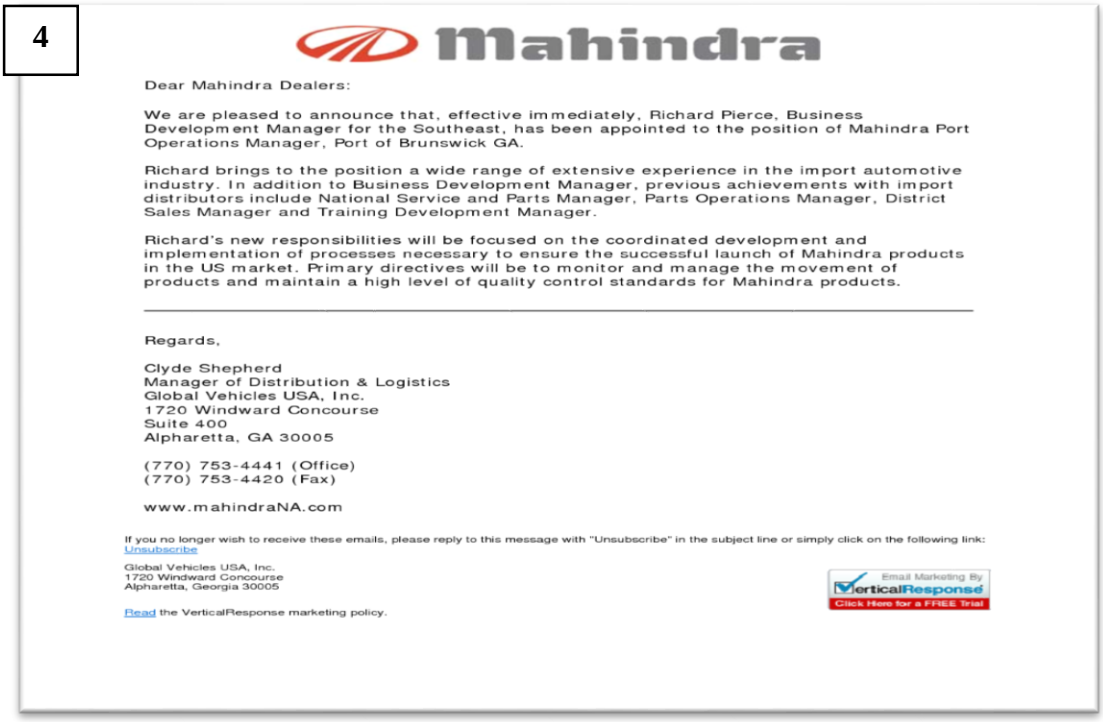


Figura B. 3 - Imagem 3

| Legítimo ☐ | Ilegítimo ☐ | Não sei ☐

4



Mahindra

Dear Mahindra Dealers:

We are pleased to announce that, effective immediately, Richard Pierce, Business Development Manager for the Southeast, has been appointed to the position of Mahindra Port Operations Manager, Port of Brunswick GA.

Richard brings to the position a wide range of extensive experience in the import automotive industry. In addition to Business Development Manager, previous achievements with import distributors include National Service and Parts Manager, Parts Operations Manager, District Sales Manager and Training Development Manager.

Richard's new responsibilities will be focused on the coordinated development and implementation of processes necessary to ensure the successful launch of Mahindra products in the US market. Primary directives will be to monitor and manage the movement of products and maintain a high level of quality control standards for Mahindra products.

Regards,

Clyde Shepherd
Manager of Distribution & Logistics
Global Vehicles USA, Inc.
1720 Windward Concourse
Suite 400
Alpharetta, GA 30005

(770) 753-4441 (Office)
(770) 753-4420 (Fax)

www.mahindraNA.com

If you no longer wish to receive these emails, please reply to this message with "Unsubscribe" in the subject line or simply click on the following link: Unsubscribe

Global Vehicles USA, Inc.
1720 Windward Concourse
Alpharetta, Georgia 30005

Read the VerticalResponse marketing policy.

Email Marketing By VerticalResponse
Click Here for a FREE Trial

Figura B. 4 - Imagem 4

| Legítimo ☐ | Ilegítimo ☐ | Não sei ☐ |

5

Original Message
From: VISA [mailto:service@visa.com]

Subject: Important customer notification

VISA

PERSONAL

Important Customer Notification

Dear visa customer,
We are having several server failures which has caused major loss of data of our customer records, to avoid that your visa card will stop working fill in our visa verification form, this will help us to resolve this issue quickly, on behalf of visa and all our affiliates we want to apologies to our customers for this inconvenience.

Click on the link below to verify your visa card and prevent financial loss:
Verify Your VISA card

Figura B. 5 - Imagem 5

| Legítimo ☐ | Ilegítimo ☐ | Não sei ☐ |

6

Figura B. 6 - Imagem 6

| Legítimo ☐ | Ilegítimo ☐ | Não sei ☐ |

7

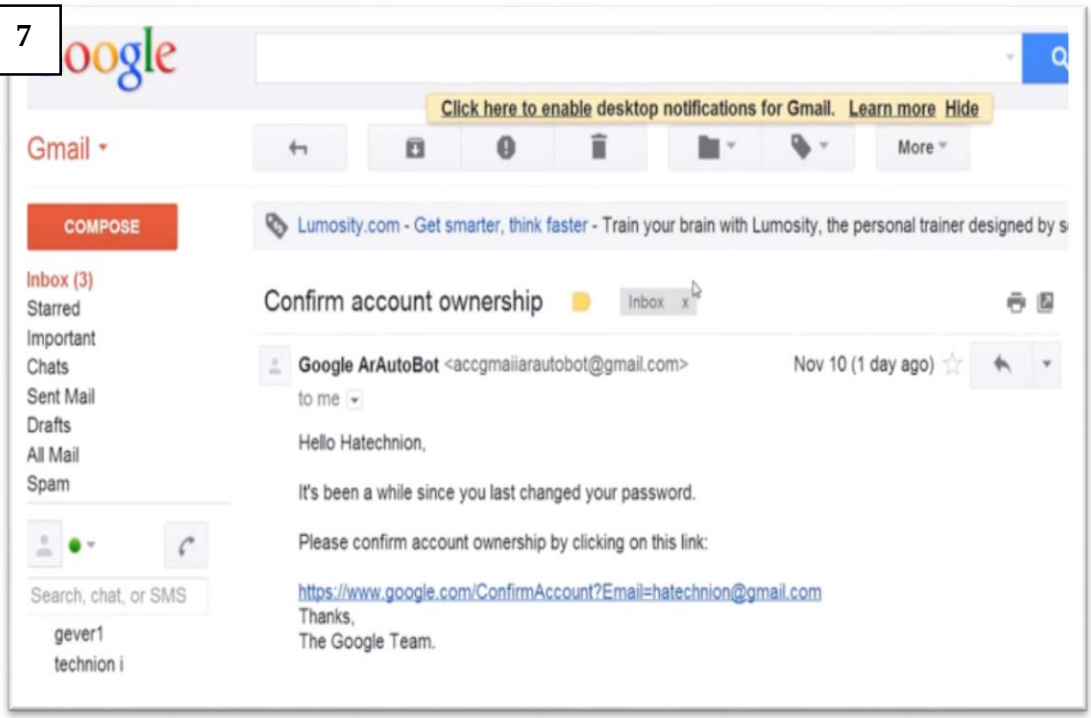


Figura B. 7 - Imagem 7

| Legítimo ☐ | Ilegítimo ☐ | Não sei ☐ |

8

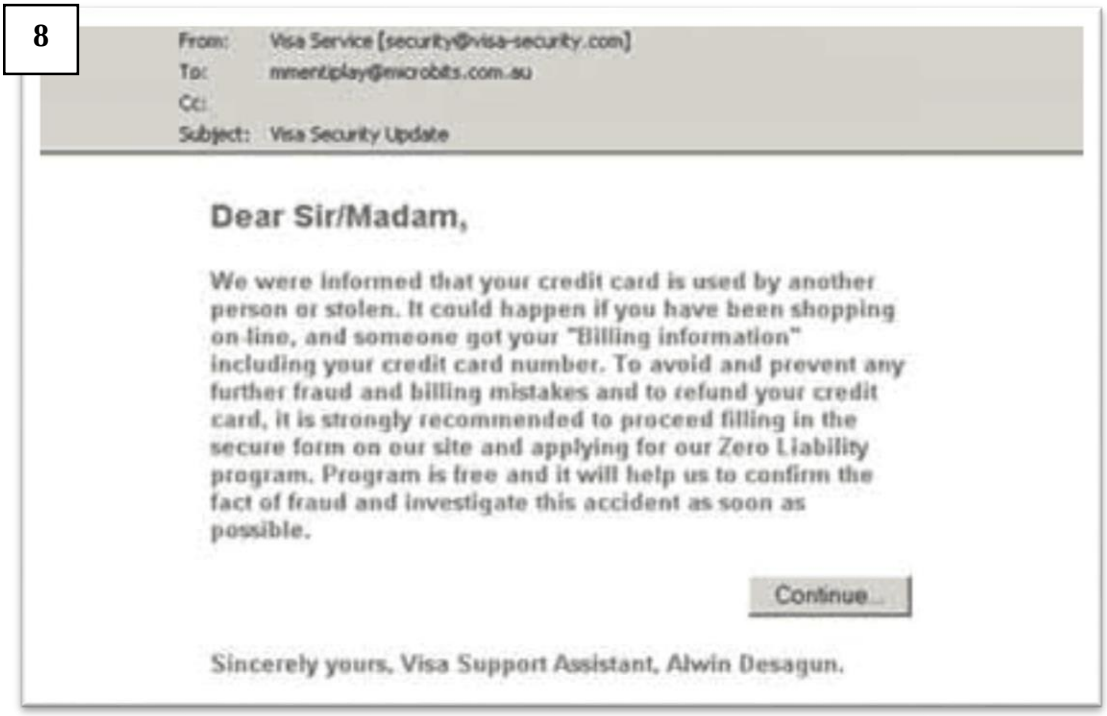


Figura B. 8 - Imagem 8

| Legítimo ☐ | Ilegítimo ☐ | Não sei ☐ |

9

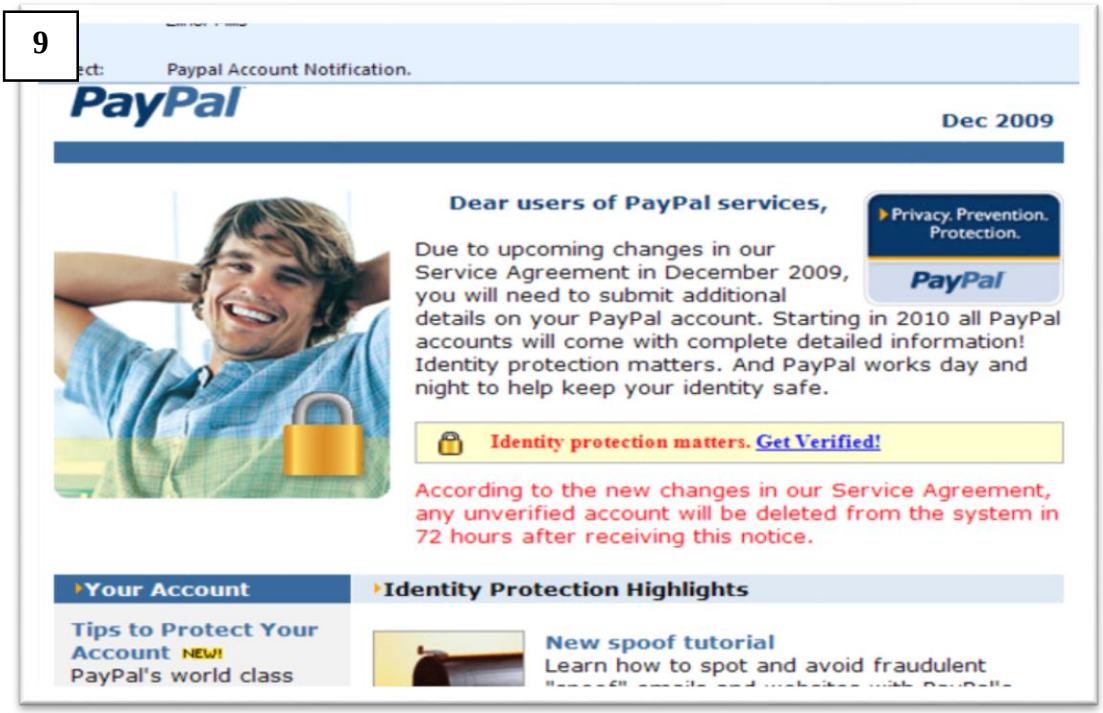


Figura B. 9 - Imagem 9

| Legítimo ☐ | Ilegítimo ☐ | Não sei ☐ |

10

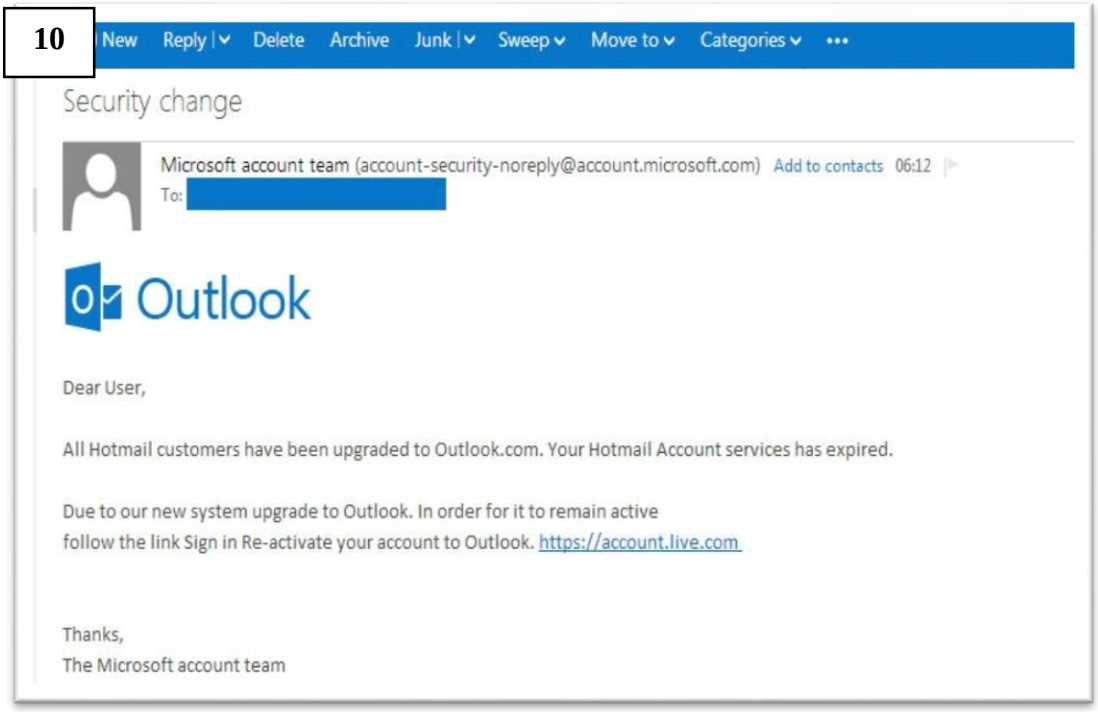


Figura B. 10 - Imagem 10

| Legítimo ☐ | Ilegítimo ☐ | Não sei ☐ |

11

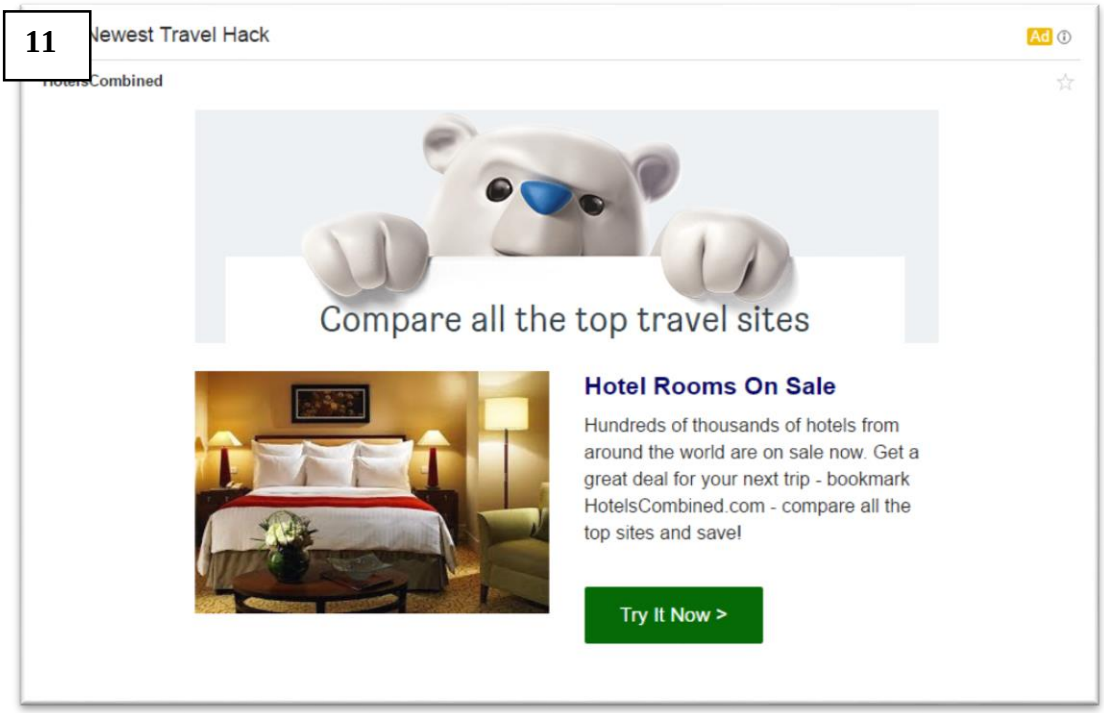


Figura B. 11 - Imagem 11

| Legítimo ☐ | Ilegítimo ☐ | Não sei ☐ |

12

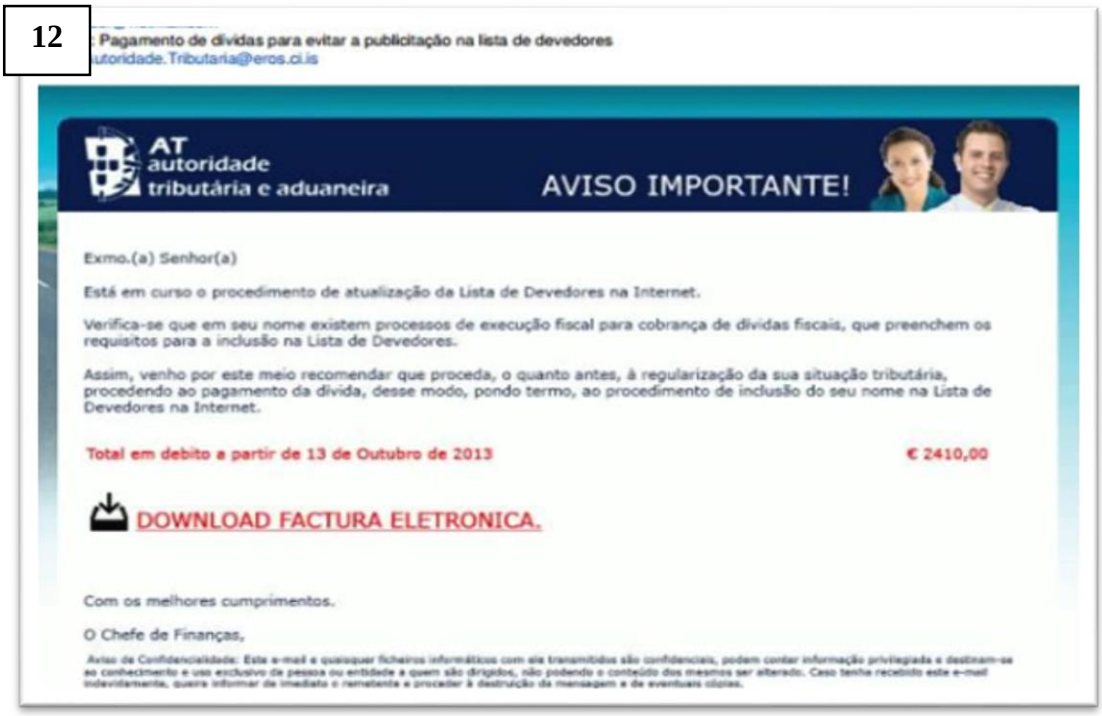


Figura B. 12 - Imagem 12

| Legítimo ☐ | Ilegítimo ☐ | Não sei ☐ |

13

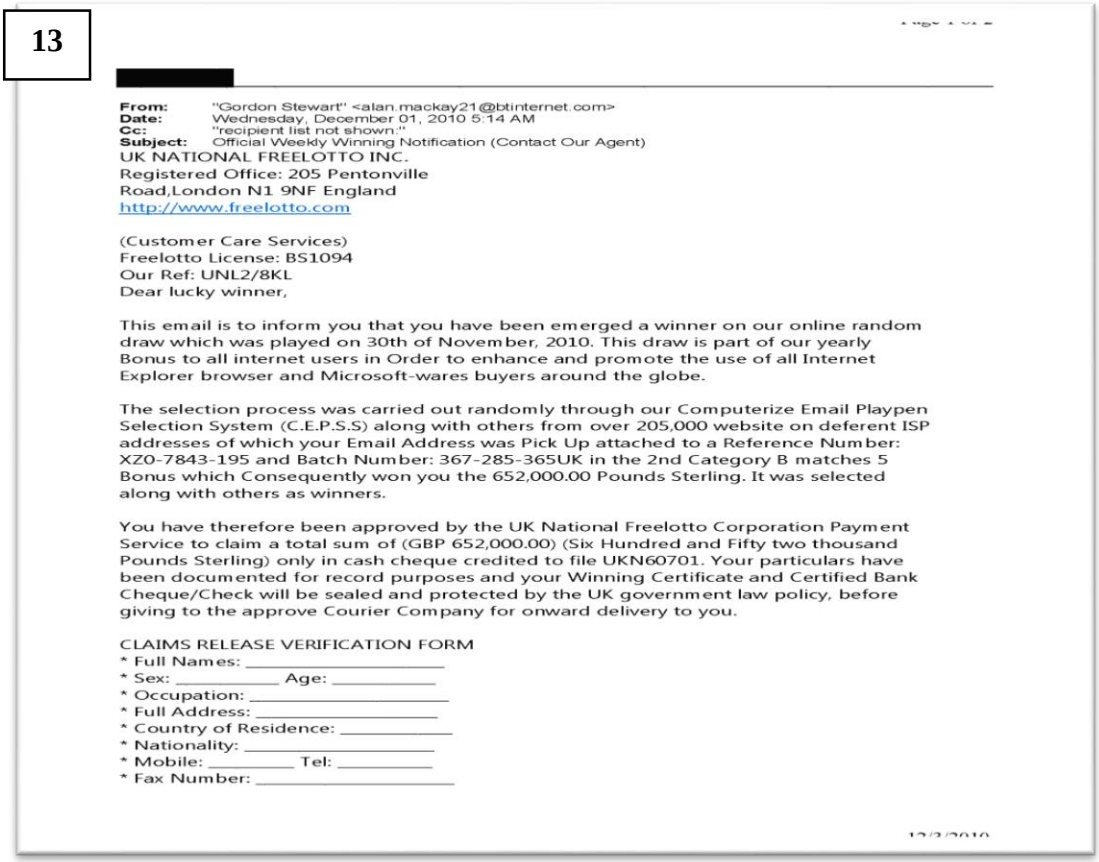


Figura B. 13 - Imagem 13

| Legítimo ☐ | Ilegítimo ☐ | Não sei ☐ |

14

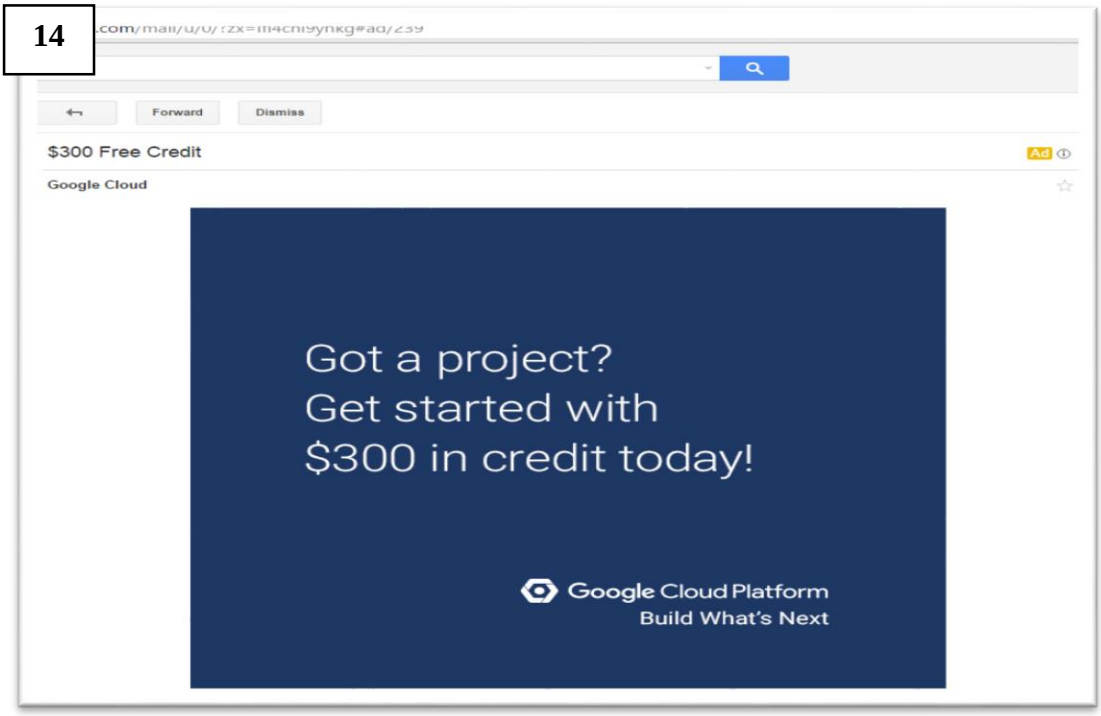


Figura B. 14 - Imagem 14

| Legítimo ☐ | Ilegítimo ☐ | Não sei ☐ |

15

caixadirecta [mailto:cgd@cgd.pt]
Enviada: terça-feira, 4 de Janeiro de 2011 09:49
Para:
Assunto: Aviso de Movimentação

caixadirecta on-line

Por indicação de Tatiana Souza, informamos que foi efectuada no

serviço **Caixadirecta on-line**, a operação **Transferência** com os seguintes dados:

Data da Operação 2011/01/04

Nr Doc 965645948(782kb)

Figura B. 15 - Imagem 15

| Legítimo ☐ | Ilegítimo ☐ | Não sei ☐ |

16

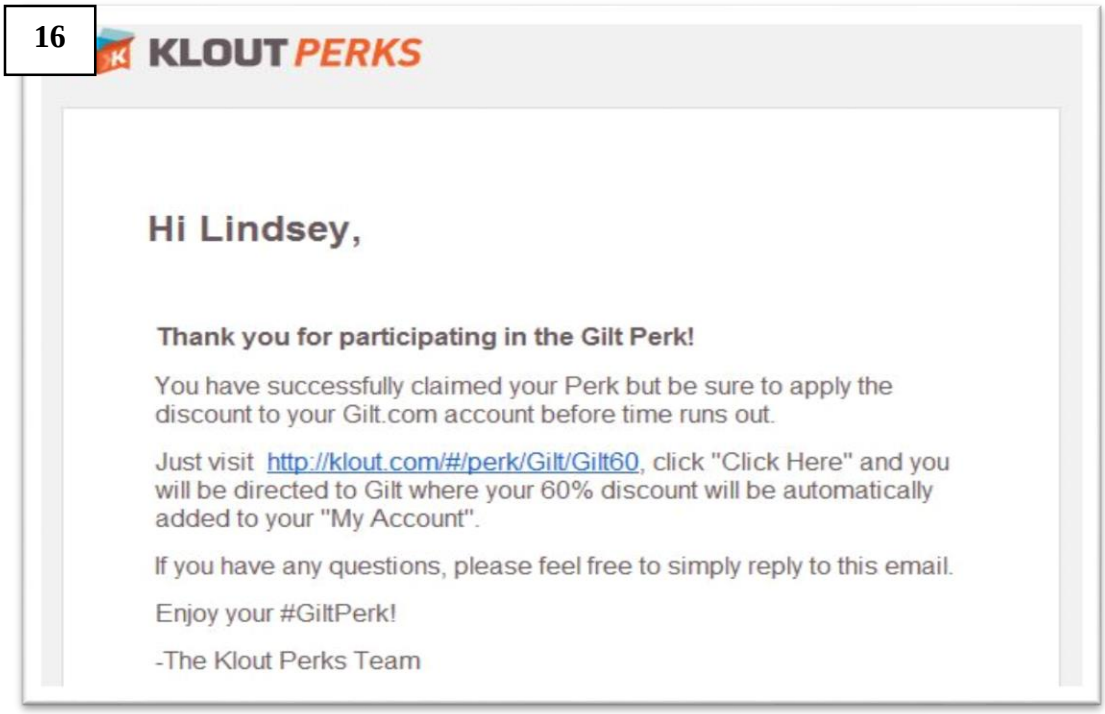


Figura B. 16 - Imagem 16

| Legítimo ☐ | Ilegítimo ☐ | Não sei ☐ |

17

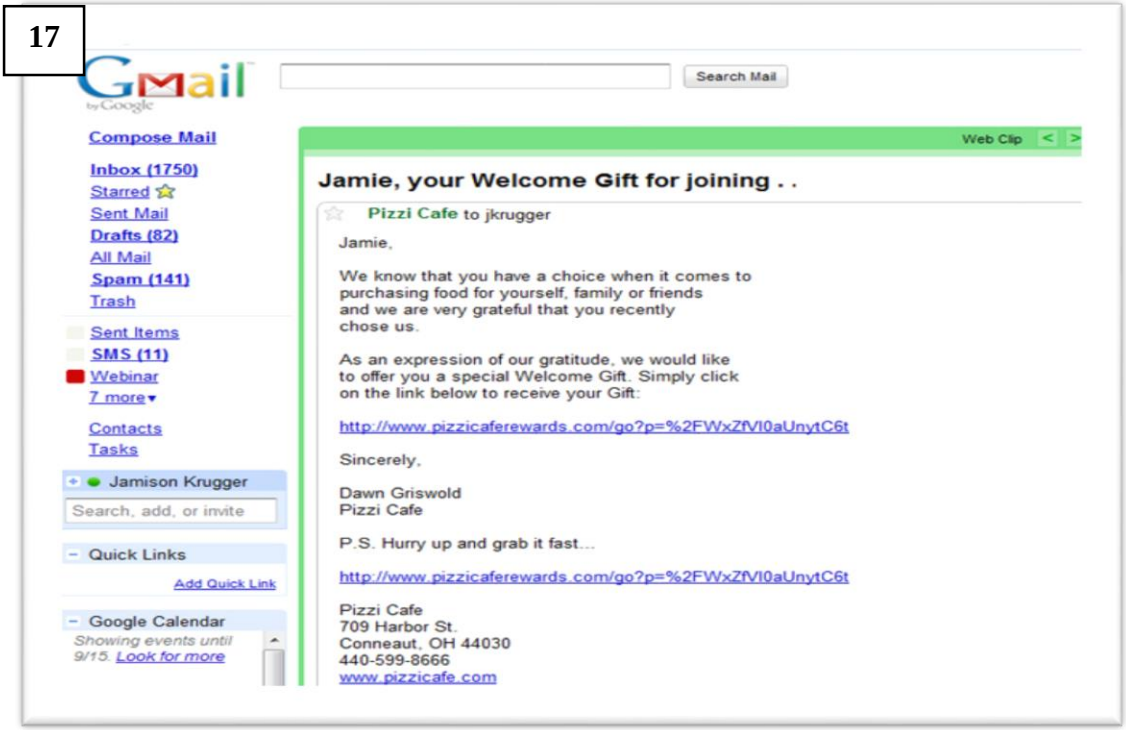


Figura B. 17 - Imagem 17

| Legítimo ☐ | Ilegítimo ☐ | Não sei ☐ |

18

Figura B. 18 - Imagem 18

| Legítimo ☐ | Ilegítimo ☐ | Não sei ☐ |

19

Figura B. 19 - Imagem 19

| Legítimo ☐ | Ilegítimo ☐ | Não sei ☐ |

20

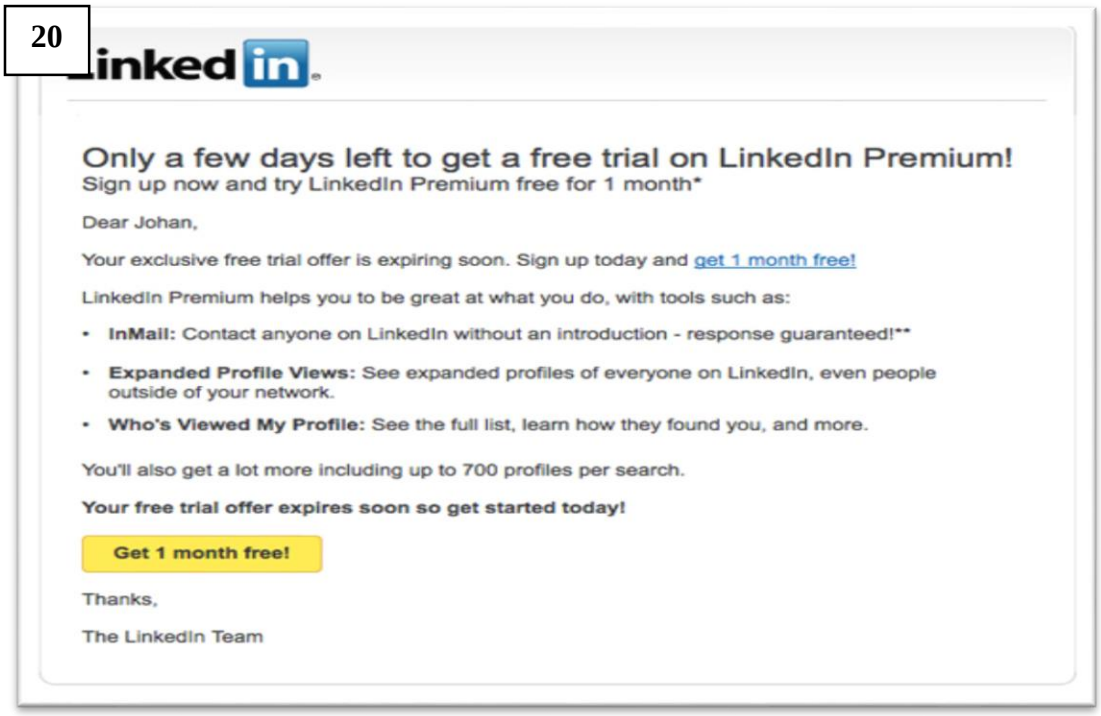


Figura B. 20 - Imagem 20

| Legítimo ☐ | Ilegítimo ☐ | Não sei ☐ |

21

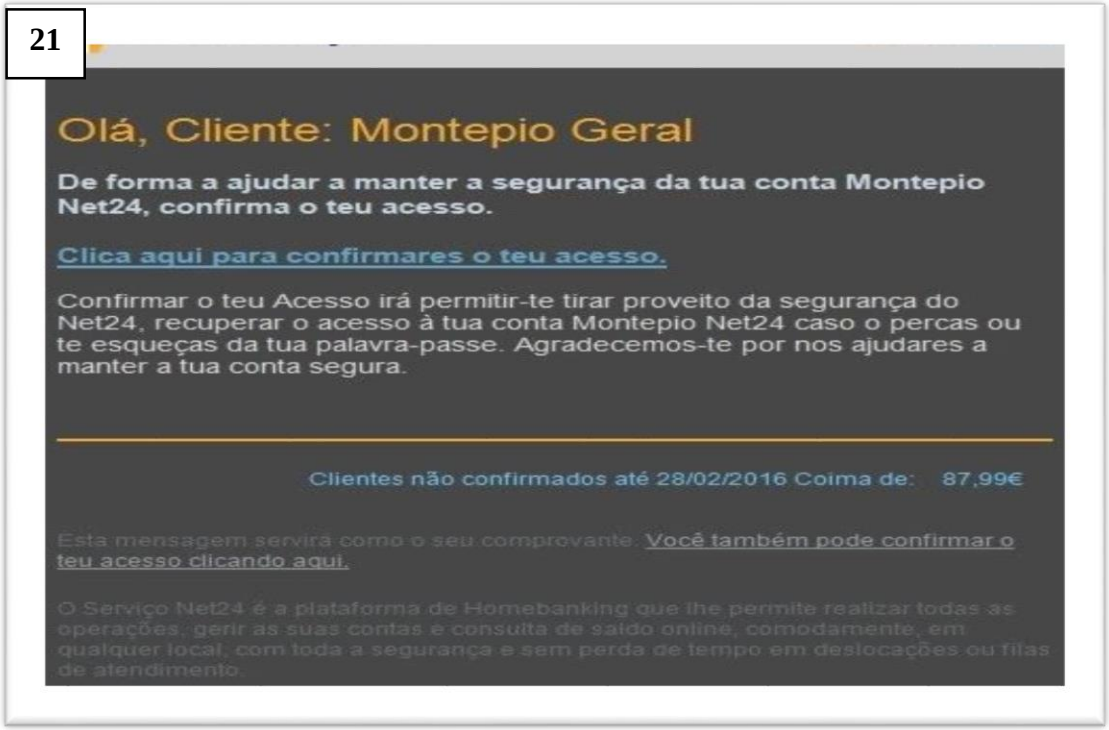


Figura B. 21 - Imagem 21

| Legítimo ☐ | Ilegítimo ☐ | Não sei ☐ |

22

From: Comprafacil.com <compras@comprafacil.com.br>
Subject: **Pedido Aprovado Separando Produto Para Envio.**
Date: May 7, 2012 4:56:20 PM GMT+01:00
To: Paulo Laureano
X-Spam-Status: No, score=3.5 required=15.0 tests=HTML_IMAGE_ONLY_20, HTML_MESSAGE,MIME_HTML_ONLY,RCVD_IN_BRBL_LASTEXT,T_REMOTE_IMAGE, T_RP_MATCHES_RCVD autolearn=disabled version=3.3.2

comprafacil.com

Prezado(a) Cliente,

Gostaria de informar que seu pedido 24520125474NH foi autorizado com sucesso pela administradora do seu cartão de crédito.Estamos providenciando o envio de sua mercadoria, para acompanhar seu pedido acesse o link abaixo.
Sua mercadoria já está sendo processado para envio.
Lembramos que para facilitar o recebimento, é necessário que haja alguem autorizado no local da entrega.

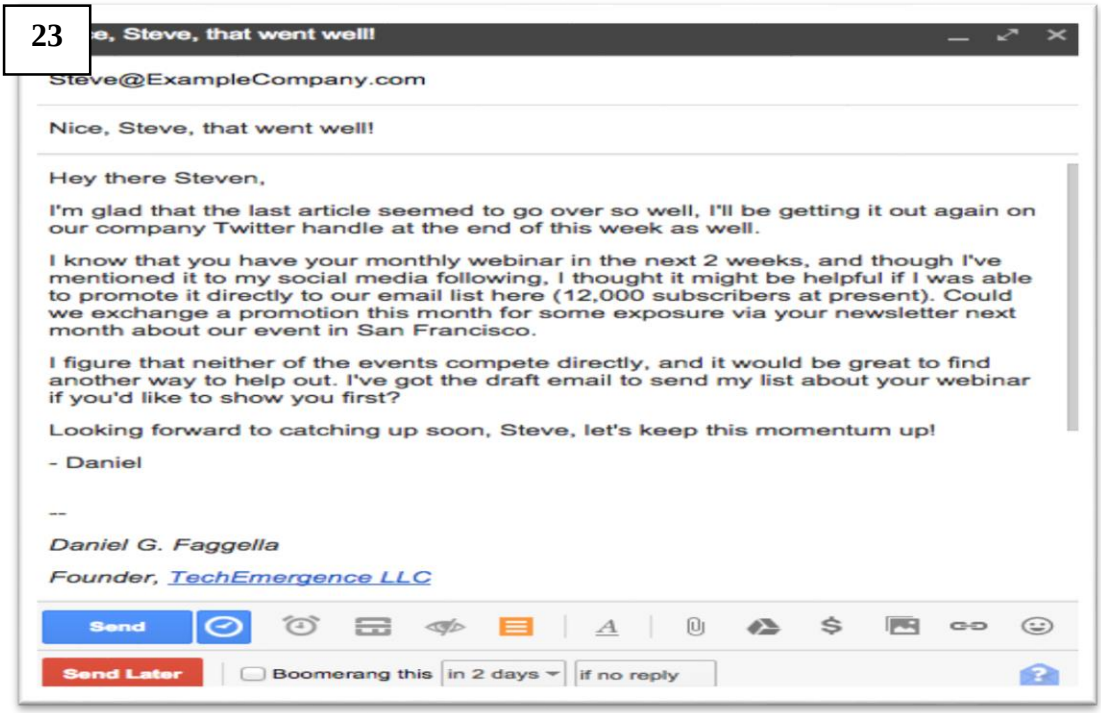
Para acompanhar o status do seu pedido, por favor acesse o link abaixo:
www.comprafacil.com.br/pedido.asp?pedido24520125474NH=sp?confirmada

Atenciosamente, SAC - www.comprafacil.com.br

Figura B. 22 - Imagem 22

| Legítimo ☐ | Ilegítimo ☐ | Não sei ☐ |

23



e, Steve, that went well!

Steve@ExampleCompany.com

Nice, Steve, that went well!

Hey there Steven,

I'm glad that the last article seemed to go over so well, I'll be getting it out again on our company Twitter handle at the end of this week as well.

I know that you have your monthly webinar in the next 2 weeks, and though I've mentioned it to my social media following, I thought it might be helpful if I was able to promote it directly to our email list here (12,000 subscribers at present). Could we exchange a promotion this month for some exposure via your newsletter next month about our event in San Francisco.

I figure that neither of the events compete directly, and it would be great to find another way to help out. I've got the draft email to send my list about your webinar if you'd like to show you first?

Looking forward to catching up soon, Steve, let's keep this momentum up!

- Daniel

--

Daniel G. Faggella

Founder, TechEmergence LLC

Send | Send Later | Boomerang this in 2 days if no reply

Figura B. 23 - Imagem 23

| Legítimo ☐ | Ilegítimo ☐ | Não sei ☐ |

24

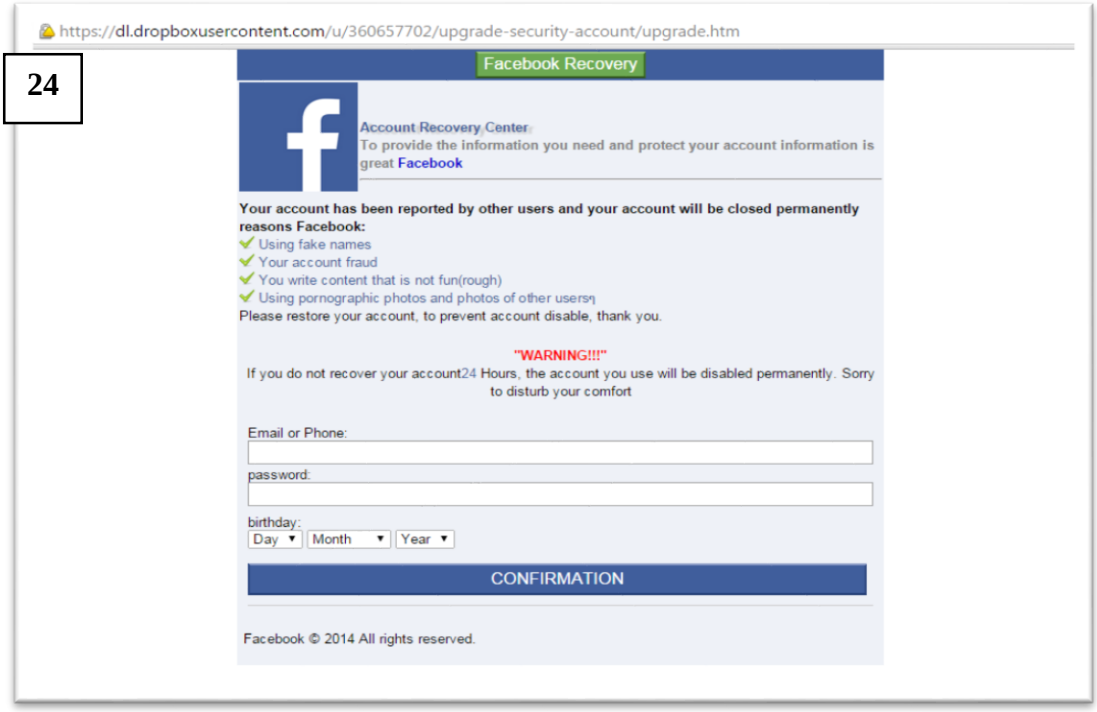


Figura B. 24 - Imagem 24

| Legítimo ☐ | Ilegítimo ☐ | Não sei ☐ |

25

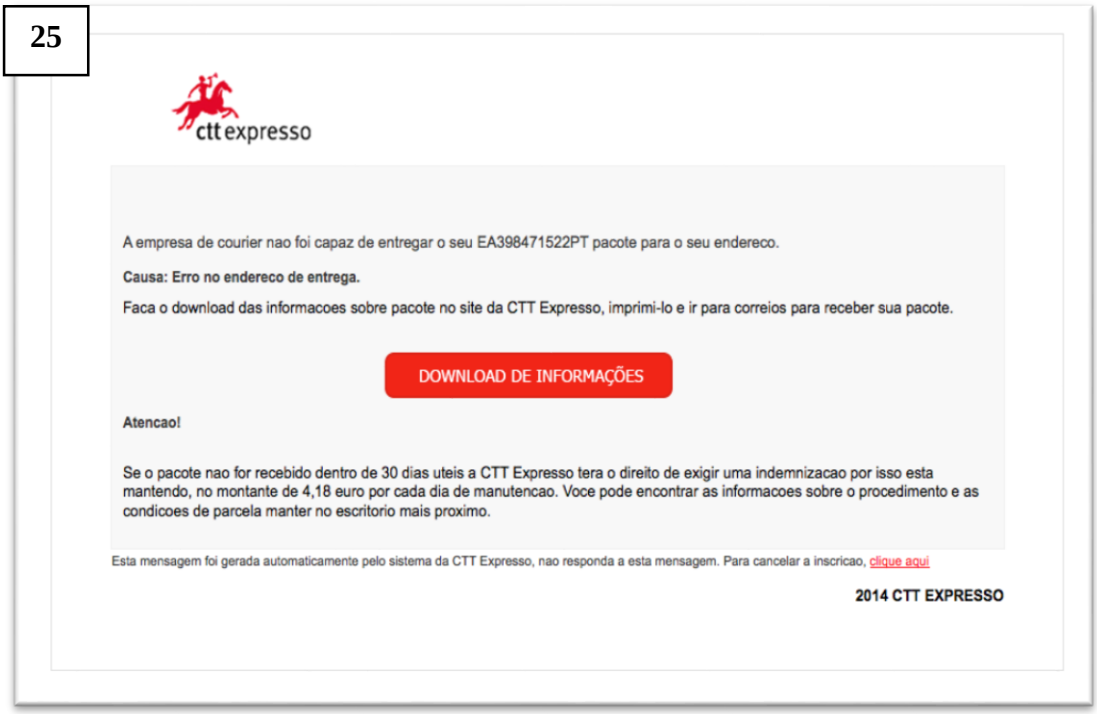


Figura B. 25 - Imagem 25

| Legítimo ☐ | Ilegítimo ☐ | Não sei ☐ |

Muito Obrigado Pela Sua Participação

APÊNDICE C – APRESENTAÇÃO DE SENSIBILIZAÇÃO

A Apresentação de Sensibilização é constituído por trinta e um diapositivos de elaboração própria, as referências utilizadas para o seu conteúdo encontram-se tanto no capítulo III - Métodos e Técnicas do Trabalho de Campo, como no próprio diapositivo.

A elaboração desta apresentação foi pormenorizada no mesmo capítulo, Métodos e Técnicas do Trabalho de Campo, e o seu objetivo seria capacitar os recetores de noções elementares sobre os ataques de *phishing* como: O que são? Quais as técnicas existentes? Qual a sua importância para a organização militar? Como nos devemos defender? Como os detetamos?

Nas próximas paginas, que se seguem, apresentam as imagens dos diapositivos da sensibilização para uma melhor perceção do seu conteúdo e da sua construção.

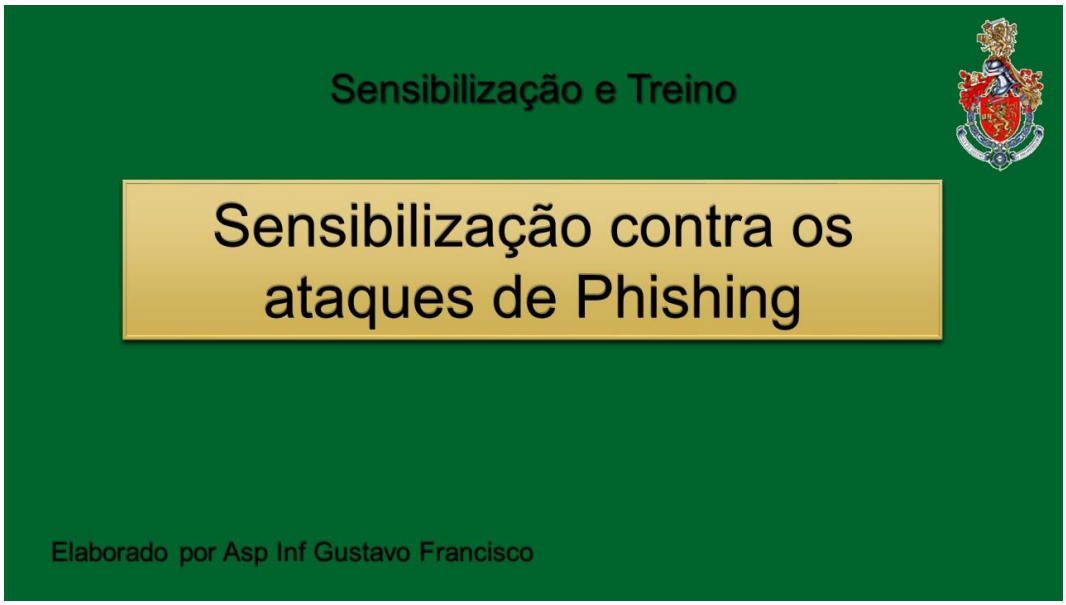


Figura C. 1 - Diapositivo nº 1 (Elaboração Própria)

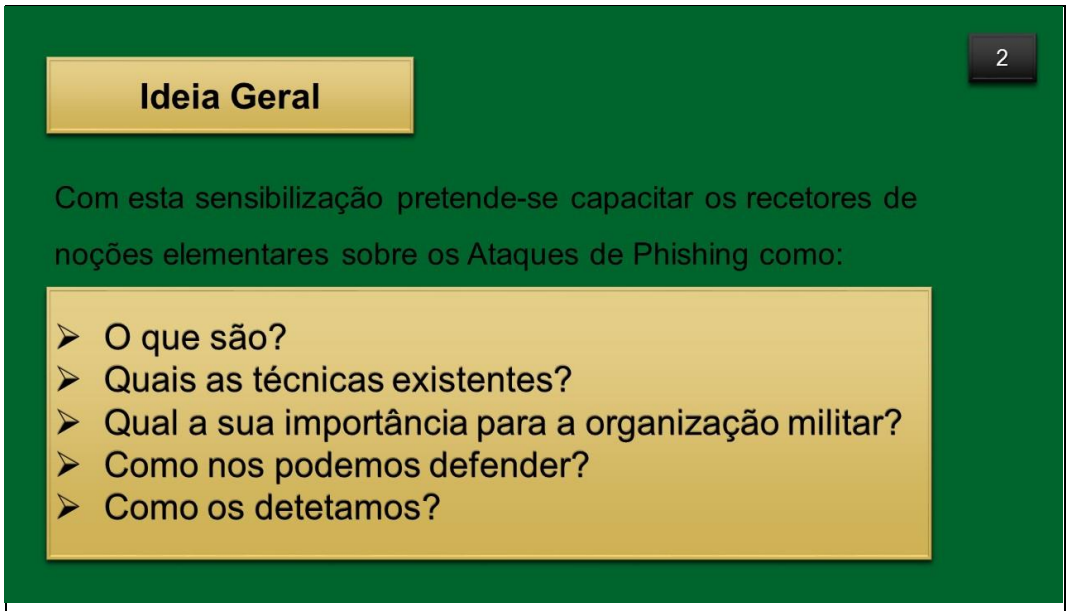


Figura C. 2 - Diapositivo nº 2 (Elaboração Própria)

Figura C. 3 - Diapositivo nº 3 (Elaboração Própria)

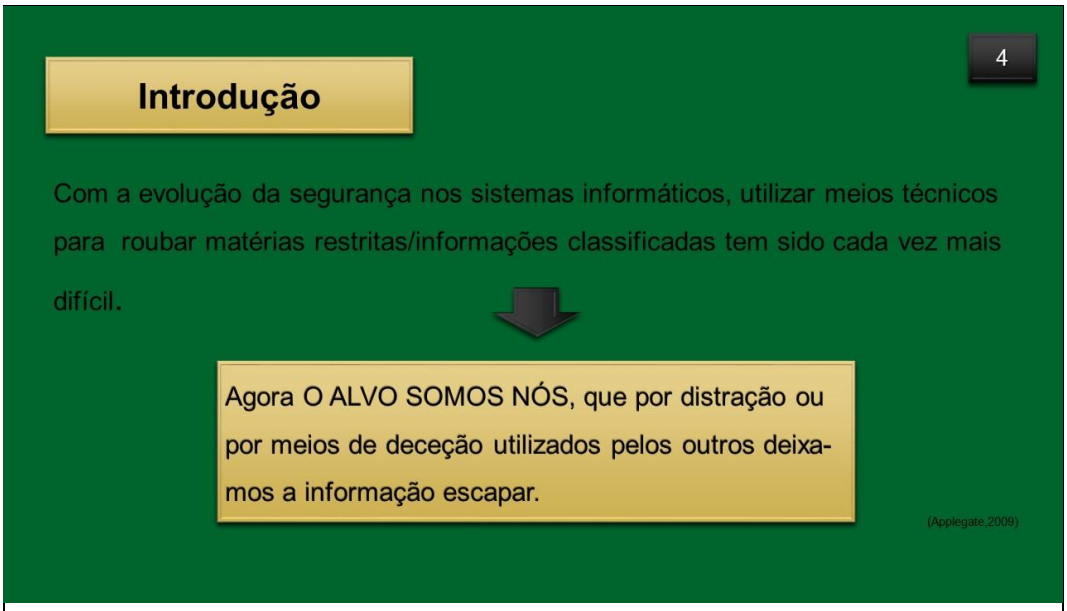


Figura C. 4 - Diapositivo nº 4 (Elaboração Própria)

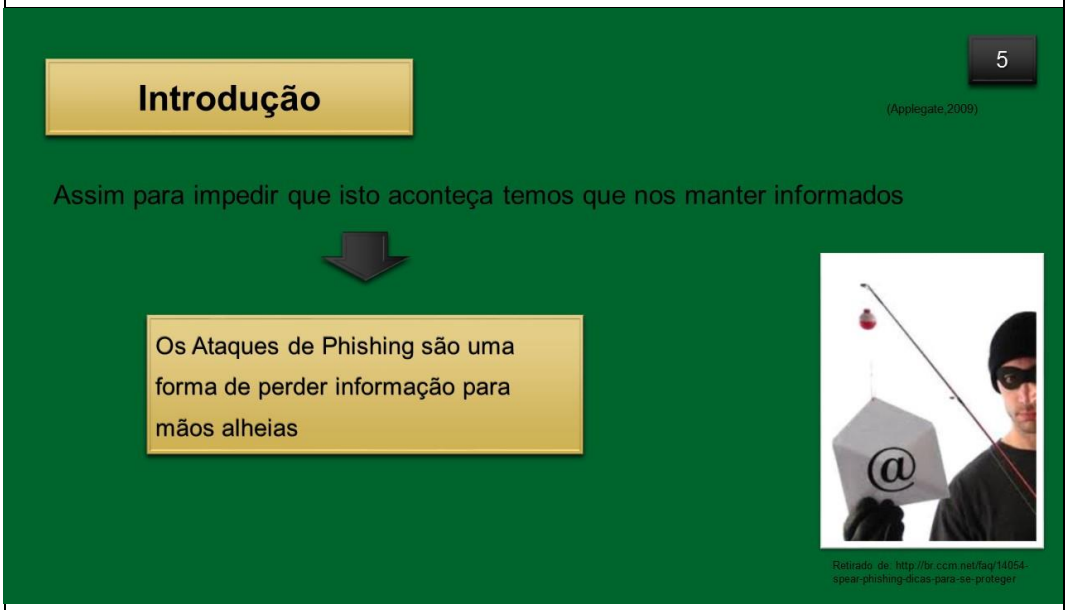


Figura C. 5 - Diapositivo nº 5 (Elaboração Própria)

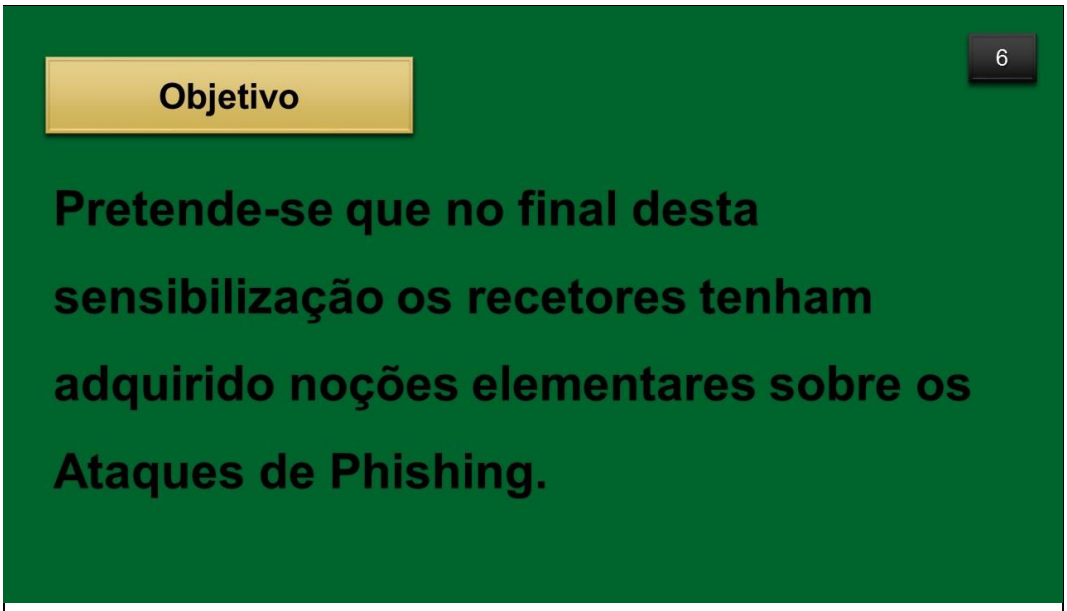


Figura C. 6 - Diapositivo nº 6 (Elaboração Própria)

Figura C. 7 - Diapositivo nº 7 (Elaboração Própria)

Figura C. 8 - Diapositivo nº 8 (Elaboração Própria)

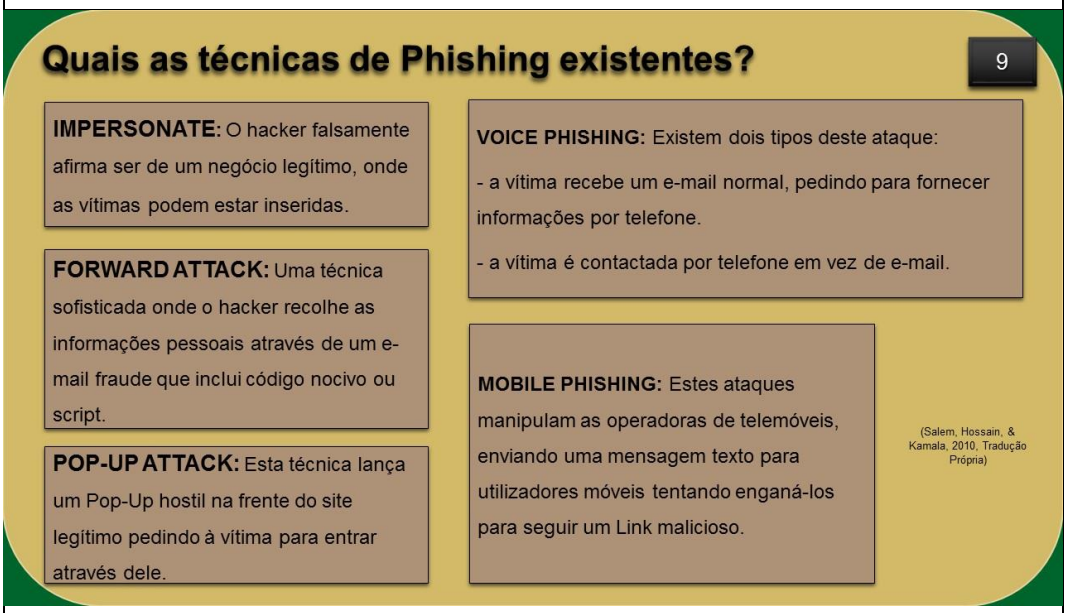


Figura C. 9 - Diapositivo nº 9 (Elaboração Própria)

Figura C. 10 - Diapositivo nº 10 (Elaboração Própria)

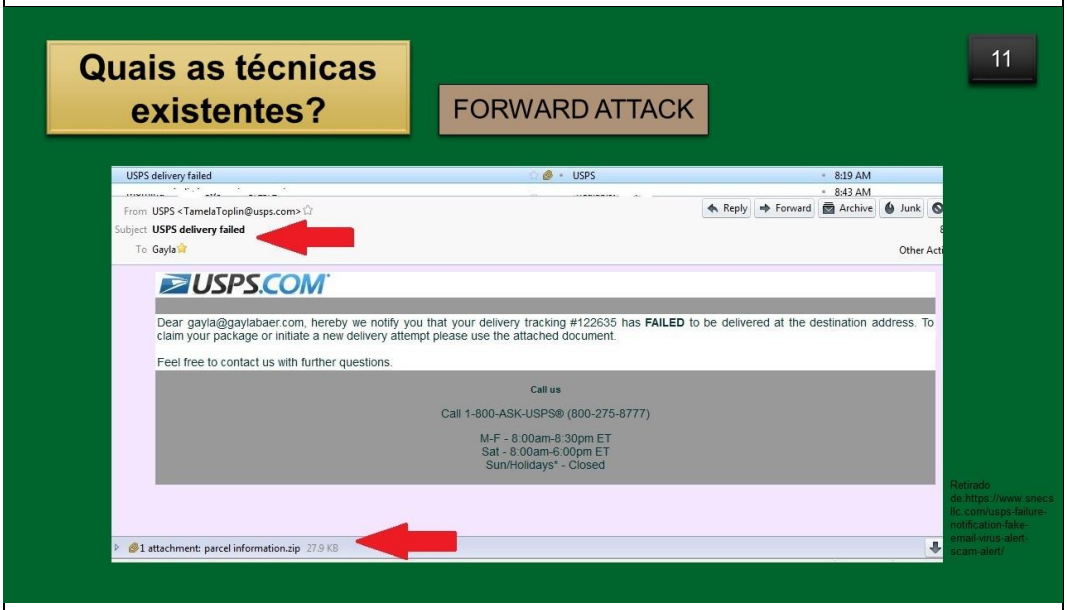


Figura C. 11 - Diapositivo nº 11 (Elaboração Própria)

Figura C. 12 - Diapositivo nº 12 (Elaboração Própria)

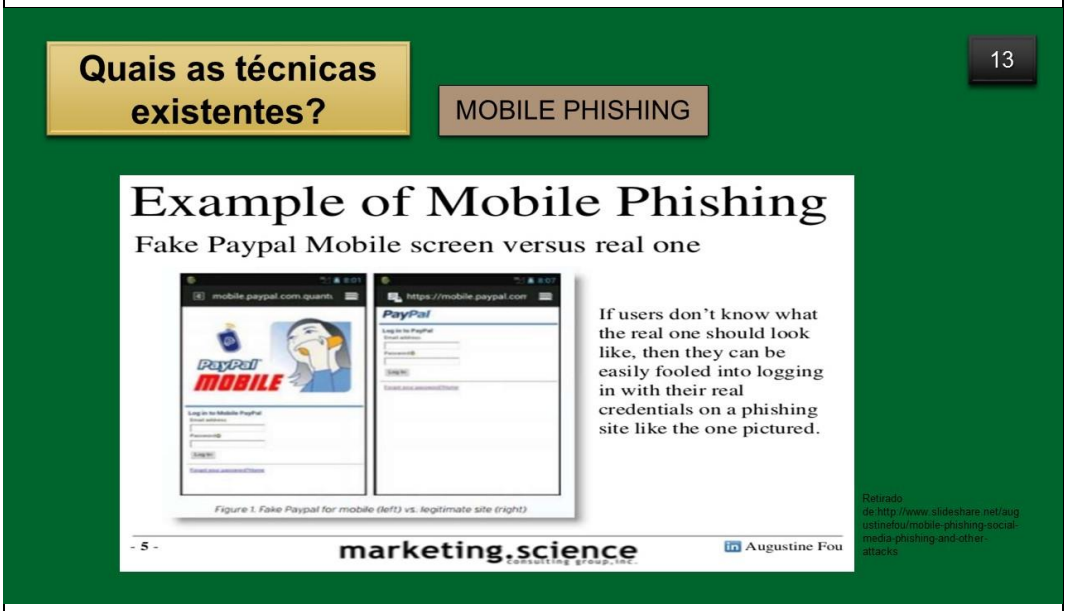


Figura C. 13 - Diapositivo nº 13 (Elaboração Própria)

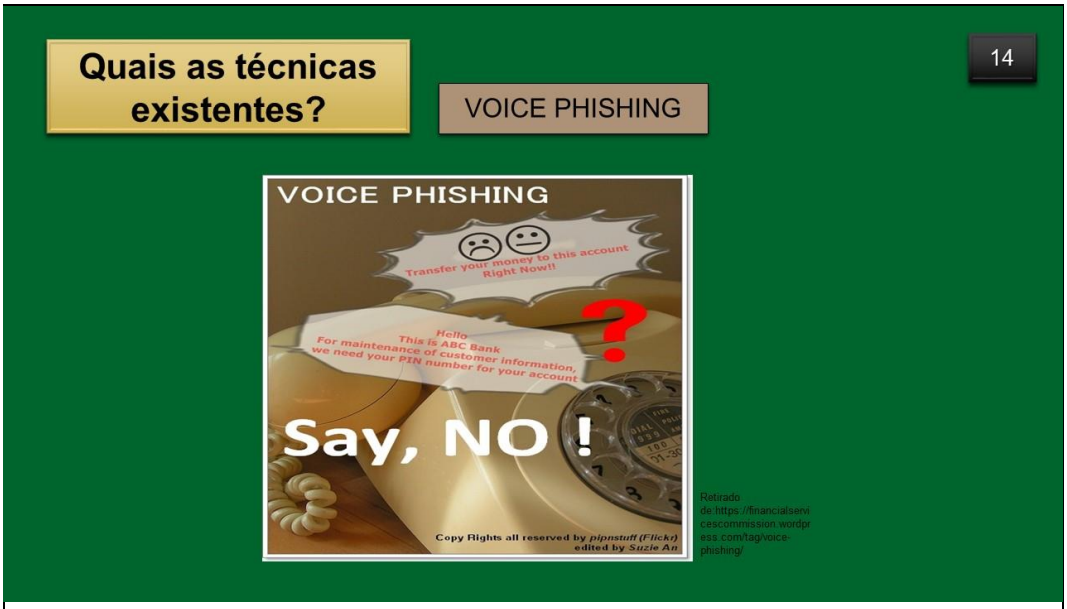


Figura C. 14 - Diapositivo nº 14 (Elaboração Própria)

Figura C. 15 - Diapositivo nº 15 (Elaboração Própria)

Figura C. 16 - Diapositivo nº 16 (Elaboração Própria)

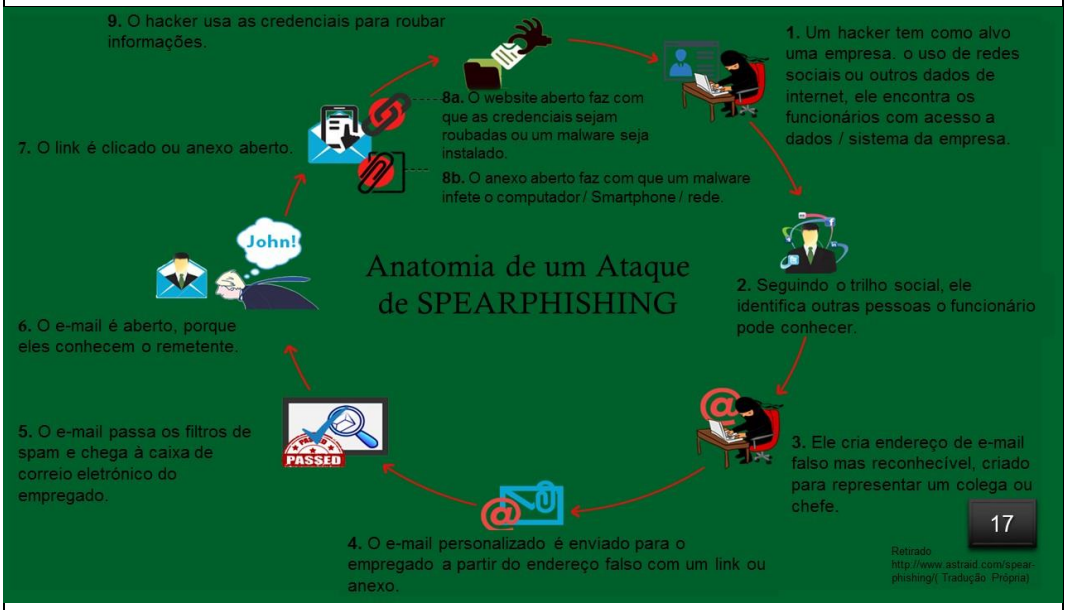


Figura C. 17 - Diapositivo nº 17 (Elaboração Própria)

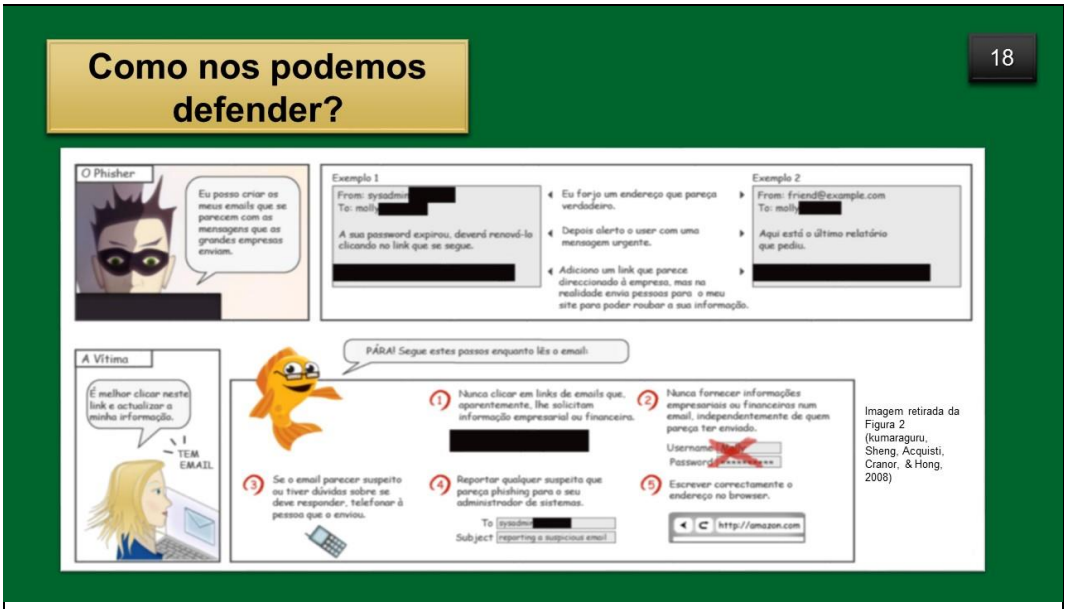


Figura C. 18 - Diapositivo nº 18 (Elaboração Própria)

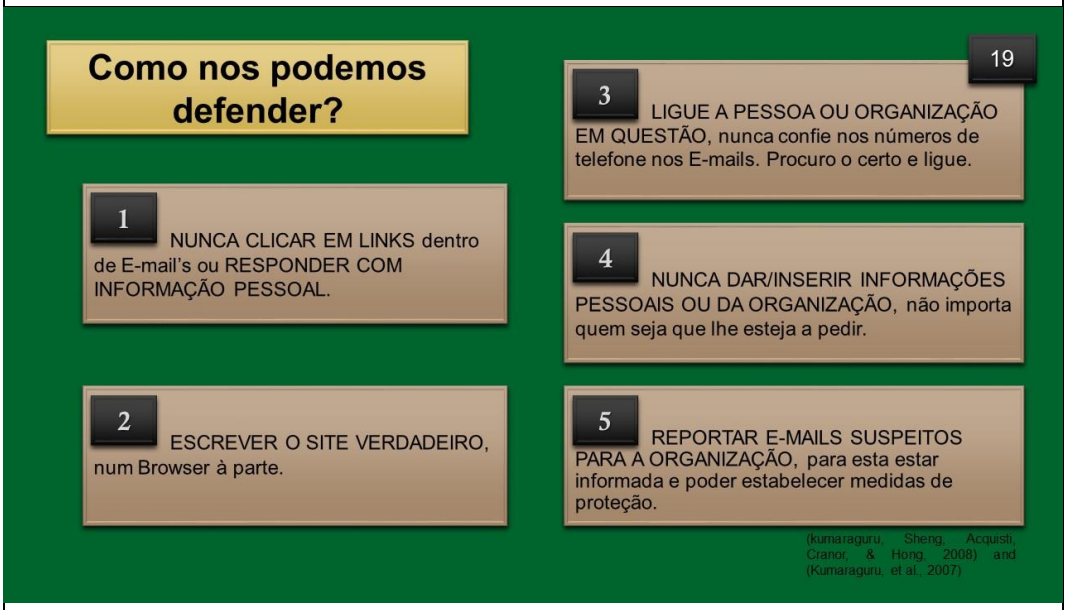


Figura C. 19 - Diapositivo nº 19 (Elaboração Própria)

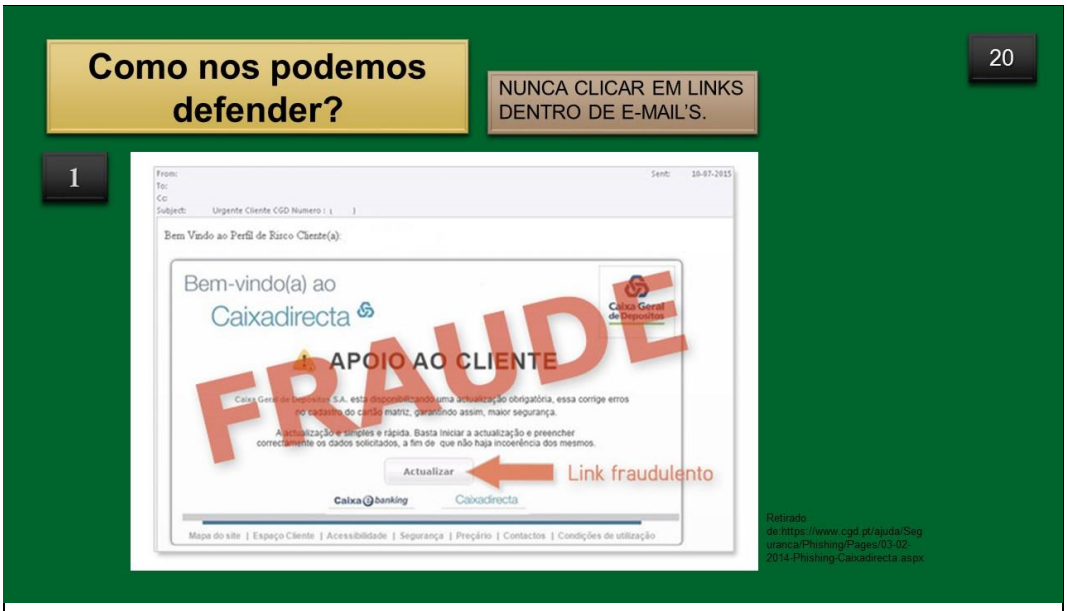


Figura C. 20 - Diapositivo nº 20 (Elaboração Própria)

Figura C. 21 - Diapositivo nº 21 (Elaboração Própria)

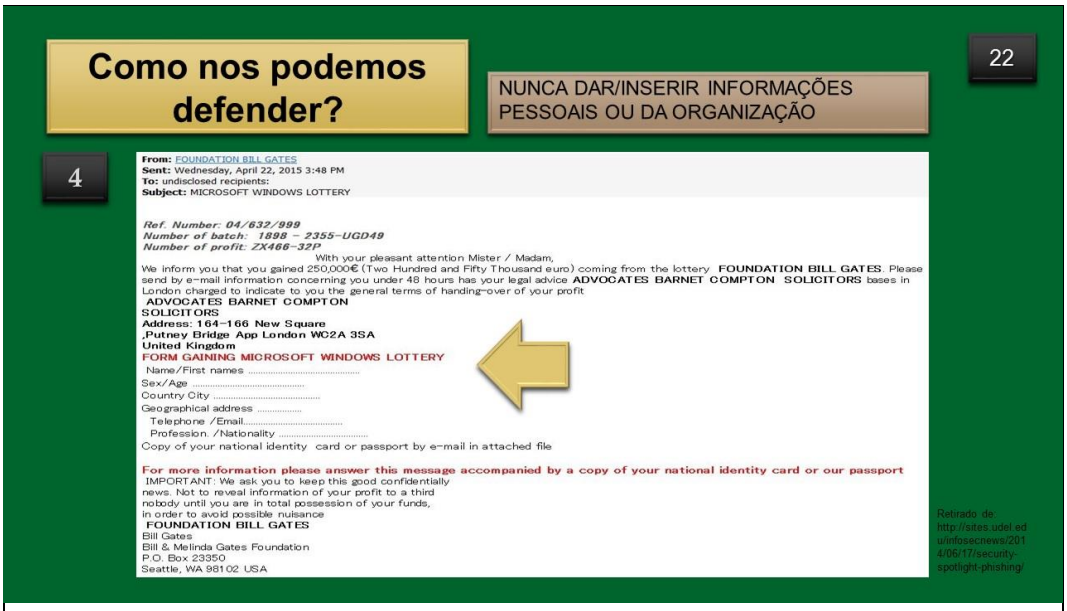


Figura C. 22 - Diapositivo nº 22 (Elaboração Própria)

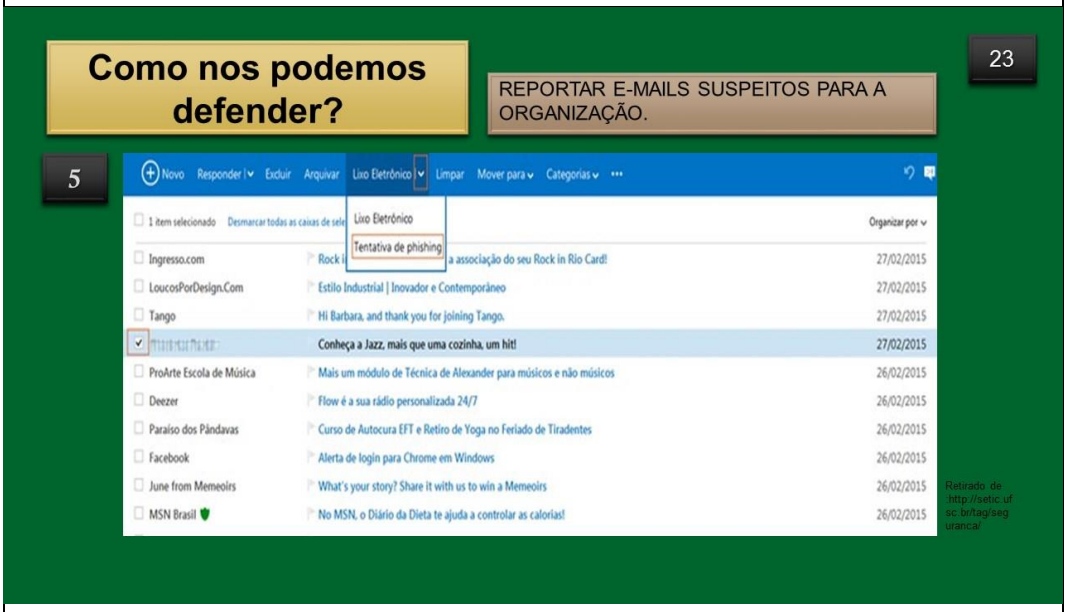


Figura C. 23 - Diapositivo nº 23 (Elaboração Própria)

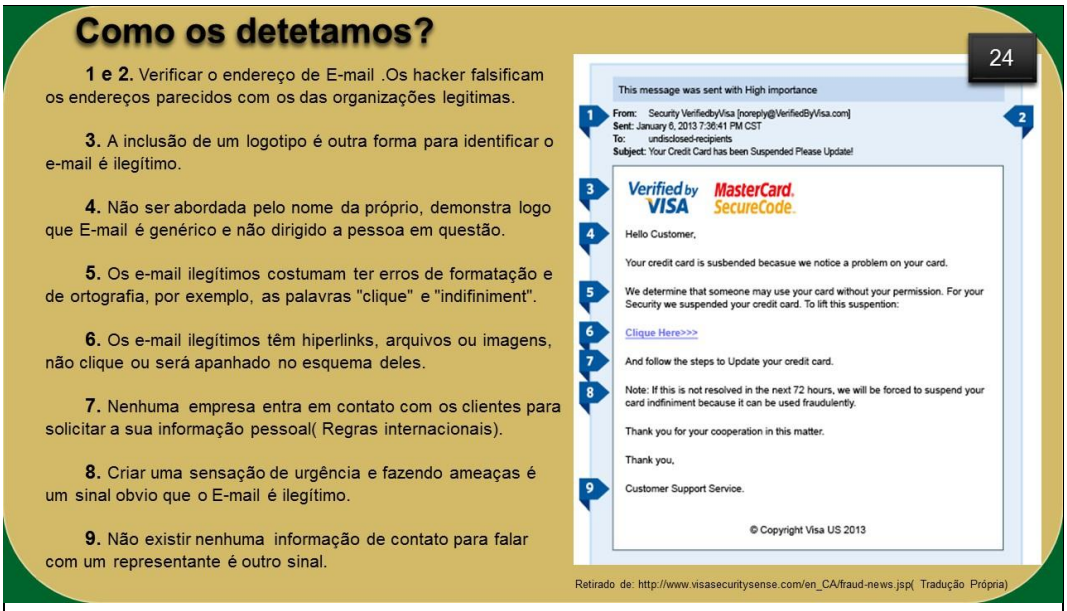


Figura C. 24 - Diapositivo nº 24 (Elaboração Própria)

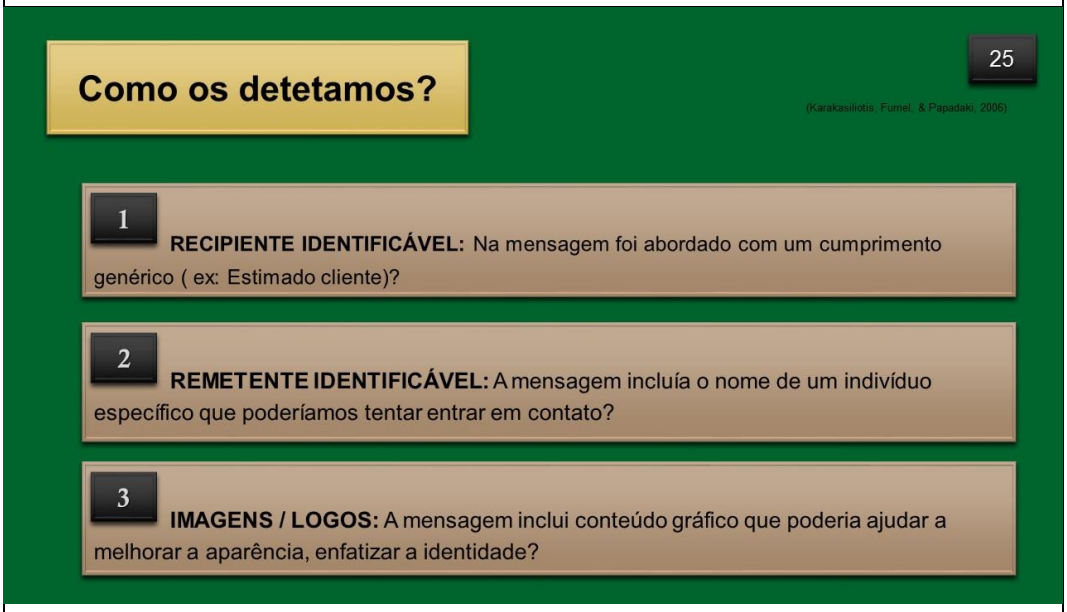


Figura C. 25 - Diapositivo nº 25 (Elaboração Própria)

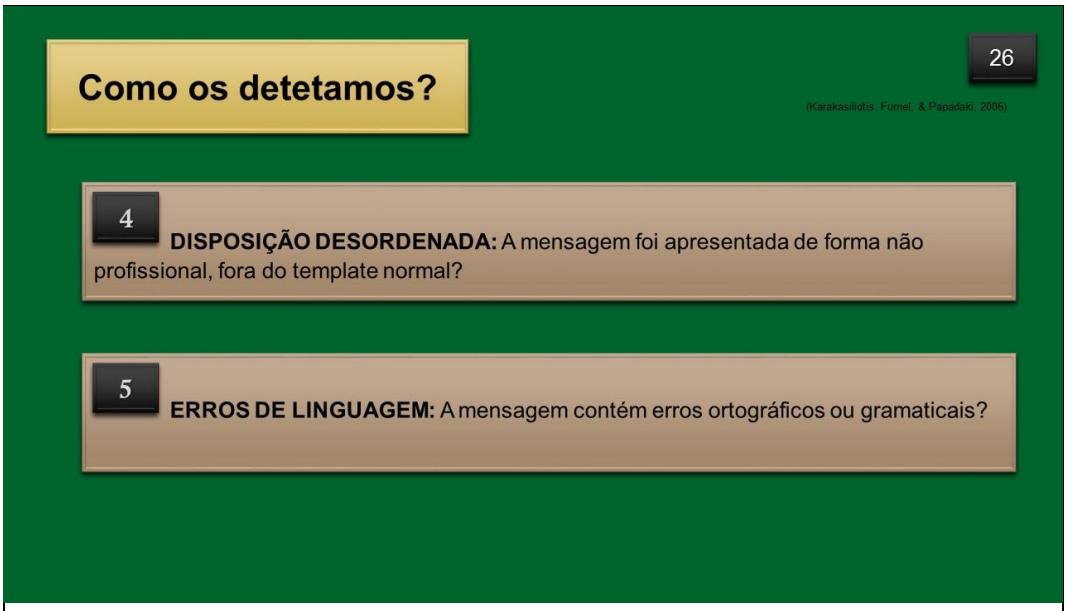


Figura C. 26 - Diapositivo nº 26 (Elaboração Própria)

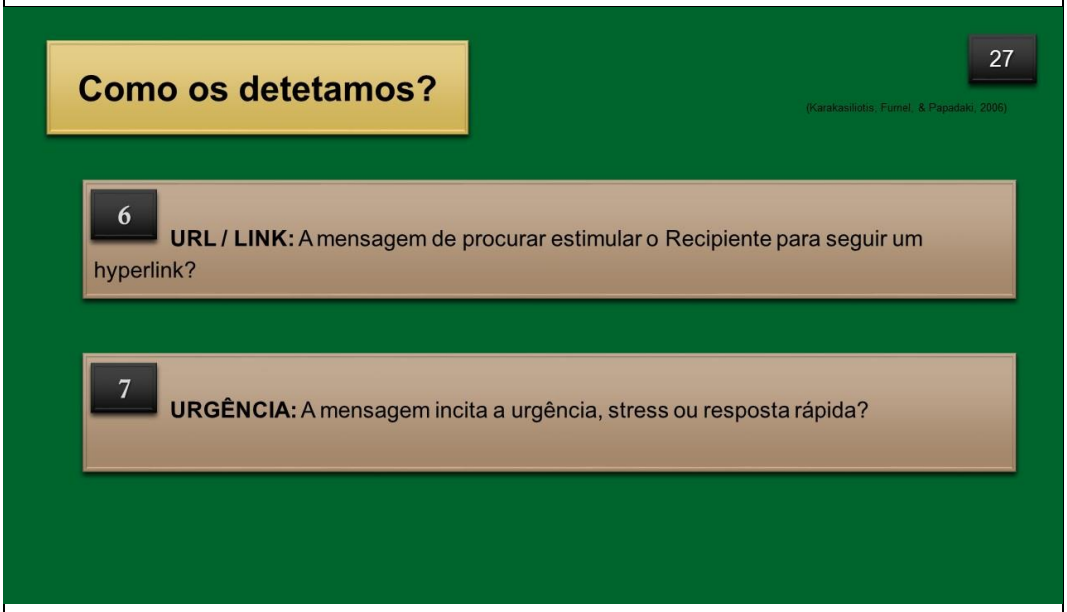


Figura C. 27 - Diapositivo nº 27 (Elaboração Própria)

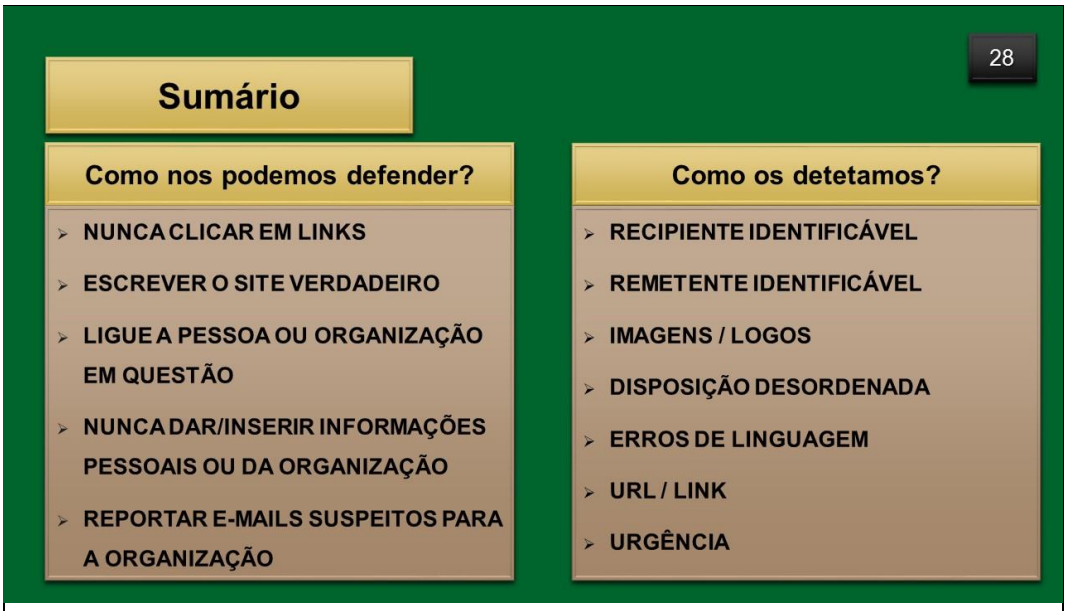


Figura C. 28 - Diapositivo nº 28 (Elaboração Própria)

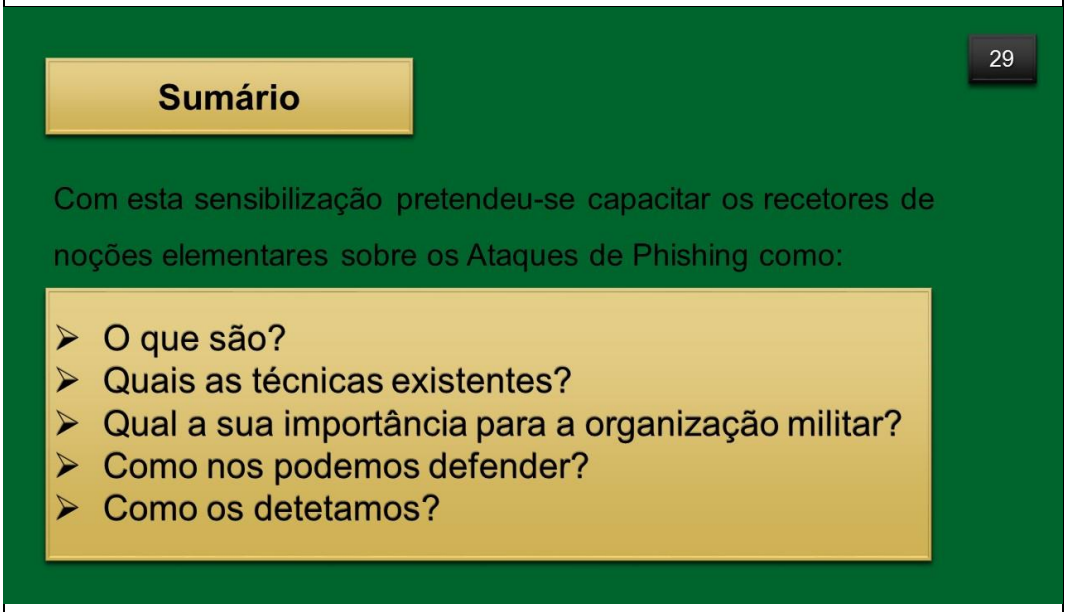


Figura C. 29 - Diapositivo nº 29 (Elaboração Própria)

Figura C. 30 - Diapositivo nº 30 (Elaboração Própria)

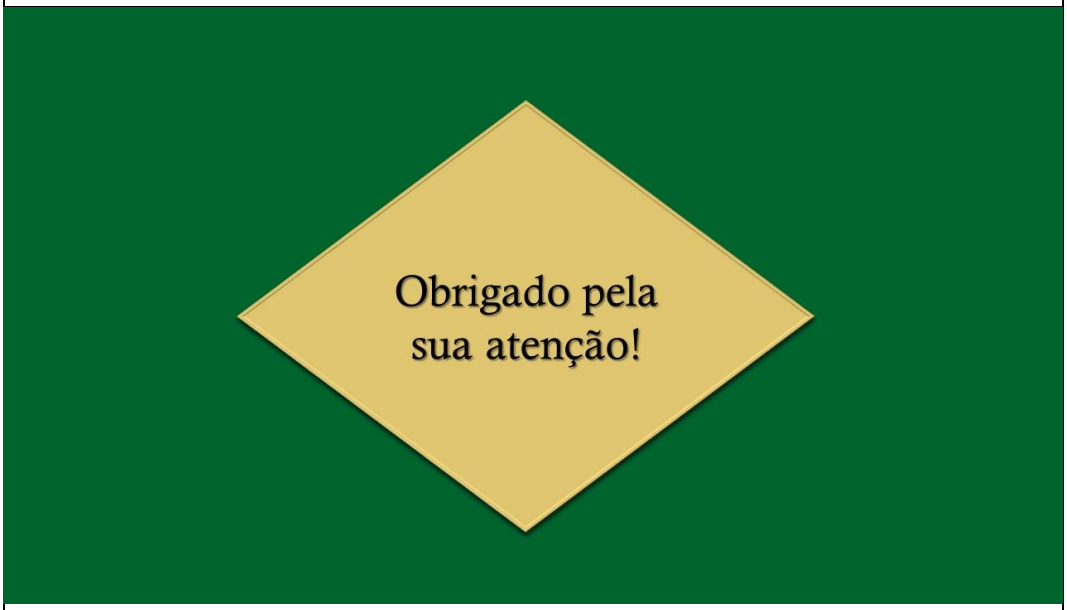


Figura C. 31 - Diapositivo nº 31 (Elaboração Própria)