Universidade Federal de Pernambuco
Centro de Informática

Graduação em Ciência da Computação

Avaliação da suscetibilidade dos discentes de TI a ataques de phishing

Simone Campos Cohen

Trabalho de Graduação

Recife
Dezembro 2017

Universidade Federal de Pernambuco
Centro de Informática

Simone Campos Cohen

Avaliação da suscetibilidade dos discentes de TI a ataques de phishing

Trabalho apresentado ao curso de Ciência da Computação da Universidade Federal de Pernambuco como requisito parcial para obtenção do grau de Bacharel em Ciência da Computação.

Orientador: Vinicius Cardoso Garcia

Recife
Dezembro 2017

Agradecimentos

Em primeiro lugar, tenho muito a agradecer à minha família, em particular e sem distinção, a minha avó, Clara; meu pai, Roberto; e minhas tias, Sheila e Suely. Agradecer por não desistirem de mim nunca, por formarem a pessoa que sou hoje, por sempre estarem ao meu lado em todas as situações, pelo amor, apoio, por me proporcionarem todos os meios possíveis para chegar até aqui, além de todo o resto.

Agradeço aos amigos que fiz, pela companhia e por todo o apoio. E jamais deixaria de enfatizar com muito carinho as melhores pessoas que podia ter conhecido durante esse longo caminho, mas que passou tão rápido: Camila (“dogs!”), Júlia (“woop”) e Victor (“lindo e maravilhoso”), cada um à sua maneira que, no final das contas, fez o Clique completo. Apesar dos aperreios, das noites viradas, dos projetos sem fim, houve momentos e experiências maravilhosas. Além dos não menos importantes amigos de longa data, Lucas e Nathalia, fico muito feliz por, em algum momento, termos nos aproximado no colégio e por nossa amizade continuar até hoje, e que seja assim para sempre.

Também agradeço ao PET-Informática por todas as oportunidades de crescimento, tanto técnico quanto como pessoa, proporcionadas e pelo grupo maravilhoso que o compõe.

Agradeço aos professores do Centro de Informática, por todo o conhecimento passado por eles e, em especial, a Vinicius que me acolheu e orientou de forma a fazer esse trabalho possível, assim como Carlo, por toda a sua ajuda.

A todos os outros que fizeram parte desse trajeto direta ou indiretamente, agradeço-os com muito carinho por tudo.

Resumo

A Web, nos últimos anos, foi se tornando cada vez mais essencial na vida das pessoas, seja para fins educativos, sociais, financeiros, de entretenimento etc. Com isso, cresceu o índice de crimes cibernéticos, como ataques de phishing que visam obter informações sensíveis das vítimas, principalmente seus dados pessoais e financeiros, possibilitando fraudes eletrônicas. Estudos apontam que todos estão suscetíveis a este tipo de ataque, mas que esse índice é maior entre os usuários mais assíduos da Web e, além disso, possuir conhecimento sobre o assunto não necessariamente diminui a vulnerabilidade ao ataque. Através de um experimento usando cenários de e-mails, foi avaliada a suscetibilidade dos discentes das áreas de Tecnologia da Informação ao phishing. Os resultados se mostraram equilibrados, mas, ainda assim, favoráveis para o sucesso do phishing, sugerindo que uma grande parcela dos discentes não está atenta à segurança digital e, portanto, está suscetível a ataques de phishing.

Palavras-chave: crimes cibernéticos, phishing, Tecnologia da Informação, segurança digital, pesquisa, engenharia social

Abstract

The Web in recent years has become essential in people's lives for many purposes, be it educational, social, financial, entertainment, etc. As a result, cybercrime has grown, such as phishing attacks targeting sensitive information from victims, particularly their personal and financial data, enabling electronic fraud. Studies indicate that everyone is susceptible to this type of attack, but that this index is higher among the more assiduous users of the Web and, moreover, having knowledge on the subject does not necessarily decrease vulnerability to the attack. Through an experiment using e-mail scenarios, it was evaluated the susceptibility of the Information Technology students to phishing. The results were balanced, but still favorable to the success of phishing, suggesting that a large portion of students is not attentive to digital security and therefore susceptible to phishing attacks.

Keywords: cyber crimes, phishing, Information Technology, digital security, survey, social engineering

Sumário

Lista de Figuras

Lista de Gráficos

Lista de Tabelas

1. Introdução

1.1. Motivação

A globalização, que pode ser definida como uma intensificação das relações sociais mundiais [18], tem a Internet como aliada, interligando ainda mais as pessoas de todo o mundo em um único e imenso ambiente através do qual os meios de comunicação tem ainda mais poder. Atualmente, estatísticas apontam que em 2017, aproximadamente, 3,773 bilhões de pessoas, cerca de 50% da população mundial, tem acesso à Internet, um crescimento de 10% em relação ao ano anterior [12]. E, no Brasil, já são contabilizados, aproximadamente, 139 milhões de usuários da Web [4] [12].

No entanto, esses dois fatores, associados a alguns outros como o desenvolvimento de dispositivos móveis, aumento das redes wireless e a sociedade que, cada vez mais, necessita e depende de computadores e conectividade, tornaram-se um problema quando observado pela ótica da segurança digital.

Crimes cibernéticos (ou cibercrimes) consistem em utilizar um sistema computacional conectado à rede como meio de praticar o ato ilegal, como roubos de identidade, fraudes eletrônicas além de, entre outros, grandes ataques em massa a infraestruturas [22]. Segundo dados do CERT.br, só no Brasil, em 2016 foi reportado um total de 647.112 incidentes de segurança [15].

Um dos ataques cibernéticos mais comuns, o phishing, uma forma de engenharia social em que um atacante se passa por uma entidade de confiança da vítima para obter suas informações sensíveis [21], é um termo relativamente recente que começou a ser descrito no final da década de 1980, mas só se fixou como tática de cibercrime em 1995, com a criação da ferramenta *AOHell* [1] que possuía a função de fazer tentativas de roubo de senhas ou detalhes financeiros de usuários da AOL.

No auge, em 2016, o pior ano da história de acordo com o *Anti-Phishing Working Group* (APWG), foram reportados 1.220.523 de ataques, sendo a maioria deles voltado para os setores de varejo e financeiro [26]. Desse número, 27,61% do

total global foi reportado apenas no Brasil, país com maior número de ataques de phishing [9].

Devido a questões éticas na realização de pesquisas sobre phishing com o uso de experimentos com um grupo de pessoas, como descrito por [17], seria necessária a aprovação de um Comitê de Ética da instituição além do total consentimento dos participantes, o que poderia afetar os resultados devido ao nível de alerta deles. Em vista disso, pesquisadores tendem a optar por "*role plays*", encenações de um caso imitando a realidade, de forma que os indivíduos não participem com qualquer tipo de propensão a uma ou outra resposta devido ao conhecimento prévio da finalidade do estudo sobre phishing.

Em 2007, pesquisadores da *Carnegie Mellon University* (EUA) realizaram uma análise comportamental das pessoas frente ao risco do phishing no artigo "*Behavioral Response to Phishing Risk*" [13], visando a descobrir os fatores associados ao sucesso dos ataques de phishing através de um exercício com uma pequena encenação da realidade (*role play*). Os resultados apontaram que quanto maior o conhecimento do indivíduo sobre o contexto da Internet, como, por exemplo, a interpretação de URLs, ataques e o próprio phishing, menor sua vulnerabilidade a ele, mas que conhecimentos de informática mais gerais não estão relacionados a diminuição da probabilidade de suscetibilidade.

Com base na pesquisa anterior, em 2010, outros pesquisadores da mesma universidade, em parceria com o *Indraprastha Institute of Information Technology* (Índia), escreveram o artigo "*Who Falls for Phish? A Demographic Analysis of Phishing Susceptibility and Effectiveness of Intervention*" [31], em que é analisada a relação entre dados demográficos e a suscetibilidade e efetividade de ataques de phishing. A partir dos resultados obtidos foi possível ver que as pessoas tendem a julgar a legitimidade de sites pela aparência deles, que, assim como no anterior, o conhecimento sobre certos conceitos não reduz sua vulnerabilidade ao phishing, e boa parte dos usuários não compreendem ou confiam nos indicadores de segurança dos navegadores.

Em ambas as pesquisas, para avaliar a suscetibilidade das pessoas ao phishing, foram realizados questionários com uma encenação (*role play*) de um possível caso (o de *Pat Jones*) a ser avaliado pelos participantes. O estudo mostra

resultados para grupos de participantes genéricos, pessoas cujo conhecimento prévio sobre certos conceitos, como a Internet, Web, vulnerabilidades, phishing e sua prevenção não era uma certeza.

A relação entre conhecimento e suscetibilidade apresentada nos resultados das pesquisas citadas leva a entender que quanto maior o conhecimento, menor é a chance de se tornar uma vítima. Mas o quão imunes, de fato, estão os indivíduos que conhecem mais?

A partir desse questionamento, foi pensada a proposta de avaliar o quão suscetíveis estão as pessoas imersas no contexto tecnológico, supostamente, as que mais possuem conhecimento técnico sobre os principais conceitos que podem levar à identificação do phishing e a real identificação dele de forma a não se tornar uma vítima. Tais indivíduos fazem parte da área de Tecnologia da Informação, cuja definição é o uso de computadores, armazenamento, rede e dispositivos físicos, infraestrutura e processos para criar, processar, armazenar, proteger e trocar todas as formas de dados eletrônicos [37].

Como mostrado na definição, integrantes dessa área lidam constantemente com dados que podem variar de irrelevantes a estritamente confidenciais, como dados médicos, por exemplo. São informações manuseadas por todos os lados e de todas as formas, mas cuja segurança deve ser uma preocupação, pois ela precisa ser planejada e garantida. No entanto, essa garantia de segurança não é via de regra, tendo em vista os inúmeros casos de vazamento de informações confidenciais (*leaks*) que ocorrem através de brechas no desenvolvimento de aplicações e várias vezes através de falhas humanas através de engenharia social.

Levando em consideração a preocupação de cada pessoa dessa área com a segurança de suas próprias informações, o que podemos inferir sobre os reflexos desse comportamento pessoal no meio profissional? O quão presente está a segurança digital entre esses indivíduos?

1.2. Objetivos

1.2.1. Geral

Utilizando a abordagem utilizada na etapa de *role play* dos artigos citados na seção 1.1 e tendo em vista o resultado sobre a relação entre maior conhecimento e suscetibilidade ao phishing, este trabalho propõe um experimento mais específico, voltado para um único grupo de participantes: os discentes de graduação e pós-graduação da área de Informática do Centro de Informática da Universidade Federal de Pernambuco (UFPE). Por meio de um questionário, que avalia as ações dos indivíduos frente a casos que retratam a realidade dos ataques de phishing mais comuns, será verificado, de forma prática, o conhecimento desses alunos acerca de segurança e, portanto, sua suscetibilidade ao phishing.

1.2.2. Específico

Por meio do questionário, este trabalho tem como objetivo avaliar 4 critérios específicos a partir dos resultados do comportamento dos participantes em relação aos casos de e-mails apresentados, são eles:

- Suscetibilidade ao phishing;
- Suscetibilidade a clicar nos links segundo o curso: ciência da computação, engenharia da computação e sistema de informação, além da pós-graduação;
- Suscetibilidade a clicar nos links segundo o nível de experiência, mensurado de acordo com o período cursado pelo participante;
- Relação entre digitar ou copiar a URL e cair no phishing.

1.3. Estrutura do trabalho

Este trabalho foi dividido em 6 capítulos, incluindo este que apresenta uma introdução à pesquisa, além de seus objetivos gerais e específicos. Os próximos serão descritos abaixo:

- **Capítulo 2** - nele é apresentada a fundamentação teórica acerca dos principais conceitos utilizados neste trabalho, como crimes cibernéticos, engenharia social e phishing.

- **Capítulo 3** - neste são apresentados os trabalhos utilizados como base para o experimento realizado.

- **Capítulo 4** - apresenta a metodologia utilizada para realizar a pesquisa.

- **Capítulo 5** - mostra os resultados da pesquisa segundo as respostas fornecidas pelos participantes, avaliando-as a partir dos critérios citados na seção 1.2.2.

- **Capítulo 6** - apresenta as considerações finais deste trabalho, segundo os resultados obtidos na pesquisa, além de possíveis trabalhos futuros envolvendo o tema desta pesquisa.

2. Conceitos fundamentais

2.1. Crimes cibernéticos

O ataque começou em maio de 2017. Milhares de sistemas ao redor do mundo foram infectados em questão de horas: do Serviço Nacional de Saúde (*National Health Service* - NHS) do Reino Unido a empresas de telecomunicações, bancos, etc. Mais de 200.000 sistemas em 150 países com seus dados sequestrados e apenas um aviso de resgate (*ransom*) para liberá-los.

O maior ataque cibernético dos últimos anos ficou conhecido por WannaCry, uma exploração de uma vulnerabilidade, conhecida como *EternalBlue*, na implementação do protocolo *Server Message Block* (SMB) que provê acesso compartilhado entre computadores, em sistemas com o sistema operacional Windows. Vulnerabilidade essa que fora descoberta e utilizada pela Agência de Segurança Nacional (NSA) dos EUA, mas não reportada para a Microsoft, que só a descobriu após um vazamento de informações e logo providenciou uma correção, através do *patch* MS17-010 lançado em março de 2017.

No entanto, aproveitando-se do fato de que muitos usuários Windows não haviam instalado o *patch* e que explorar o *EternalBlue* continuava possível, o ataque se propagou rapidamente através de um ataque de *ransonware*, em que um sistema é bloqueado até que um resgate seja pago, um dos inúmeros tipos da mais promissora área criminal da atualidade: a de crimes cibernéticos.

De acordo com Halder e Jaishankar [19], crimes cibernéticos (ou cibercrimes) podem ser definidos como ofensas cometidas contra indivíduos ou grupos de indivíduos com o intúito de, intencionalmente, ferir a reputação da vítima, causar-lhe dano físico ou mental, ou, direta ou indiretamente, qualquer tipo de perda, através do uso da rede de telecomunicações.

CEO (*Chief Executive Officer*) da IBM, multinacional americana de tecnologia, Ginni Rometty, em 2015, disse [20]:

> Nós acreditamos que os dados são o fenômeno do nosso tempo. É o novo recurso natural do mundo. É a nova base da vantagem competitiva e está transformando todas as profissões e a indústria. Se tudo isso for verdade, mesmo que inevitável, crimes cibernéticos, por definição, é a maior ameaça a todas as profissões, todas as indústrias, todas as companhias do mundo.

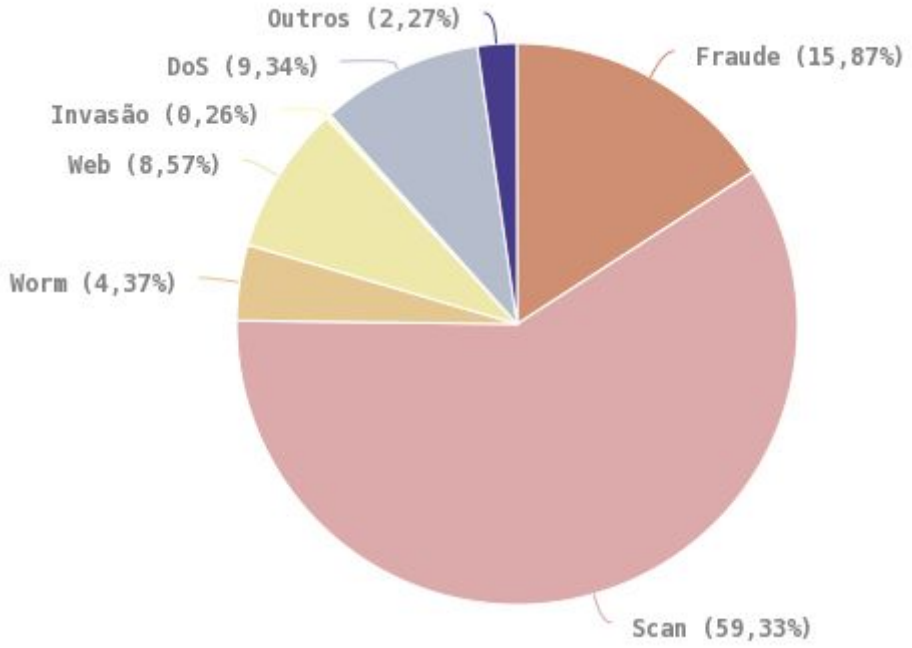
Os primeiros casos de crimes cibernéticos começaram a surgir por volta da década de 1960, tendo como principais alvos as instituições financeiras. Casos mais notórios só surgiram na década seguinte quando, em 1971, John Draper descobriu que um apito, que vinha de brinde em uma caixa de cereal, reproduzia o tom usado para acessar o satélite para ligações de longa distância e, assim, conseguiu fazer ligações gratuitas. Outro caso foi o de Ian Murphy, primeira pessoa a ser condenada por um cibercrime em 1981 por conseguir hackear a rede AT&T, a maior empresa de telecomunicações do mundo, mudando o relógio interno do sistema e alterando as tarifas que variavam de acordo com o horário [38].

Mas foi no final da década de 1980 que surgiram os primeiros grandes ataques: a tentativa de roubo de 70 milhões de dólares do *First National Bank of Chicago* através de uma transferência de fundos para a Áustria; a primeira grande infecção por um *ransomware* foi reportada quando o vírus *AIDS* infectou vítimas através de um quiz, cobrando 500 dólares pelo resgate do computador; e, na mesma época, um grupo foi pego roubando informações do governo americano e repassando para a KGB russa [35] [38].

À medida que a Internet evoluía, junto a ela evoluíram também as estratégias e as técnicas, o conhecimento passou a se propagar com mais velocidade e fronteiras foram diminuindo. Na década de 1990, os prejuízos causados por crimes cibernéticos foram aumentando cada vez mais, como o roubo de 10 milhões de dólares do Citibank em 1994; a alteração dos websites de órgãos como o Departamento de Justiça e Força Aérea americanos, FBI e CIA em 1996; e o maior ataque por *worm* (um tipo de malware que se replica, espalhando-se por outros sistemas), o Melissa, que causou prejuízos de aproximadamente 80 milhões de dólares, além de muitos outros. Segundo estatísticas, o prejuízo dos crimes cibernéticos chegarão a 2 trilhões de dólares em 2019 [2].

Na Figura 1, são mostradas os números de incidentes virtuais do ano de 2016 no Brasil, de um total de 647.112 incidentes relatados ao CERT.br (Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança) [7].

Figura 1: Incidentes reportados ao CERT.br de janeiro a dezembro de 2016.



Fonte: CERT.br

Os incidentes apresentados na Figura 1 tem como maioria o ataque do tipo scan, que é uma forma automatizada de obter informações da rede a partir de checagens de computadores e serviços ativos nela. Em segundo lugar estão as fraudes, modalidade onde podem ser inseridos ataques de phishing que serão descritos na seção 2.3. Os outros ataques têm como principais objetivos ataques mais diretos à aplicações e serviços, como é o caso das invasões e negação de serviço - *DoS* (*Denial of Service*).

A comunidade online OWASP (Open Web Application Security Project ou Projeto Aberto de Segurança em Aplicações Web), que produz conteúdo gratuito referente a segurança de aplicações Web, divulgou seu *Top* 10 dos maiores riscos de segurança desse tipo de aplicação para o ano de 2017 [25].

Segundo o relatório, os três principais riscos são: injeção, autenticação quebrada e gerenciamento de sessão e exposição de dados sensíveis. Em primeiro

lugar está uma vulnerabilidade que ocorre quando se é possível inserir um dado na aplicação de forma a conseguir acesso a informações as quais não deveria ter acesso. Em segundo ficou a vulnerabilidade que ocorre quando há a possibilidade de comprometimento de senhas ou de identificadores de sessão, cuja obtenção pode ocorrer de forma manual, através de ferramentas e até através engenharia social, como o phishing (Seções 2.2 e 2.3), permitindo a exploração da aplicação. Em terceiro está a exposição de dados sensíveis, que ocorre quando a aplicação não protege corretamente dados sensíveis, como informações sobre cartão de crédito ou credenciais de acesso, de serem obtidos por atacantes.

Assinado em 2001, a Convenção sobre Cibercrime, primeiro tratado internacional na busca por crimes cibernéticos numa cooperação entre nações, distingue, em seu código, esses crimes em 4 tipos de ofensas [36]:

- contra a Segurança da Informação, ou seja, integridade, confidencialidade e disponibilidade de sistemas ou dados [1];
- relacionadas a computadores, como fraudes [2];
- relacionadas ao conteúdo, como, por exemplo, pornografia infantil [3];
- relacionadas aos direitos autorais [4].

Um ano antes, em 2000, Bruce Schneier [30], um especialista da área de segurança e criptografia, descreveu as ondas de ataques cibernéticos. A primeira estava relacionada à ataques físicos, diretamente à computadores, fios e eletrônicos. O que foi abrandado pela Internet que, justamente, se defendia desse tipo de ataque físico.

Ao longo dos anos seguintes, foi se concretizando a segunda onda, a de ataques sintáticos, nos quais o foco estava na lógica operacional dos computadores e da rede. Sendo assim, o alvo eram as vulnerabilidades dos softwares, das criptografias utilizadas, dos protocolos, etc.

Foi então que surgiu a terceira onda, a de ataques semânticos, que não mais explora falhas de hardwares ou softwares, mas sim da forma como os próprios

[1] Art. 2 (Illegal access), Art. 3 (Illegal interception), Art. 4 (Data interference), Art. 5 (System interference), Art. 6 (Misuse of devices).
[2] Art. 7 (Computer-related forgery), Art. 8 (Computer-related fraud)
[3] Art. 9 (Offences related to child pornography)
[4] Art. 10 (Offences related to infringements of copyright and related rights)

humanos lidam com o conteúdo ao qual são expostos. Como, por exemplo, a credibilidade que damos ao que lemos, pois raramente temos a visão de ir em busca da confirmação daquilo, já levamos como verdade desde o primeiro momento.

É essa ingenuidade por trás da credulidade que alguns indivíduos usam para explorar outros. É aproveitar a forma como lidamos com *inputs* e nossa capacidade de raciocinar sobre eles.

2.2. Engenharia social

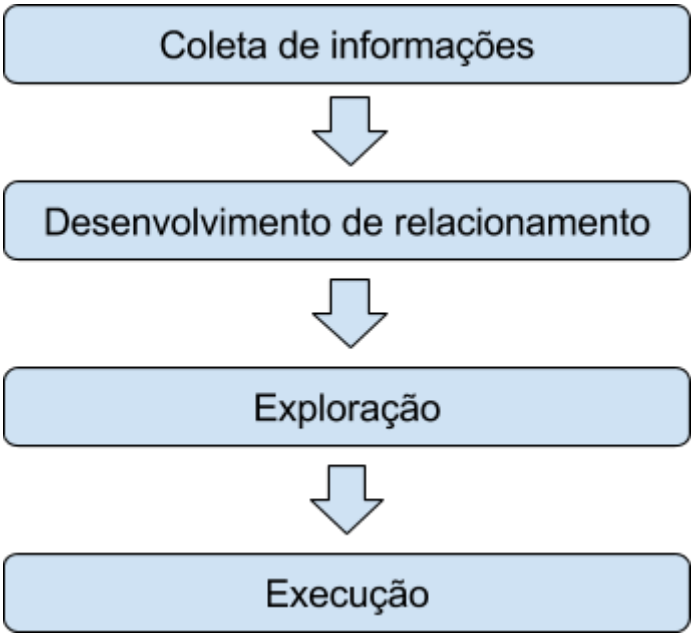
No contexto de segurança da informação, o termo “engenharia social” se refere à manipulação psicológica da tendência humana natural de confiar [34] ou ainda qualquer estratégia não-técnica para se aproveitar dos aspectos humanos conhecidos como “os sete pecados capitais”: curiosidade, cortesia, credulidade, ganância, irreflexão, timidez e apatia [39].

O principal objetivo do ataque é o de ganhar acesso a um sistema ou a informações de forma a cometer fraudes, invasões da rede, espionagem industrial, roubo de identidade ou até uma perturbação a um sistema ou rede internos [34]. E, por não envolver diretamente nenhum aspecto técnico que possa ser reconhecido por ferramentas de segurança tradicionais, os ataques de engenharia social estão entre as maiores ameaças atualmente.

A empresa Verizon, multinacional de telecomunicações, em 2016, estudou 42.068 de incidentes de segurança reportados a ela e, do total, 1.935 resultaram em vazamento de informação, apontando como causa de 43% desse número ataques de engenharia social [33].

Apesar das diversas técnicas existentes, que serão citadas a seguir, e das diferentes formas de aproximação de cada uma, estudiosos observaram um padrão no ataque, dividido-o em 4 fases [3] [23], são elas:

Figura 2: Fases do ataque de engenharia social.



Fonte: The Attack Cycle [3]

Na coleta de informações, considerada a mais custosa, mas mais importante fase para a eficácia do ataque, é necessário um bom engajamento na pesquisa, que pode ser restringida segundo os objetivos do atacante. Para facilitar a obtenção dos dados online, geralmente são usadas ferramentas, mas também podem ser usadas outras formas de aproximação, inclusive física, a fim de extrair o máximo de informação.

Essa aproximação pode, inclusive, ser caracterizada como da fase seguinte, a de desenvolver um relacionamento. Nesta fase é onde o atacante começa a perceber o nível de cooperação da vítima, o quanto ela fornece ou não informações.

Depois, na fase de exploração, o objetivo é fortalecer a relação de forma a ganhar mais e mais confiança da vítima para que a execução, de fato, ocorra na próxima fase sem problemas. Então, o ciclo chega ao fim na quarta fase (execução) na qual o atacante deve garantir que acabe da forma mais suave possível, sem que a vítima questione o acontecido e sem deixar “fios soltos” para que não haja formas de rastreamento.

Os tipos mais comuns de ataques de engenharia social são [29]:

- *Baiting* - Por meio de um dispositivo infectado por um *malware*, um software malicioso, é explorada a curiosidade do indivíduo. O sucesso desse ataque

depende de três ações da vítima: encontrar o dispositivo, abrir o conteúdo e instalar o *malware* sem perceber, fazendo com que o atacante obtenha acesso ao sistema desejado.

- *Pretexting* - Através de informações falsas sobre determinadas circunstâncias, um atacante entra em contato com a vítima, após pesquisas de background online, e se passa por uma pessoa de confiança para confirmar dados e obter credenciais.
- *Quid pro quo* - Termo que significa “isso por aquilo”, neste ataque é dado algum tipo de oferta à vítima em troca de informações sensíveis. Uma forma de abordagem é oferecer brindes ao final de pesquisas de campos nas quais são pedidas informações sensíveis do participante.
- *Tailgating* - Essa se trata de uma técnica física quando um atacante não autorizado segue a vítima até uma determinada localização para obter acesso a uma área com informações confidenciais ou ativos valiosos. Um exemplo disso é fazer uso de dispositivos emprestados para infectá-los.

Além desses, existe outro tipo, ainda mais comum e foco deste trabalho, que será descrito na próxima seção.

2.3. Phishing

O termo “phishing” teve sua primeira menção registrada por volta da metade da década de 1990, em grupos online da *America-online Usenet*. Inicialmente, a aproximação com a vítima se dava através de mensagens instantâneas no AIM (*AOL Instant Messenger*) em que o atacante, precisando de informações legítimas, se passava por um funcionário da AOL e pedia a senha da vítima. Logo depois, para facilitar o processo, surgiram ferramentas como a *AOHell* [1], cuja função era fazer tentativas de roubo de senhas ou detalhes financeiros dos usuários da plataforma de forma que o processo fosse automatizado.

A técnica, no entanto, anos antes em 1987, havia sido, pela primeira vez, descrita no artigo “*System Security: A Hacker's Perspective*”, apresentado na *International HP Users Group*, Interex [16], no qual foi discutido um método feito por terceiros para imitar um serviço confiável.

Uma mistura da palavra em inglês “*fishing*”’, que significa pescar, com o termo “*phreak*”, do inglês “*freak*” que significa aberração, usado na época para nomear os primeiros hackers de telefonia, como o citado John Draper, o termo “phishing”, um exemplo de técnica de engenharia social, pode ser tido como qualquer tipo de golpe que faz uso da tecnologia para obter informações sensíveis da vítima [21] [24], com as finalidades de roubo, extorsão, sabotagem, espionagem ou até múltiplos objetivos combinados [5].

O phishing pode ser executado de diversas formas, que inclui e-mail, VOIP, SMS, mensagens instantâneas, redes sociais ou até jogos multiplayer, mas, essencialmente, pode ser divididos em dois tipos. O **phishing tradicional**, termo que faz alusão a “pescar com rede”, está mais relacionado a um ataque massivo, como, por exemplo, o envio de e-mails, cujo baixo esforço proporciona facilidade para mandar milhares, e qualquer retorno de pessoas afetadas já é uma vantagem [5].

O outro tipo, o ***spear* phishing**, do inglês lança ou arpão, apresenta um objetivo mais específico e direcionado. Nele faz-se o uso de técnicas mais elaboradas, como uma pesquisa de *background*, a fim de atingir o alvo da forma mais eficaz e convincente possível [5].

Segundo o PhishTank, uma plataforma colaborativa que reúne dados sobre phishing, são características a serem observadas em e-mails de phishing [28]:

- Cumprimento genérico - como, geralmente, o ataque é em grande escala, não vale a pena usar detalhes específicos como nomes próprios;
- Links forjados - nem sempre o link escrito no corpo do e-mail corresponde ao que ele realmente está apontando. Além disso, deve-se observar sempre se o protocolo utilizado é o HTTPS na hora de inserir dados pessoais, pois ele garante a segurança dos dados ao encriptá-los, ao contrário do HTTP;
- Pedidos por informações pessoais - dado que o objetivo principal do phishing é obter tais dados, deve-se sempre ficar atento a esses pedidos;

- Urgência - como não é do interesse do atacante esperar, ele faz com que a vítima aja o mais rápido possível ao dar um tom de urgência no pedido.

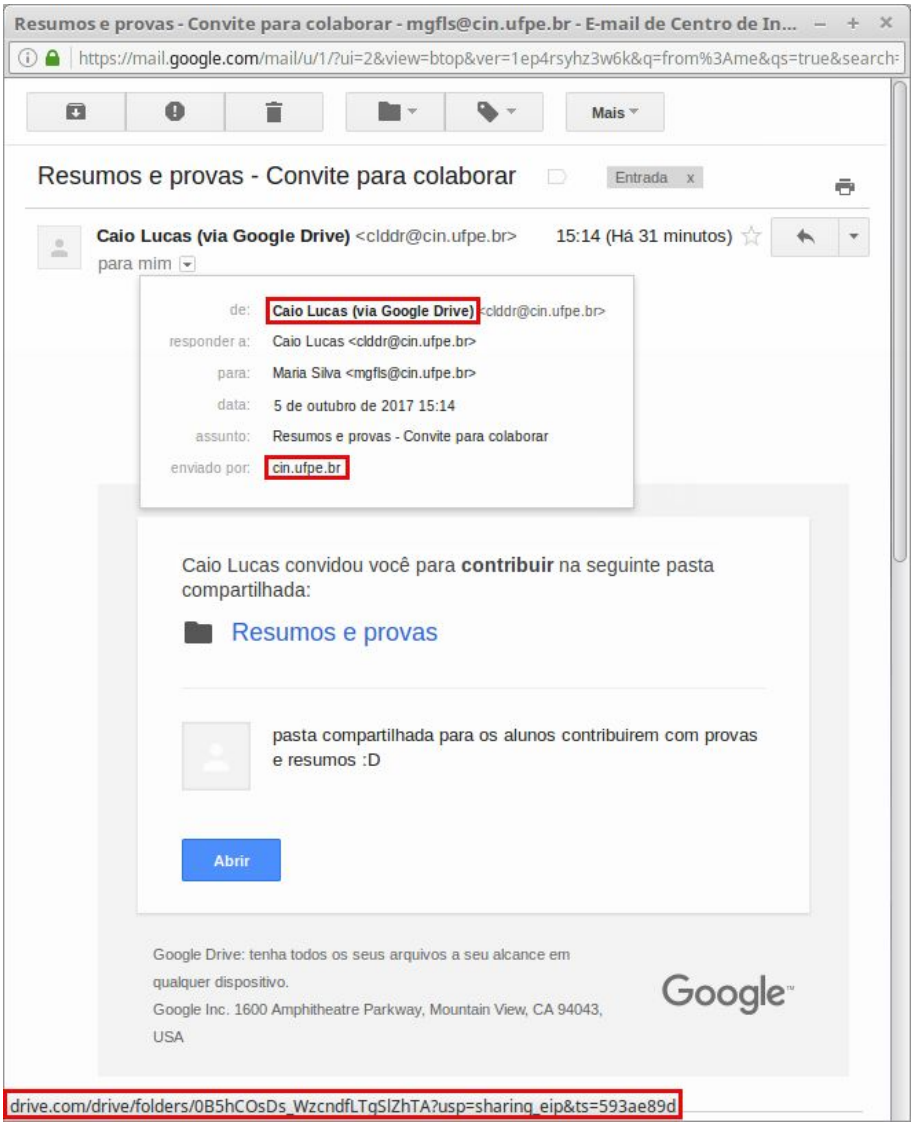
Essas características funcionam pois, ao contrário da exploração de vulnerabilidades computacionais, como *bugs* ou brechas na implementação de softwares, o phishing explora as falhas humanas dos usuários da Internet. No artigo “Why Phishing Works” [11] foram analisados relatórios sobre phishing mantidos pelo *Anti Phishing Working Group* (APWG), organização que se dedica à prevenção, detecção, combate e monitoramento do Phishing [6]. Nele, os autores chegaram às principais estratégias de exploração usadas pelos atacantes ao longo dos anos separadas em 3 dimensões:

- Falta de conhecimento;
- Ilusão de ótica;
- Falta de atenção.

A falta de conhecimento implica que a vítima não sabe alguns conceitos determinantes do ataque e, portanto, pode não distinguir as diferenças entre o que é verdadeiro ou falso. Já a ilusão de ótica, que também pode ser associada a falta de conhecimento, considerando uma pessoa que entenda um pouco mais sobre o assunto ou até uma pessoa que entende de verdade, torna o falso tão parecido com o verdadeiro que a diferença é quase imperceptível. Já a falta de atenção é para os detalhes sutis, como a falta de uma letra no texto que, se o indivíduo não estiver atento, deixa passar com facilidade.

Na Figura 3, exemplo de e-mail de phishing utilizado nesta pesquisa com e-mails e nomes fictícios, podemos observar algumas estratégias utilizadas. Nele, um e-mail de compartilhamento de uma pasta do *Google Drive*, vemos que o domínio usado para envio do e-mail foi o da própria instituição de ensino, mas o remetente indica “via Google Drive”, ou seja, o compartilhamento, que deveria partir do *Google Drive*, não veio dele, podendo indicar que o corpo do e-mail é uma cópia do original. Além disso, o link “*http://drive.com”* para abrir a página não corresponde ao original “*https://drive.google.com”*, mas ambos são bastante similares, apelando para a falta de atenção da vítima.

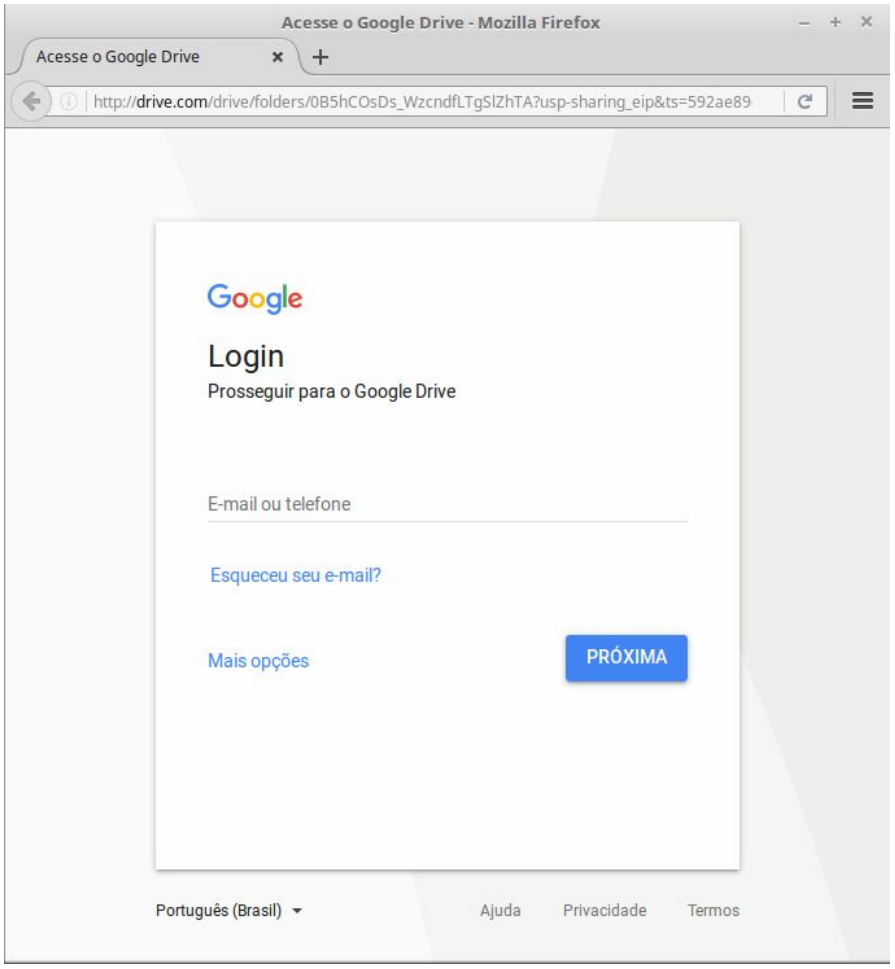
Figura 3: Exemplo de e-mail de phishing utilizado na pesquisa.



Fonte: Simone Cohen (2017)

Ou seja, ao acessar o link do e-mail, o indivíduo seria direcionado a uma página falsa, uma réplica o mais idêntica possível à original, e nela, como mostrado na Figura 4, seria dada a opção de *login*, fazendo, então, com que a vítima digitasse seus dados, sendo fisgada pelo phishing. Note que, para uma pessoa com mais conhecimento, a falta da verificação de segurança através do certificado digital - simbolizada por um cadeado, geralmente, junto à URL no *browser* - seria um alerta sobre a falsidade da página, além da utilização do protocolo HTTP.

Figura 4: Página redirecionada do link do e-mail de phishing utilizado na pesquisa.

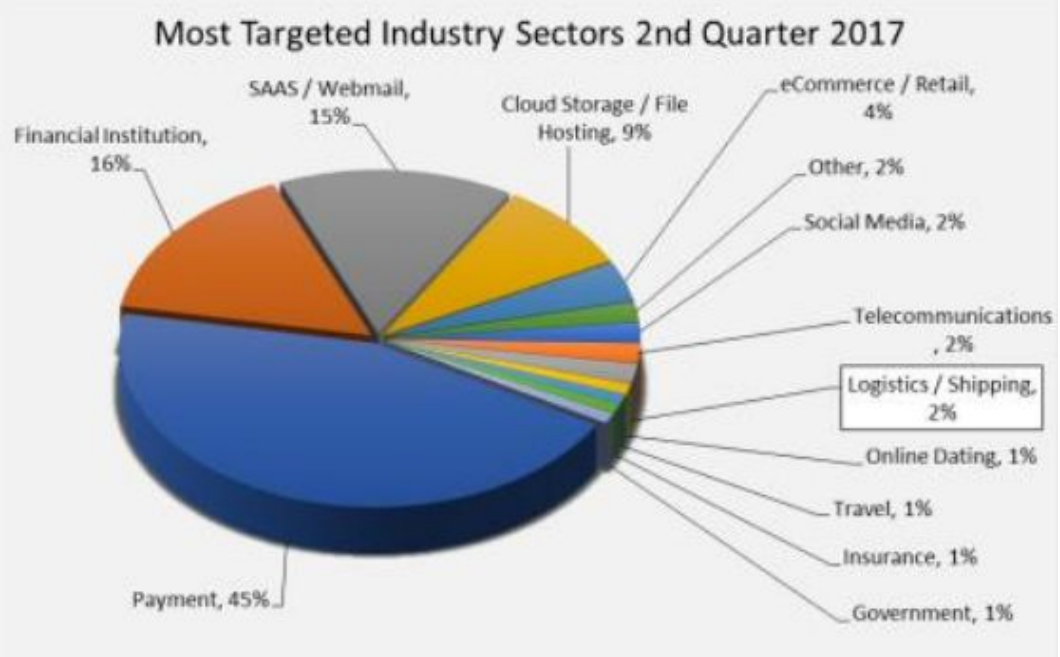


Fonte: Simone Cohen (2017)

São vários os objetivos por trás do phishing, mas os principais deles têm o teor de fraude, seja por meio do roubo de informações, sabotagens, extorsão (casos similares ao do *ransomware* WannaCry), espionagem, etc.

A APWG, em seu relatório sobre o primeiro semestre de 2017 [27], divulgou dados sobre os setores da indústria mais afetados por ataques de phishing e mais de 50% do total estava relacionado ao setor financeiro, como mostrado na Figura 5.

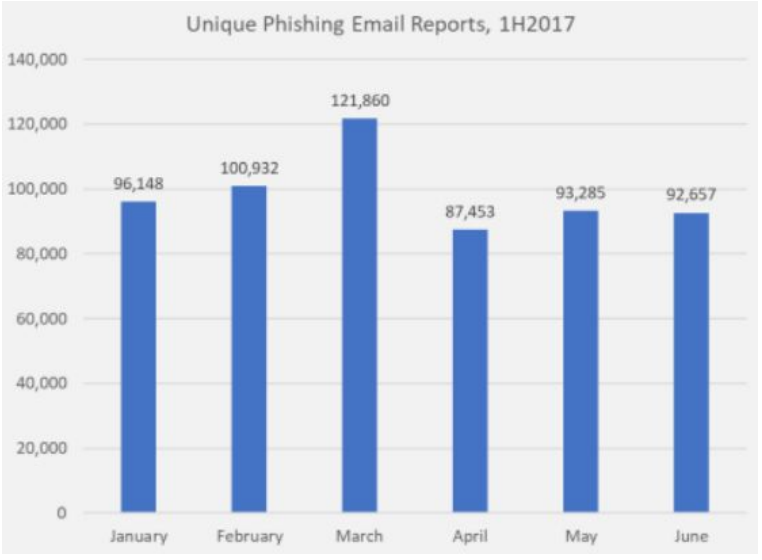
Figura 5: Setores da indústria afetados por ataques de phishing.



Fonte: APWG Phishing Attack Trends Reports 1H 2017 [27].

O mesmo relatório também mostra números altos de casos reportados de janeiro a junho, totalizando cerca de 590.000 incidentes reportados, como pode ser observado na Figura 6. Após ela, na Figura 7, temos os números relativos aos websites usados para phishing.

Figura 6: Incidentes de phishing por e-mail em números.



Fonte: APWG Phishing Attack Trends Reports 1H 2017 [27]

Figura 7: Websites de phishing reportados.

Fonte: APWG Phishing Attack Trends Reports 1H 2017 [27]

Na análise sobre os domínios chamados de *country-code top-level domains* (ccTLDs), ou seja, os domínios da Internet referentes aos países (.br), o Brasil aparece entre os mais usados, ficando em segundo lugar. Assim como, em outro relatório do primeiro quarto de 2017 da *Kaspersky Lab* [10], o Brasil aparece em segundo lugar na quantidade de usuários vítimas, tendo ficado em primeiro no relatório referente ao ano de 2016.

2.3.1. Modalidades do ataque

Nesta seção serão apresentados as principais modalidades do phishing, dos mais simples, que depende apenas de convencer a vítima, aos mais complexos que utilizam softwares maliciosos para o atacante conseguir o que deseja [5] [8], sendo possível a combinação dessas modalidades na realização de um ataque.

2.3.1.1. Fraude de antecipação de recursos (*Advance fee fraud*)

Nesse tipo de ataque, a vítima é induzida pelo atacante por meio de algum enredo a fornecer dados ou a realizar pagamentos adiantados com a promessa de receber uma recompensa futura. Um dos tipos desse tipo de fraude é o chamado

Golpe Nigeriano no qual a vítima recebe um e-mail com a história de um representante de uma família, de um país distante, que encontra-se em dificuldade de tirar seus bens do país e, para isso, seria necessário o envio de uma quantia para que a documentação fosse resolvida. A recompensa seria uma porcentagem da fortuna da família assim que o dinheiro fosse transferido para a conta da vítima.

2.3.1.2. Pharming

Nesse tipo de ataque, a vítima tem sua navegação redirecionada, por meio de DNS (*Domain Name System*)[5], de forma que, ao tentar acessar sites verdadeiros, ocorra um redirecionamento para sites fraudulentos muito similares, sem que isso seja percebido pela vítima.

2.3.1.3. Whaling

Semelhante ao Golpe Nigeriano, este ataque de *spear phishing* é voltado para grandes empresas com o objetivo de conseguir informações ou até transferências de fundos por meio de funcionários. O atacante se passa por um executivo que faz um pedido urgente e confidencial a um dos funcionários, passando-lhe alguns detalhes internos que torne a situação mais real e fazendo com que a ordem seja cumprida.

2.3.1.4. Atendente impostor

Nesse ataque, o atacante entra em contato com a vítima se passando por atendentes de uma dada empresa com o objetivo de conseguir informações privilegiadas. O golpe pode acontecer por meio de e-mail, no qual, por exemplo, a vítima é informada de algum problema em sua conta pessoal na empresa e precisa realizar uma ação para resolver o problema, como acessar um site para trocar sua senha; ou ainda por telefone para resolver, por exemplo, problemas técnicos de Internet ou até sobre contas bancárias e cartão de crédito.

---

[5] DNS: Sistema que associa informações atribuídas a nomes de domínios a cada entidade participante, como, por exemplo, a tradução de nomes de domínio (URL) ao seu endereço IP correspondente.

2.3.1.5. Malware

Malwares são softwares maliciosos que podem surgir com diversos propósitos, entre eles: *keyloggers*, que captura ações no teclado da vítima; *screenloggers*, que captura a tela do usuário, mantendo um registro do que foi aberto nela em um período de tempo; *ransomware*, como o *WannaCry*, que bloqueou computadores em troca de um resgate em dinheiro; APTs (*Advanced Persistent Threat* ou Ameaça Persistente Avançada) que tem o objetivo ficar no sistema da vítima pelo maior tempo possível capturando informações e as repassando para o atacante; entre outros.

2.3.2. Prevenção

O phishing nada mais é do que uma forma de se aproveitar das ações humanas, então, ao entrar no mundo virtual, é preciso se conscientizar e até aprender certos conceitos sobre esse meio de forma a não se tornar uma vítima de ataques. São vários os cuidados que devem ser tomados, entre eles os principais são [5] [8]:

- Verificar o remetente dos e-mails - não somente se o e-mail é familiar, mas também verificando a escrita, se o domínio de envio está correto ou se ele corresponde com o e-mail de quem o enviou;
- Verificar o link - pode acontecer de o link mostrado no corpo do e-mail não corresponder ao qual ele está direcionando o usuário, então, é recomendado digitar a URL direto no navegador;
- Nunca passar informações pessoais por e-mail - empresas nunca pedem dados pessoais dos clientes, então, caso seja pedido, é recomendado entrar em contato direto com a empresa através de outro meio de comunicação;
- Desconfiar da urgência em e-mails e SMS - a brevidade de tempo que o usuário tem para resolver um certo problema ou receber um prêmio,

por exemplo, pode fazê-lo agir sem pensar direito, então, antes de tomar qualquer atitude, o ideal é checar a veracidade daquilo que está sendo dito;

- Checar as regras de privacidade nas redes sociais - uma forma de conseguir informações sobre uma vítima é a partir das informações que ela própria coloca em suas redes sociais. Portanto, é preciso verificar a exposição dessas informações para que estranhos não tenham permissão de visualizá-las, assim como avaliar o que se diz mesmo que em um círculo fechado de conhecidos;
- Desconfiar de mensagens de texto - o phishing também pode ocorrer via SMS, *WhatsApp* ou outros serviços de mensagens instantâneas, então é importante validar a informação através de outras fontes e não clicar diretamente em links ou baixar aplicativos.

2.4. Considerações finais

Segundo um relatório da Sophos de 2016, companhia inglesa de segurança de software e hardware, consumidores da Internet temem mais os ataques cibernéticos que os ataques físicos. A pesquisa foi realizada com a participação de pessoas de 5 diferentes países sobre seus maiores medos em relação a segurança e os resultados mostraram que 63% deles estão mais preocupados com perdas financeiras causadas por vazamentos de dados, em contraste com 46% que se preocupa com assaltos ou roubos de carro [14].

O vice-presidente do grupo Sophos, John Shaw, observou:

> As pessoas entendem como proteger sua casa ou seu carro - elas sentem que o mundo físico está acobertado. Enquanto que cibercriminosos são invisíveis e o mundo do crime virtual é imprevisível e complicado, especialmente quando se trata de ameaças cibernéticas como phishing e *ransonware* [...]

E isso pode ser relacionado ao conhecimento do indivíduo sobre os ambientes em que habita. As regras e riscos do mundo real são mais palpáveis, podemos, por exemplo, acompanhar noticiários, atentando para informações locais

sobre segurança pública e tomar conhecimento dos riscos. Ao contrário do mundo virtual onde, como dito por Shaw, os criminosos são invisíveis, podem surgir de qualquer lugar e realizar feitos sem deixar rastros. Ao mesmo tempo que um crime cibernético ganha notoriedade e passa a ser mais observado, outro já está em andamento e se aproveita tanto de novas oportunidades quanto de resquícios do primeiro, tornando muito complicado prever um comportamento dos ataques de forma a impedi-los de acontecer.

Procurar conhecer e entender o mundo virtual é um caminho difícil quando o indivíduo não faz parte do meio tecnológico e apenas o usufrui. Mas, para as pessoas que estão imersas nesse mundo, que têm interesse no assunto e que o conhecem e entendem, quão menos suscetíveis elas estão ao crime cibernético? E, restringindo o escopo e levando em consideração o quão comum e abrangente é o phishing, essas pessoas prestam atenção a ele a ponto de não se tornarem vítimas?

Esses questionamentos serviram de base para este trabalho que busca compreender o nível de cuidado dos indivíduos imersos na área de Tecnologia da Informação com seus dados, a partir de um experimento, com casos de phishing sob o contexto deles, cuja fonte de inspiração partiu dos artigos citados na seção seguinte onde são apresentados os trabalhos relacionados.

3. Trabalhos relacionados

Em 2007, no artigo “Behavioral Response to Phishing Risk” [13], Downs et al realizou uma pesquisa piloto, em menor escala, que, mais tarde, seria trabalhada de forma mais extensiva, visando a analisar o comportamento dos indivíduos frente ao risco de um phishing. A proximidade com a realidade do comportamento dos indivíduos ao enfrentar casos fictícios ajudam a compreender melhor a forma como as pessoas agem com o phishing e, com isso, é possível desenvolver com mais eficácia ferramentas de prevenção que já prevêem certas características do phishing e o comportamento do indivíduo.

Como não é possível, por questões éticas, realizar um experimento de phishing propriamente dito, a pesquisa se dá por meio de um questionário online com encenações de casos reais em que os respondentes avaliam as opções com possíveis ações a serem tomadas. Para isso foram recrutados participantes, todos membros da comunidade da *Carnegie Mellon University* (EUA), de funcionários a estudantes, registrados em um grupo com a possibilidade de concorrer a prêmios.

No questionário, os participantes deveriam se colocar (*role play*) no lugar de *Pat Jones*, uma pessoa fictícia que trabalha numa empresa chamada *Cognix*, e observar imagens de 5 e-mails na caixa de mensagens dela, cada uma contendo um pequeno contexto para que o participante pudesse julgar melhor sua atitude em relação àqueles e-mails. Na Figura 8, retirada do artigo, são mostradas as características relevantes de cada e-mail usado no questionário.

Figura 8: Características relevantes dos e-mails usados na pesquisa.

Email	Legitimacy	Relevant features of email and sites
Cognix	real	•regarding work details •link in email: www.cognix.com •URL in status bar: http://www.cognix.com
NASA	real	•sender is known person •addressed to user •link in email: "this" •URL: antwrp.gsfc.nasa.gov/apod /astropix.html
eBay	real	•registered name "Pat Jones" displayed •link in email: "PAY [Click to confirm…]" •URL: https://payments.ebay.com/ws/eBay ISAPI.dll?item=6600378513
PayPal	phishing	•urgent request •lock image in body of web page •link: "Click here to activate your account" •URL: http://payaccount.me.uk/cgi-bin/ webscr.htm?cmd=_login-run
laptop	spear phishing	•generic message about eBay item •link: www.set-ltd.net •URL: www.set-ltd.net

Fonte: Behavioral Response to Phishing Risk, Downs et al [13]

A pesquisa foi apresentada como relativa ao uso do computador, em vez de falar sobre segurança, para não deixar os participantes tão alertas para a finalidade dela. E foi dividida em várias seções: *role play* de e e-mails no qual os participantes avaliavam imagens de e-mails e *websites*, uma avaliação de URLs (*Uniform Resource Locator*) quanto a suas características, uma seção sobre os conhecimentos dos participantes em relação a termos e ícones referentes à Internet, e uma avaliação sobre as consequências negativas do phishing.

Para cada um dos casos de e-mail foram apresentadas 7 opções de resposta: responder por e-mail, contactar o remetente por telefone ou pessoalmente, deletar o e-mail, salvar o e-mail, clicar no link, copiar o link e colar no navegador, ou digitar a URL no navegador, assim como poderiam optar por não responder ou marcar "outro" como resposta e detalhar melhor suas ações num campo de texto. Era permitido que marcassem mais de uma opção e, caso uma delas envolvesse clicar no link, o participante seria direcionado para uma imagem da página web correspondente ao link. Nessa etapa, eram dadas 6 opções: clicar em um ou mais links da página,

entrar com os dados pedidos na página, salvar a página como favorita, salvar ou arquivar a página, visitar uma página relacionada, ou deixar o website, além de poderem não responder ou marcar a opção “outro”.

Depois, na segunda parte do questionário, os participantes foram indagados sobre sua forma de avaliar URLs apenas ao olhar para elas, sem acessar o link, para dizerem, por exemplo, se conseguiriam identificar a qual empresa àquele site pertencia, se o site era seguro ou até se não fosse possível saber se era seguro ou não.

Em seguida, vieram questões sobre alguns termos, como *cookie*, *spyware*, *vírus* e *phishing*; e sobre alguns ícones presentes nos navegadores, como o cadeado de indicação de verificação de segurança. A partir de uma lista, havia apenas uma definição correta para cada um dos termos, como, por exemplo, para phishing havia: “E-mail que tenta enganá-lo para que forneça informações sensíveis para ladrões”.

E, por último, perguntas relativas a experiências passadas e consequências negativas de um ataque malicioso, como, por exemplo, o roubo de informações financeiras de forma que o indivíduo pudesse ter perdido dinheiro e bens sem que houvesse forma de recuperá-los, ou se o computador do indivíduo envia automaticamente softwares maliciosos para todas as pessoas no seu livro de endereços online.

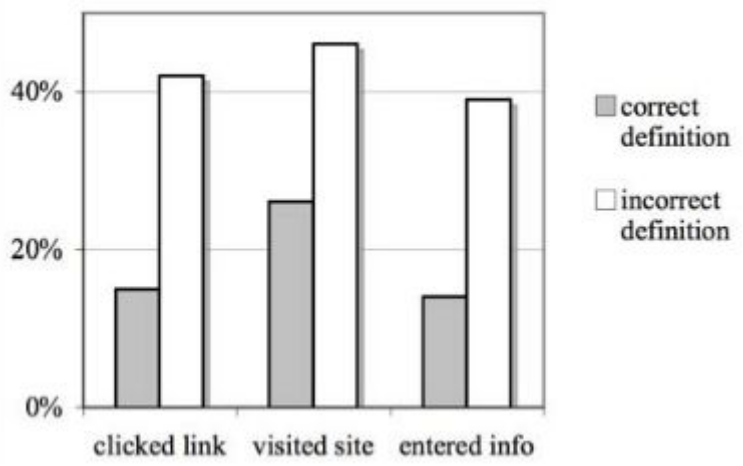
Os resultados mostraram que uma minoria dos participantes haviam enfrentado problemas que poderiam ser causados por phishing, mas que, não necessariamente, ocorreu através dele, como terem dados de cartão de crédito roubados (21%), informações roubadas ou comprometidas (14%) ou até roubo de identidade (3%).

Em relação ao *role play*, foi atestado que os participantes o levaram a sério e a maioria “respondeu“ aos e-mails de uma forma muito similar a como teria respondido um que chegasse para ele próprio. Além disso, foi analisada a frequência dos cliques, quando o participante clicava no link ou digitava sua URL no navegador, mostrando que eles tinham a tendência a acessarem sites com temas similares. Se o participante acessasse o primeiro site do tema financeiro, como o do eBay, ele tinha a tendência de também acessar o do PayPal. Em contrapartida, a avaliação de

cliques do e-mail que apresentava o spear phishing não mostrou nenhum padrão claro em relação aos outros e-mails, mostrando-se um dado não muito confiável e não sendo, portanto, amplamente usado para os fins da pesquisa.

Além disso, foi verificado que os participantes que responderam corretamente a questão conceitual sobre phishing tinham menor probabilidade de caírem no no ataque, seja por meio do clique, visitando o site ou digitarem suas informações nos sites, como pode ser visto na Figura 9. No entanto, conhecer outros conceitos não tinha relação direta com essas 3 ações. Também foi observada a correlação entre o resultado da etapa de avaliação de URLs com o comportamento do participante no *role play,* mostrando que, de fato, as pessoas que julgavam URLs inseguras tinham menos propensão a clicarem nos links.

Figura 9: Comportamento dos participantes quanto às suas respostas sobre a definição de phishing.



Fonte: Behavioral Response to Phishing Risk, Downs et al [13]

Em 2010, tendo como base a pesquisa citada anteriormente, foi realizada outra por Sheng et al [31] com o viés de uma análise demográfica da suscetibilidade ao phishing e a efetividade de uma intervenção. Assim, com participantes recrutados a partir de um site que fornecem inteligência humana para trabalhos que a necessitam, foi realizada uma pesquisa no mesmo molde da citada anteriormente, mas que os dividia em 2 grupos: o primeiro que responderia ao *role play*, com perguntas para avaliar experiências passadas e conhecimento prévio sobre phishing,

e depois passaria por um treinamento; e o segundo que passaria pelo processo na ordem contrária, avaliando assim a eficácia do treinamento anti-phishing.

Assim como no primeiro artigo, foram apresentadas imagens com 14 casos de e-mails, entre eles os mostrados na Figura 10, e opções similares de resposta, também levando os participantes a páginas web caso fosse marcada a opção de “clicar no link”.

Figura 10: Casos de e-mails usados na pesquisa.

Email Subject	Legitimacy	Relevant features of email and websites
Earn Bonus Points #1	real	win a prize in an online scavenger hunt from BRU Information Security Office link: https://www.bru.edu/iso/aware/ncsam/hunt/bonus
Picture from last weekend's party	possible malware	impersonal greeting link: http://picasaweb.google.com/stevewulitzer/Partypics/ actual url: http://128.3.72.234/Partypics.jpg.exe
No obligation bankruptcy consultation	spam	text of link: “Apply online now” actual url: https://www.bankruptcylawyerfinder.com/freeconsultation.htm?...
Bandwidth Quota Offer	phishing	misspelling in url and .org domain link http://www.brubandwithamnesty.org/bandwidth/agree.htm actual url: same
eBay Accounts Security	phishing	threatens account suspension link: https://signin.eBay.com/ws/eBayISAPI.dll?SignIn&sid=verify … actual url: http://www.security-validation-your-account.com/signin.ebay/…
Your Amazon.com Order (#103-0607555-6895008)	real	problem with shipping link: www.amazon.com/help/confirmation actual url: same
Your eBay item sold!	real	text of link: “Send Invoice Now” actual url: http://payments.ebay.com/eBayISAPI...

Fonte: Who falls for phish?, Sheng et al [31]

Os resultados foram observados a partir de dois tipos de erros dos participantes: os falsos positivos, quando um site verdadeiro é considerado falso erroneamente, e cair no phishing. Nessa pesquisa, assim como em outros trabalhos, “cair no phishing” é determinado por inserir seus dados no site e, de acordo com o resultado, 90% dos indivíduos que clicaram no link também forneceram suas informações.

Em relação à questão demográfica, foi observado que mulheres, antes do treinamento, têm maior propensão a clicarem nos links e procederem com o fornecimento de seus dados, em um comparativo de 54,7% de mulheres e 49% de homens. Também foi percebido que o grupo etário entre 10 e 25 anos são mais

suscetíveis, devido à menor exposição a treinamentos, menos anos de experiência com a Internet e menor medo dos riscos financeiros.

Os resultados, assim como no primeiro artigo, apontaram que o conhecimento prévio sobre phishing ajudava na menor suscetibilidade do indivíduo ao ataque, entretanto o conhecimento sobre outros conceitos computacionais não estava relacionado à diminuição na probabilidade de cair no ataque. E, em relação ao treinamento, os participantes que o fizeram depois do *role play* caíram em 47% dos sites de phishing, enquanto que, do contrário, esse número caiu para 28%.

3.1. Considerações finais

Os resultados apresentados em ambos os trabalhos mostraram-se similares, validando a eficácia do método na avaliação da suscetibilidade ao phishing que, mesmo não sendo igual a realidade, se aproxima bastante dela.

No entanto, houve limitações que estavam na pouca diversidade do grupo de participantes, pois todos eles faziam parte da comunidade da Universidade e não uma parcela geral dos usuários de e-mail; na pequena quantidade de casos de phishing de modo a não deixar o questionário tão longo (no caso do primeiro artigo citado); e na falta de consequências mais diretas do comportamento, visto que os participantes poderiam agir com maior risco por não haver consequências para suas ações.

A metodologia utilizada nesses trabalhos foi usada como base para este que, por meio de uma adaptação do questionário, tendo como principal etapa a do *role play*, para avaliar apenas um grupo específico de participantes, focando, portanto, na avaliação da relação entre o conhecimento e a suscetibilidade ao phishing.

No capítulo seguinte, será apresentada a metodologia utilizada para a realização deste trabalho.

4. Metodologia

A partir dos resultados obtidos na pesquisa foi possível extrair conhecimentos acerca do comportamento dos indivíduos quanto aos seus hábitos em relação a e-mails recebidos em sua caixa de mensagens. Em vista disso, podemos classificar a pesquisa como de natureza básica que, como definido por [32], tem como objetivo gerar novos conhecimentos que sejam úteis para o avanço da ciência sem que haja, necessariamente, uma aplicação prática.

Foram utilizadas as técnicas bibliográfica, pois foram usados estudos já publicados em artigos e materiais disponibilizados na Internet como base para a elaboração do material, e a de levantamento realizada através do questionário feito com uma amostra cujo comportamento seria analisado.

Além disso, foi usado o método dedutivo, visando a explicar dadas premissas e chegar a uma conclusão sobre os dados obtidos. E, possui finalidade descritiva, que expõe as características de uma determinada amostra da população através de um questionário online. Quanto a abordagem, foram adotadas tanto a qualitativa quanto a quantitativa, pois é realizada uma análise numérica, além da compreensão e interpretação dos dados levantados sobre uma determinada amostra da população, ou seja, dos resultados obtidos a partir do questionário, embasado em técnicas realizadas nos principais estudos científicos sobre a suscetibilidade ao phishing.

Para verificar a relação entre conhecimento e suscetibilidade ao phishing, este trabalho propõe a avaliação por meio de um questionário que restringe os participantes a indivíduos inseridos na área de Tecnologia da Informação, verificando sua forma de interagir com e-mails e, assim, avaliar o nível de preocupação com a segurança de suas informações.

4.1. O questionário

4.1.1. Participantes

A pesquisa foi realizada dentro do Centro de Informática (CIn), da Universidade Federal de Pernambuco (UFPE). Para responder ao questionário, os participantes deveriam possuir o e-mail com o domínio da instituição (*cin.ufpe.br*), como forma de não permitir respostas de outras pessoas de fora e garantir respostas únicas.

Assim, participam dessa pesquisas os discentes de Tecnologia da Informação dos três cursos de graduação: ciência da computação, engenharia da computação e sistemas de informação, além dos discentes da pós-graduação.

4.1.2. Role play

Com base nos artigos citados no Capítulo 3, foi elaborado um questionário similar para este trabalho. No entanto, tendo em vista o grupo restrito de participantes, os discentes de Tecnologia da Informação do Centro de Informática da UFPE, cujo conhecimento sobre certos conceitos da Internet é tido como prévio, algumas partes dos questionários dos artigos foram omitidas, como as perguntas conceituais, sendo avaliado aqui o conhecimento obtido ao longo do curso e também fora dele acerca de segurança. Assim, foram criados 5 casos de e-mails dentro do contexto do CIn para que os participantes os avaliasse como se no lugar de uma estudante fictícia, Maria Silva.

Assim como nos artigos, o enfoque da pesquisa não foi explicitado no questionário, sendo descrito nele o caráter avaliativo sobre hábitos no uso do serviço de e-mail do CIn. Então, em seguida, foram realizadas perguntas relativas ao discente, como curso e período; e, depois, sobre a frequência de acesso ao e-mail e o principal meio utilizado para tal.

Em seguida foi iniciado o *role play*, contendo 5 questões, de forma a não tornar o questionário extenso, relativas a e-mails recebidos por Maria Silva, com suas devidas considerações, usadas para contextualizar o participante.

O objetivo do questionário era verificar a principal ação do participante, perguntando-lhe o que ele faria diante dos e-mails mostrados, dando-lhe as seguintes opções, adaptando-as a cada caso: responder o e-mail, encaminhar o e-mail, apenas ler a mensagem e deixá-la na caixa de mensagens, deletar o e-mail, clicar no link do e-mail, e digitar ou copiar a URL no navegador. Caso o participante escolhesse clicar no link ou digitar a URL no navegador, seria mostrada a imagem da página Web correspondente e novamente uma pergunta sobre sua ação diante dela, também adaptando as opções a cada caso, como responder o formulário, fazer login, preencher com os dados, deletar o e-mail, etc.

Tabela 1: 5 casos de e-mails utilizados na pesquisa.

E-mail	**Legitimidade**	**Considerações**
Convite Formulários Google	real	1- Maria acha importante responder formulários acadêmicos
Convite de colaboração de pasta Google Drive	phishing	1- O remetente é conhecido
Oportunidade de vagas	possível malware	1- Maria tem interesse em vagas de trabalho 2- O remetente é conhecido
Dropbox	real	1- Maria possui uma conta do Dropbox cadastrada neste e-mail 2- Maria acha possível ter arquivos importantes armazenados no Dropbox
Netflix	spear phishing	1- Maria possui cadastro do Netflix neste e-mail

Fonte: Simone Cohen (2017)

O primeiro e-mail era legítimo e se tratava de um convite do *Formulários Google* para responder a um questionário. Enviado ao "*grad-l@cin.ufpe.br*", lista de e-mail dos estudantes de graduação do CIn, por um e-mail da própria instituição, não havia nenhuma característica de phishing no e-mail. A página direcionada pelo link era também legítima e possuía a verificação de segurança do *Google* através de certificado digital, indicada pelo cadeado próximo à URL.

O segundo, um e-mail similar ao anterior, era de um convite ilegítimo de colaboração de uma pasta do *Google Drive*, armazenamento na nuvem bastante utilizado pelos alunos do CIn. Embora o corpo do e-mail fosse idêntico ao original, nele podemos observar algumas características de sua ilegitimidade, como o domínio de envio "*cin.ufpe.br*" sem assinatura, sendo que o mais comum seria um dos domínios utilizados pelo *Google Drive*, como o "doclist.bounces.google.com". Além disso, o link não corresponde ao original "https://drive.google.com", sendo ele "http://drive.com" sem o uso do protocolo HTTPS (Hypertext Transfer Protocol Secure), que implementa o HTTP simples sobre uma camada de segurança, utilizando o protocolo SSL/TLS (*Secure Socket Layer / Transport Layer Security*) e fazendo com que os dados sejam transmitidos através de uma conexão criptografada e com o uso de certificados digitais. A página direcionada pelo link era idêntica à original e pedia para o participante fazer *login* com sua conta do CIn.

O terceiro e-mail, em relação a vagas de trabalho, também foi ilegítimo e possuía 2 imagens anexas que mostrariam detalhes sobre as vagas. As características do phishing apareciam no formato das imagens "*.jpeq*" no lugar de "*.jpeg*", fazendo com que o *Gmail* não reconhecesse o formato para mostrar a pré-visualização da imagem. Então, ao clicar na imagem, era exibida uma mensagem "Nenhuma visualização disponível" e o botão para *download*, obrigando o destinatário do e-mail a baixar os anexos se quisesse visualizá-los. O perigo do e-mail estava, justamente, em fazer esse *download*, pois um possível *malware* poderia infectar a máquina do indivíduo.

O quarto e-mail era verídico, um comunicado do *Dropbox* sobre o encerramento da conta de usuário após muito tempo de sem uso. Nele havia um link para a página do *Dropbox* que deveria ser acessado caso o usuário desejasse manter sua conta. Ao acessar, era exibida uma página de *login* legítima, inclusive com verificação de segurança.

O último caso se tratava de um aviso do *Netflix* sobre confirmação de cadastro. Esse e-mail foi baseado em casos reais de ataques de phishing que vêm acontecendo [40]. Em um e-mail com aparência idêntica a do *Netflix*, o texto fala sobre uma atualização dos dados de pagamento devido a um problema da empresa na hora de validar essas informações, implicando em uma possível suspensão da

conta até a realização da atualização. Então, há um link malicioso que direciona o usuário para uma página falsa, muito similar a do *Netflix*, que pede todos os dados do cartão de crédito da vítima.

4.2. Validade das respostas

É importante considerar que neste tipo de pesquisa, através de um questionário online, nem todos os participantes respondem com total ciência da importância de sua resposta e isso pode aparecer, consequentemente, no resultado final da pesquisa em casos de respostas notavelmente incongruentes.

Uma possível solução para isso seria tornar o questionário mais específico e extenso, como sugerido na seção 6.1, de forma a tratar tais tipos de respostas e, assim, criar um critério para separação das respostas.

4.3. Considerações finais

Neste capítulo foi apresentada a metodologia utilizada para a realização do experimento através do questionário com os casos de e-mail a serem avaliados pelos participantes. Foram todos casos simples e com características marcantes de phishing para verificar o nível de alerta dos respondentes.

No próximo capítulo, serão discutidos os resultados obtidos com essas respostas, avaliando-as de acordo com critérios que serão apresentados.

5. Resultados

Neste capítulo serão apresentados os resultados obtidos no questionário que foi aplicado durante os meses de Outubro e Novembro, obtendo 414 respostas de um total de 2.115 alunos do centro, o que correspondeu a 19,5% dos alunos matriculados. Não é considerada nesse valor total uma margem de erro que leve em consideração desistências após a matrícula no início do período ou alunos pouco participativos na instituição.

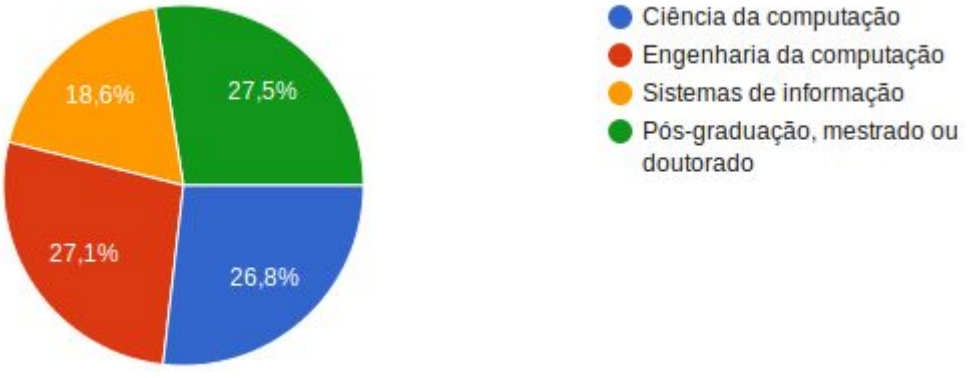
Em seguida, serão realizadas análises dos dados obtidos seguindo os seguintes critérios:

- Suscetibilidade ao phishing;
- Suscetibilidade a clicar nos links segundo o curso;
- Suscetibilidade a clicar nos links segundo o nível de experiência, mensurado de acordo com o período cursado pelo participante;
- Relação entre digitar ou copiar a URL e cair no phishing.

5.1. Curso e período dos participantes

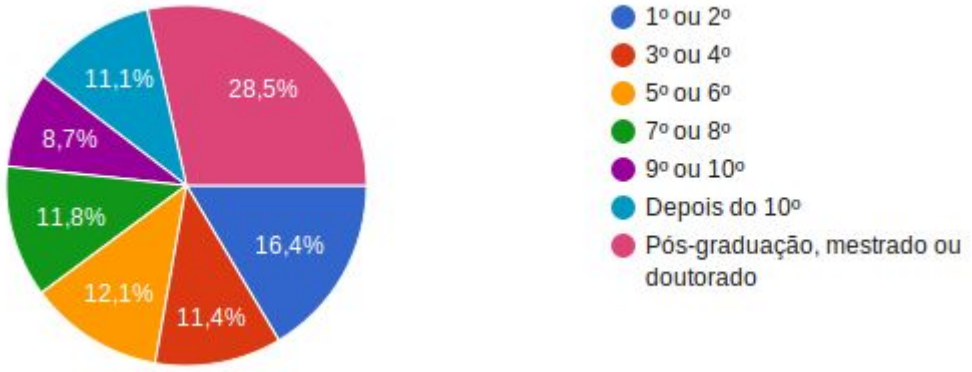
As duas primeiras perguntas do questionário foram referentes a amostra populacional dos participantes quanto ao seu curso e período, caso fossem discentes de graduação, ou da pós-graduação, como pode ser visto nos Gráficos 1 e 2.

Gráfico 1: Resultado para o curso dos respondentes.



Fonte: Simone Cohen (2017)

Gráfico 2: Resultado para o período dos respondentes.

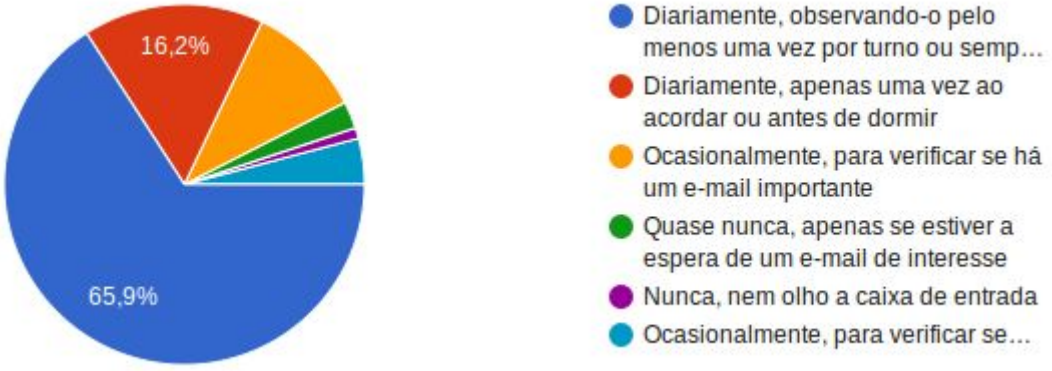


Fonte: Simone Cohen (2017)

5.2. Uso do e-mail

As perguntas 3 e 4 foram referentes à frequência de acesso ao e-mail do Centro de Informática e o principal meio para acessar sua caixa de entrada, como pode ser visto nos Gráficos 3 e 4. Os usuários que observam seus e-mails assiduamente foram maioria entre os participantes, assim como o meio de acessá-lo foi através de cliente de e-mail para dispositivos móveis.

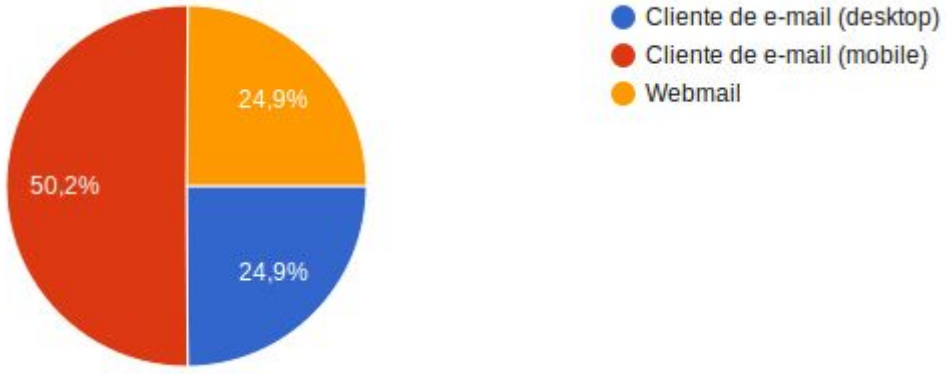
Gráfico 3: Resultado para a frequência de acesso ao e-mail do Centro de Informática.[6]



Fonte: Simone Cohen (2017)

[6] O texto cortado representa: “Diariamente, observando-o pelo menos uma vez por turno ou sempre que chega um novo e-mail” e “Ocasionalmente, para verificar se há um e-mail importante”.

Gráfico 4: Resultado para o principal meio de acesso ao e-mail do Centro de Informática.



Fonte: Simone Cohen (2017)

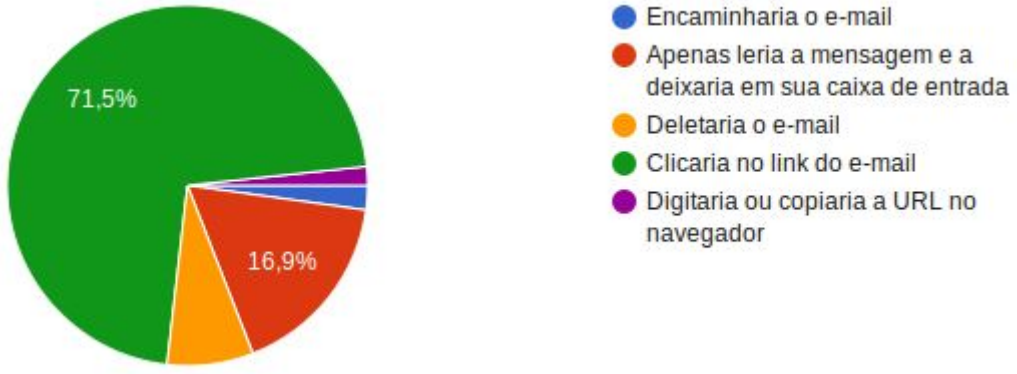
5.3. *Role play*

Nesta seção serão apresentados os resultados para cada uma das perguntas relacionadas aos casos de e-mail.

5.3.1. Convite Formulários Google

O resultado obtido revelou que 71,5% dos participantes tendem a clicar no link, o que pode indicar a confiança dele em relação ao site.

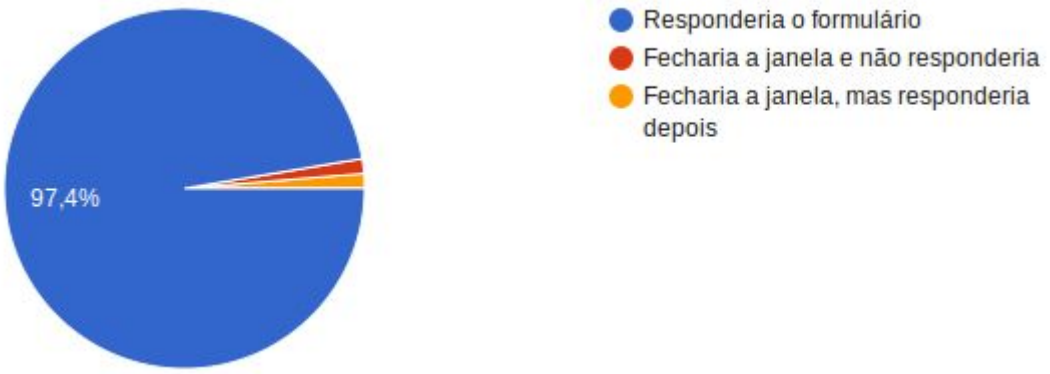
Gráfico 5: Resultado percentual dos participantes em relação ao e-mail do Formulários Google.



Fonte: Simone Cohen (2017)

Desses, considerando os que optaram por clicar no link ou digitar ou copiar a URL no navegador, 73,2% foram direcionados para uma imagem de um website com o formulário e, nesse caso, 97,4% dos participantes optaram por responder o formulário, 1,3% fechariam a janela sem responder e 1,3% fechariam mas responderiam depois.

Gráfico 6: Resultado percentual dos participantes sobre sua ação ao acessar o website do formulário.



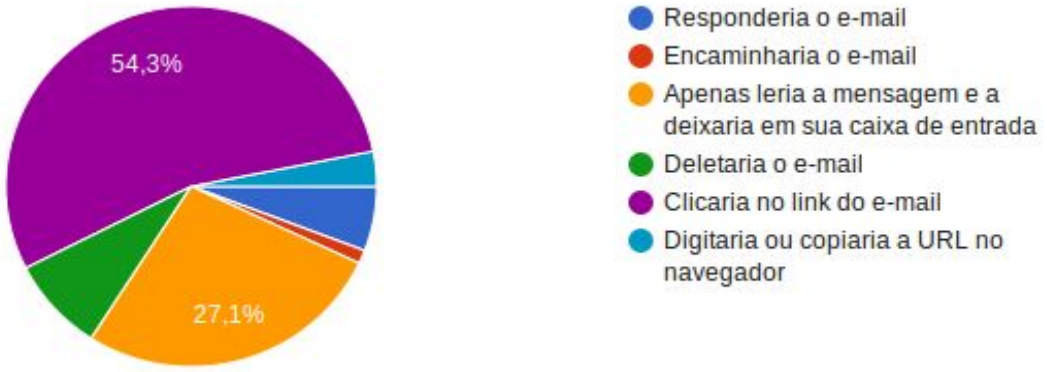
Fonte: Simone Cohen (2017)

Esse foi o caso de teste, para ambientar os participantes ao contexto do questionário e, por isso, não será levado em consideração nos critérios citados no início do capítulo.

5.3.2. Convite de colaboração de pasta do Google Drive

O resultado mostrou que 54,3% dos participantes clicariam no link, número expressivo que também se mostra nos 63,9% que preencheriam os campos de login e senha para acessar o *Google Drive* do site falso, como pode ser visto nos Gráficos 7 e 8. Essa atitude poderia trazer grandes prejuízos caso um atacante usasse as credenciais do e-mail e nele obtivesse acesso às plataformas cadastradas com ele. No caso do e-mail institucional talvez esse não fosse tanto o caso, embora seja possível, mas a mesma atitude no e-mail pessoal poderia ter esse resultado.

Gráfico 7: Resultado percentual dos participantes em relação ao e-mail do Google Drive.



Fonte: Simone Cohen (2017)

Gráfico 8: Resultado percentual dos participantes sobre sua ação ao acessar o website ilegítimo do Google Drive.

Fonte: Simone Cohen (2017)

De um total de 3,1% dos participantes que escolheram a opção “Digitaria ou copiaria a URL no navegador”, 61,5% não faria login, indicativo de que esses participantes podem ter percebido a ilegitimidade da URL e, por isso, não procederam com o login. Entretanto, mesmo no caso de escolher essa opção, houve participantes que fariam login, ou seja, o nível de atenção para a URL foi pequeno a ponto de sua semelhança com a original ser capaz de enganar os participantes.

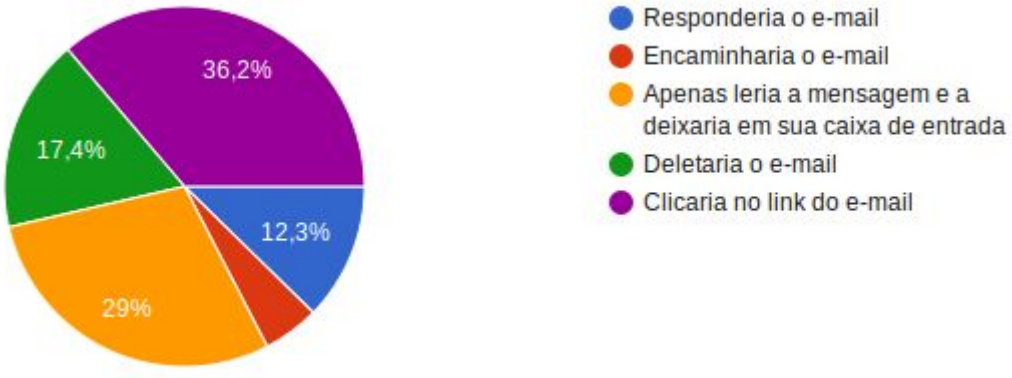
Nesse caso, segundo as recomendações da seção 2.3.2 para não cair no phishing, a principal estratégia seria ter atenção à URL do link e perceber que a conexão insegura através de HTTP não seria utilizada numa página de *login* do Google.

5.3.3. Oportunidade de vagas

Caso de e-mail que utilizava uma abordagem diferente dos demais, em que não havia uma página web extra redirecionada a partir de um link, o usuário precisaria observar a extensão dos arquivos anexados ao e-mail, atentando para o fato de que a imagem não possuía uma visualização prévia, sem que fosse necessário o download, justamente para que um possível usuário fosse obrigado a fazer o download e abrir o arquivo, tendo assim sua máquina comprometida por um possível malware.

O resultado para esse caso se mostrou menos favorável para o sucesso do phishing, pois, comparado ao resultado do caso da seção 5.3.2, a quantidade de participantes que clicaram no link foi bem menor, apenas 36,2%. No entanto, mesmo com o menor número de cliques, ainda assim 60,7%, o que corresponde a 91 participantes, faria o download do arquivo, como mostrado no Gráfico 10.

Gráfico 9: Resultado percentual dos participantes em relação ao e-mail sobre as vagas de emprego.



Fonte: Simone Cohen (2017)

O percentual de participantes que responderia o e-mail, tanto na pergunta principal quanto na secundária, pode indicar que não houve a percepção sobre sua ilegitimidade e que, de fato, tentariam entrar em contato por acreditar, por exemplo, no arquivo como corrompido.

Gráfico 10: Resultado percentual dos participantes sobre sua ação ao optarem por visualizar a imagem.

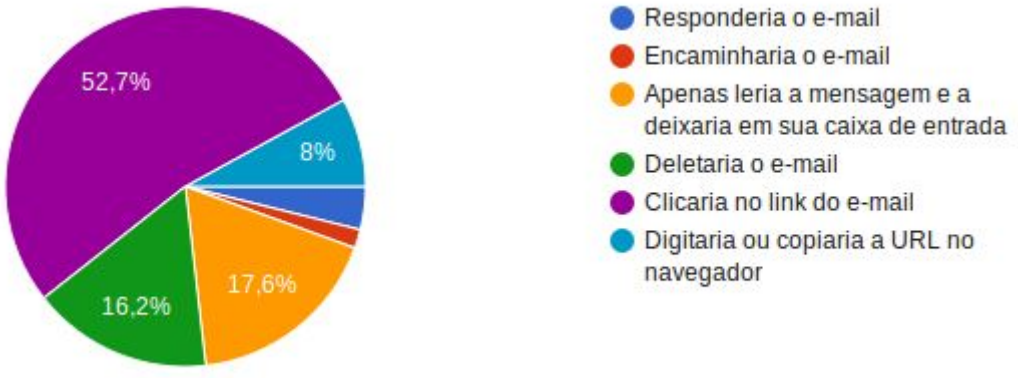
Fonte: Simone Cohen (2017)

Nesse caso, era imprescindível observar a extensão do arquivo e desconfiar por ela não estar entre as mais comuns extensões de arquivos de imagem, além de impossibilidade de pré-visualização que obriga o download para que o indivíduo veja seu conteúdo. Como casos de arquivos são mais difíceis de reconhecer, geralmente, a recomendação é não fazer download de nenhum arquivo a menos que o remetente seja totalmente confiável.

5.3.4. Dropbox

Caso de e-mail legítimo, o resultado demonstrou que a maioria dos participantes clicariam no link, um total de 52,7%.

Gráfico 11: Resultado percentual dos participantes em relação ao e-mail do Dropbox.



Fonte: Simone Cohen (2017)

Sobre o resultado apresentado no Gráfico 12, podem ser indícios de desconfiança os 8,8% que não fariam login e os 5,2% que voltariam ao e-mail para acessar o link novamente, apesar do ícone de verificação de segurança do site.

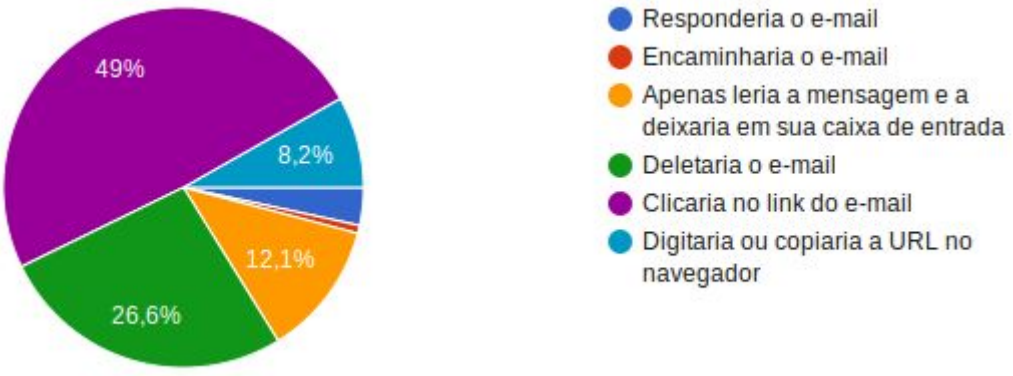
Gráfico 12: Resultado percentual dos participantes sobre sua ação ao optarem por acessar o website do Dropbox.

Fonte: Simone Cohen (2017)

5.3.5. Netflix

Caso de e-mail com tema financeiro e, dentre todos, o que poderia trazer maiores prejuízos para o indivíduo que preenchesse seus dados no site. Embora uma considerável parcela dos participantes tenha optado por deletar o e-mail, 49% deles clicariam no link e 8,2% digitariam ou copiariam a URL no navegador.

Gráfico 13: Resultado percentual dos participantes em relação ao e-mail do Netflix.

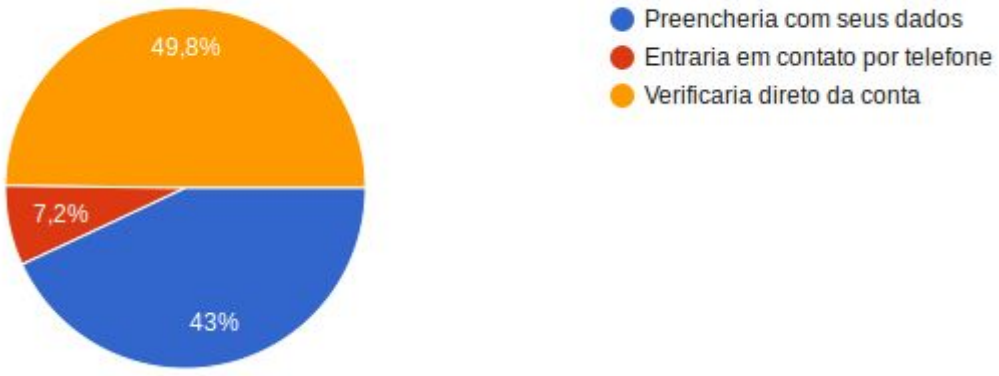


Fonte: Simone Cohen (2017)

O resultado para aqueles que acessariam o website se mostrou bastante dividido entre os que preencheriam com seus dados (43%) e os que verificariam direto da conta (49,8%). Apesar disso, o número de participantes que preencheriam com seus dados do cartão de crédito, um total de 102 de 237, foi considerável a ponto de ser preocupante. Em uma escala maior, um ataque de phishing nesse molde seria capaz de vitimizar milhares de pessoas, levando a um prejuízo enorme.

É preciso ter consciência de que nenhuma grande empresa pediria dados pessoais diretamente por e-mail e, principalmente, é necessário desconfiar de pedidos desse tipo, principalmente quando envolvem dados financeiros, pois são os maiores alvos de fraudes.

Gráfico 14: Resultado percentual dos participantes sobre sua ação ao optarem por acessar o website ilegítimo do Netflix.



Fonte: Simone Cohen (2017)

Para não cair no phishing nesse caso, seria preciso seguir recomendações da seção 2.3.2 e prestar atenção ao remetente, buscando garantir sua legitimidade, além de observar bem a URL do link, verificando se havia uma conexão segura HTTPS na página que pedia por informações sensíveis do usuário. Também seria recomendado desconfiar da urgência do e-mail, pois ele dá a entender que a conta do usuário pode ser desabilitada justamente para causar medo e o indivíduo não procurar outros meios de resolver o problema.

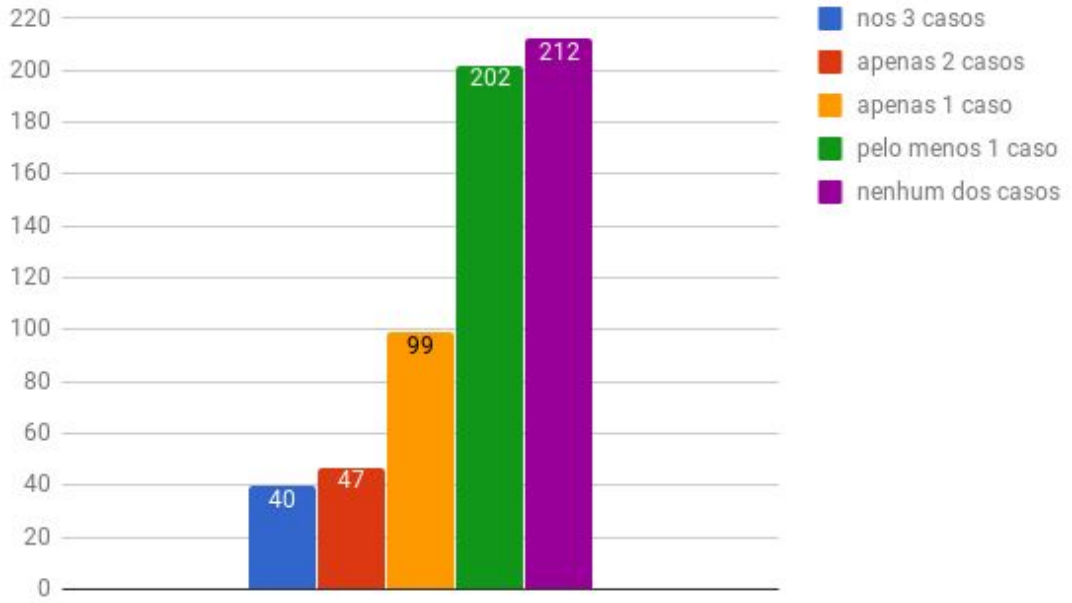
5.4. Análise dos resultados

A análise é feita a partir dos dados verificando quem cairia no phishing, considerando os participantes que chegaram a fornecer suas informações ou fazer o download do arquivo em pelo menos 1 caso; e os que não cairiam em nenhum deles. No entanto, não é possível diferenciar aqueles indivíduos que responderam conscientemente dos que não o fizeram e, por isso, todas as respostas serão consideradas como válidas.

5.4.1. Suscetibilidade ao phishing

Os resultados mostraram que 212 participantes não cairiam em nenhum dos ataques de phishing, enquanto que 202 estão suscetíveis a ele. Um resultado bastante equilibrado que demonstra que os participantes demonstram atenção e cautela frente aos casos de e-mail. Entretanto, não foi um número baixo o de participantes suscetíveis ao phishing.

Gráfico 15: Suscetibilidade ao phishing

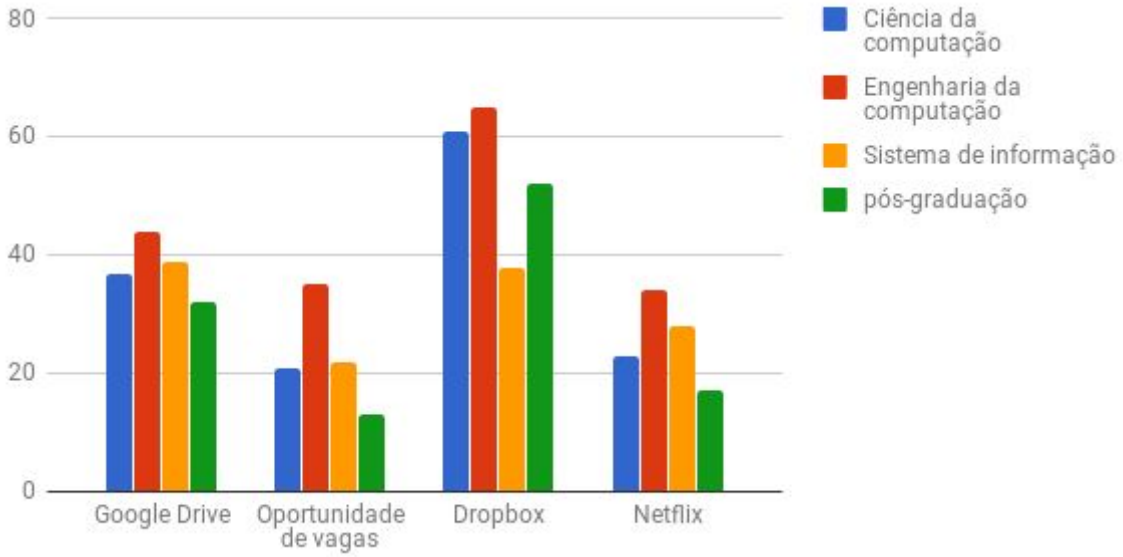


Fonte: Simone Cohen (2017)

5.4.2. Suscetibilidade a clicar nos links segundo o curso

Filtrando os resultados de “clicar no link / digitar ou copiar a URL no navegador” e proceder com “fazer login / fazer download do arquivo / preencher com os dados”, ou seja, que resultem em sucesso do phishing, por curso para cada um dos casos, temos que o mais suscetível deles, em dados brutos, é o de Engenharia da Computação, Gráfico 16.

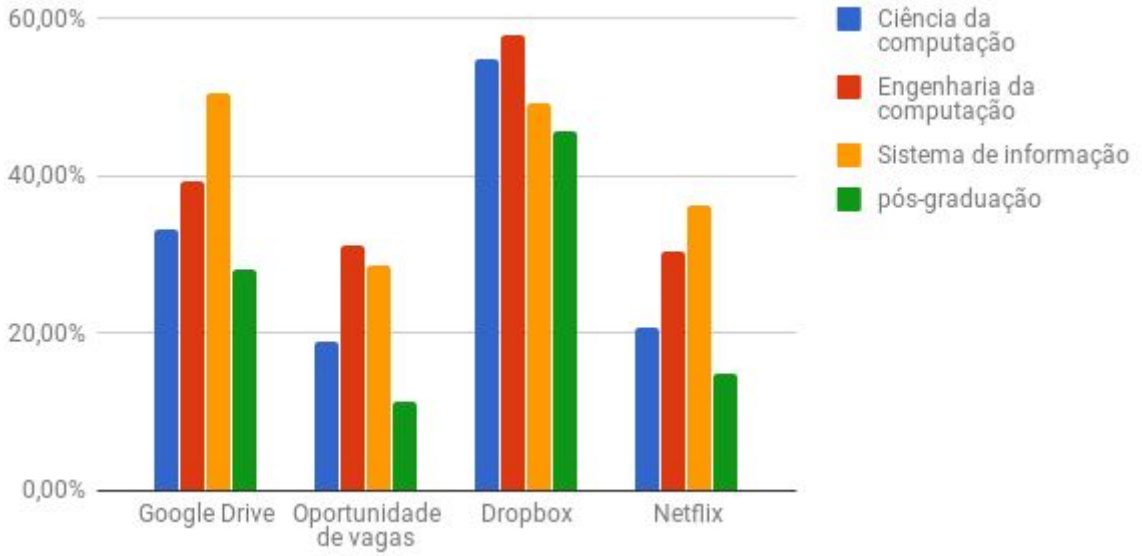
Gráfico 16: Relação entre curso de graduação ou pós-graduação e quantidade de respostas de sucesso para o phishing ao optar por “clicar no link” e “preencher com os dados / fazer login / fazer download do arquivo”.



Fonte: Simone Cohen (2017)

No entanto, proporcionalmente, o curso de Sistema de Informação supera os demais em 2 dos casos, o do “Google Drive” e do “Netflix”, como pode ser visto no Gráfico 17. Enquanto que o curso de Engenharia está, aproximadamente, 2,7% à frente do curso de Sistema de Informação no caso de “Oportunidade de vagas”.

Gráfico 17: Relação proporcional entre curso de graduação ou pós-graduação e quantidade de respostas de sucesso para o phishing ao optar por “clicar no link” e “preencher com os dados / fazer login / fazer download do arquivo”.



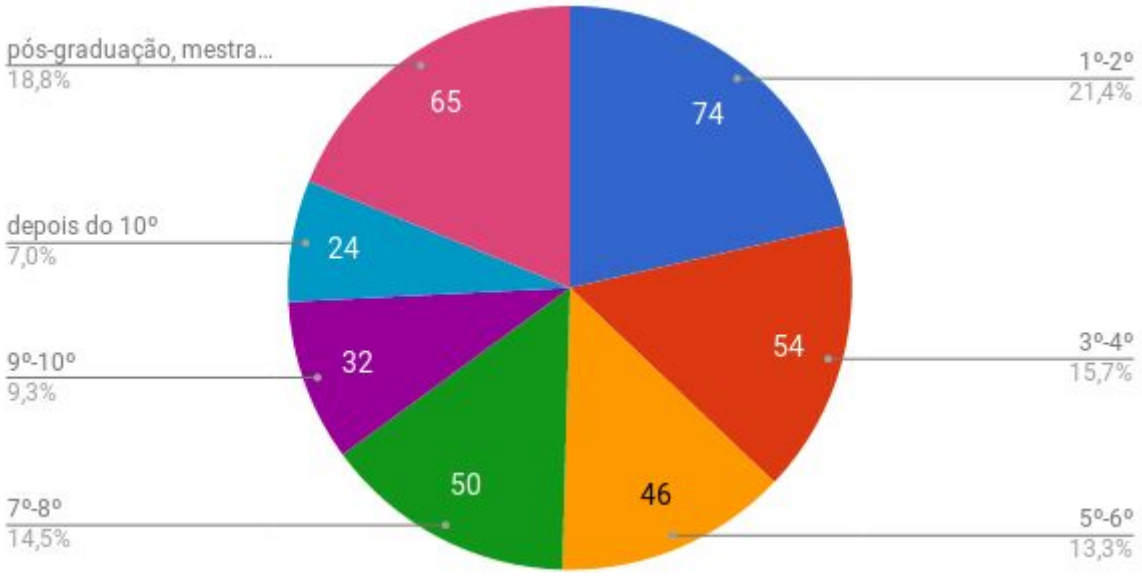
Fonte: Simone Cohen (2017)

Nos gráficos, o caso do Dropbox, por ser legítimo, é exibido apenas para fins comparativos.

5.4.3. Suscetibilidade a clicar nos links segundo o nível de experiência

O critério de experiência foi mensurado segundo o período cursado pelo participante. Assim, foram filtrados, por período, os dados relativos aos casos de phishing nos quais os participantes clicaram no link. O Gráfico 18 mostra o somatório de cliques, envolvendo os 3 casos de phishing, em que o ataque seria bem sucedido, ou seja, se os dados fossem inseridos ou o arquivo baixado, totalizando 345 cliques (podendo ser contabilizado o mesmo participante mais de uma vez para casos de e-mail distintos).

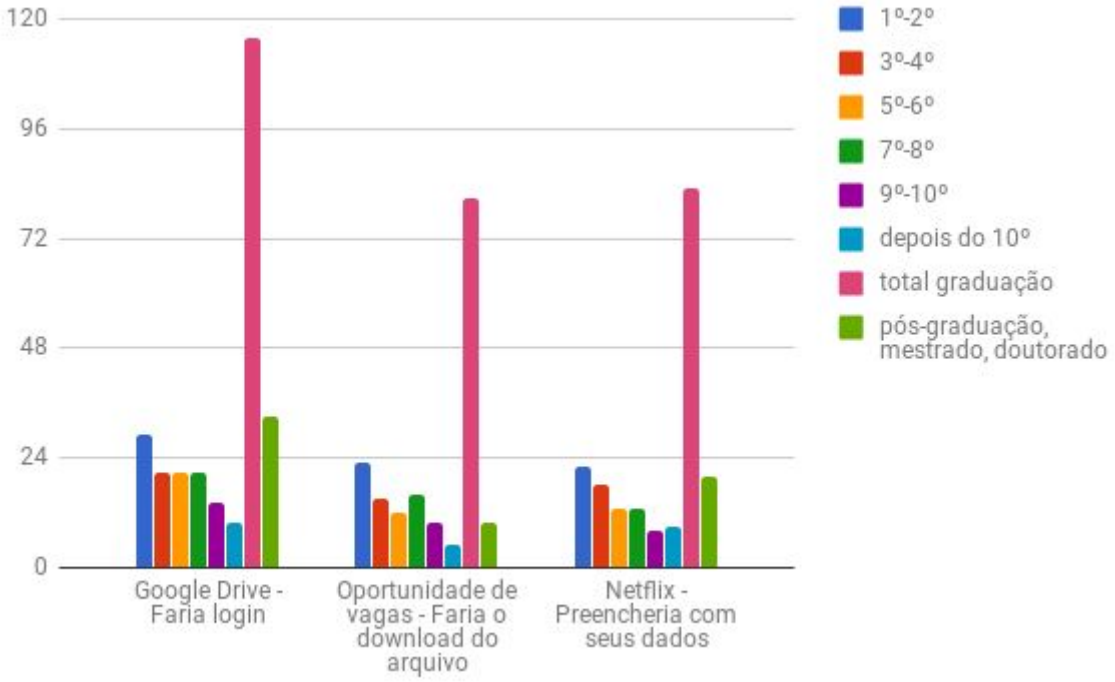
Gráfico 18: Quantidade de cliques, por período, que resultariam no fornecimento de dados ou no download do arquivo.



Fonte: Simone Cohen (2017)

Separando as respostas por período é possível perceber, em cada um dos casos, que a quantidade de respostas tende a diminuir à medida que aumenta o período de graduação do participante. São pontos fora da curva o caso do “7º-8º” períodos no caso de “Oportunidade de vagas” e “depois o 10º” para o caso do “Netflix”, em que cairiam no phishing mais do que participantes de períodos passados.

Gráfico 19: Relações entre período de graduação ou pós-graduação e quantidade de respostas de sucesso para o phishing.



Fonte: Simone Cohen (2017)

No entanto, foi constatado que os participantes da pós-graduação obtiveram um grande número de respostas em dois dos casos, superando todos os períodos da graduação, no caso do "*Google Drive",* e todos os períodos a partir do 3º-4º, no caso do "Netflix". Isso pode implicar que, embora tenham sido um dos grupos mais atentos à extensão errada do arquivo do caso "Oportunidade de vagas", talvez um indicativo do seu desinteresse pelo conteúdo do e-mail, eles não foram completamente capazes de distinguir os detalhes que caracterizavam os outros dois casos (de "Oportunidade de vagas" e "Netflix") como phishing, como, por exemplo, a URL incorreta do ou a falta do cadeado de verificação de segurança.

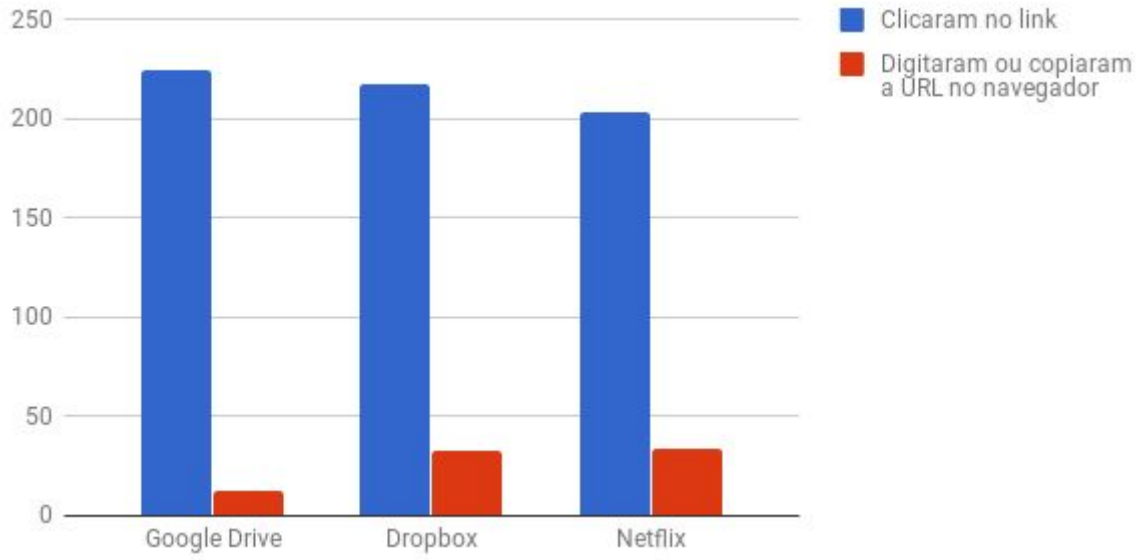
Além disso, é interessante considerar que entre os participantes da pós-graduação pode haver indivíduos de graduações fora da área de Informática, o que pode ter aumentado o sucesso do phishing.

5.4.4. Relação entre digitar ou copiar a URL e cair no phishing

A partir dos resultados obtidos, ficou perceptível o baixo nível de desconfiança dos participantes por não se preocuparem em digitar ou copiar a URL no navegador, como pode ser visto no Gráfico 20, ação que poderia evitar a eficácia do phishing nos casos como o do "Netflix" em que a URL possui erros de grafia ("*http://netflx.com"*, sem o "i") ou do "Google Drive" com a URL diferente da original ("*http://drive.com*", em contrapartida com o original "*https://drive.google.com*"), indicando a ilegitimidade de ambos.

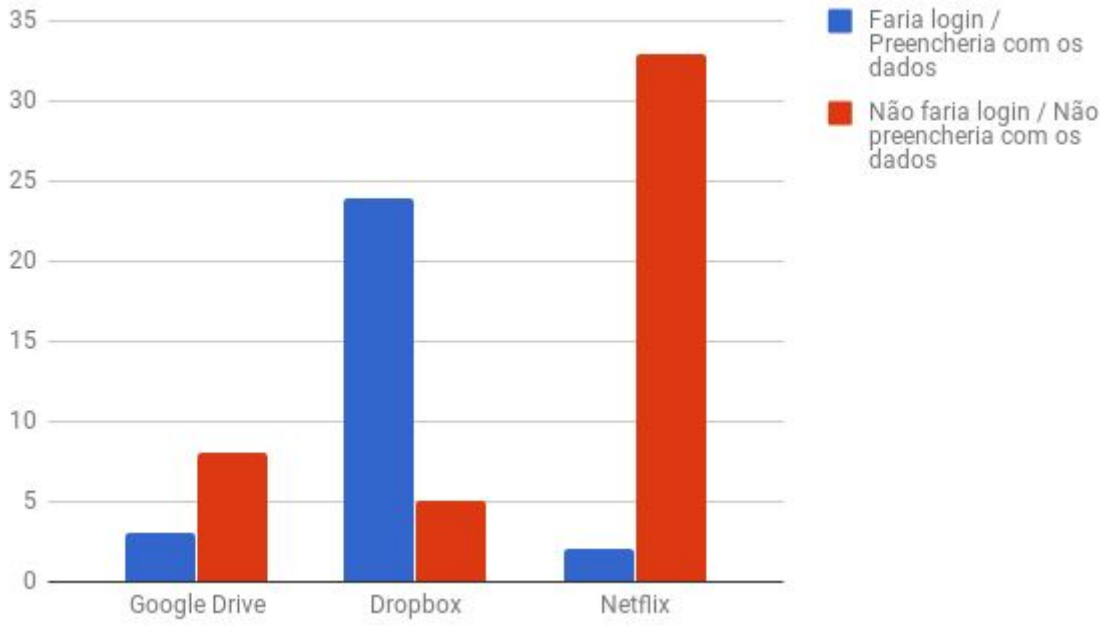
Não é possível atestar se todos que clicaram no link conferiram a URL, mas, dado o grande número de casos de phishing bem sucedido, podemos inferir que a maioria, de fato, não deu atenção à URL. Em contrapartida, os números mostram, de acordo com o Gráfico 21, que os participantes que digitaram ou copiaram a URL tiveram uma menor tendência a cair no phishing, assim como a maioria deles chegou a fazer login no "Dropbox" corretamente, pois o site era legítimo.

Gráfico 20: Comparativo entre "clicar no link" e "digitar ou copiar a URL no navegador".



Fonte: Simone Cohen (2017)

Gráfico 21: Comparativo entre inserir ou não os dados ao escolher a opção “digitar ou copiar a URL no navegador”.



Fonte: Simone Cohen (2017)

Mas também, assim como não é possível afirmar se os que clicaram no link conferiram a URL, no caso de “digitar ou copiar a URL no navegador” também não é possível. Dados os casos mostrados no Gráfico 21, vemos que mesmo assim ainda houve casos de participantes que caíram no phishing, o que pode significar que a resposta não foi tão consciente como esperado, e isso mostra a importância de validar tais respostas, como sugerido na seção 6.1.

5.5. Considerações finais

Neste capítulo foram apresentados os resultados da pesquisa que mostraram um total de 48,8% dos participantes suscetíveis ao phishing, quase metade da amostra de respondentes, o que indica um alto nível de alerta para um dos mais comuns ataques cibernéticos. Além de mostrar, proporcionalmente que o curso de Sistema de Informação é o mais suscetível entre os de graduação.

Os números também mostram que a experiência adquirida ao longo da graduação faz diminuir a suscetibilidade, no entanto, mostrando um número alto para os participantes de pós-graduação. E, além disso, foram poucos os que

optaram por digitar ou copiar a URL no navegador, o que mostra maior confiança dos participantes em relação ao remetente dos e-mails.

No *role play* havia a possibilidade, em cada um dos casos, de “responder o e-mail” e “encaminhar o e-mail”. Na primeira opção, podemos observar a escolha dessa opção como uma forma de desconfiança e responder o e-mail poderia significar que o indivíduo desejava uma confirmação dele. Já no caso de encaminhar seria o contrário, pois o indivíduo confiou tanto naquele e-mail que, mesmo não sendo de seu interesse, valeria a pena compartilhar com quem se interessasse mais, o que, no caso de um phishing, significaria o aumento de seu alcance, pois pessoas serviram de vetor para espalhá-lo ainda mais.

Em um caso como o do “Dropbox”, de um e-mail legítimo, houve uma parcela de respondentes que deletariam o e-mail. Seja por desinteresse ou desconfiança dos participantes, esse caso pode ser exemplo de que manter o e-mail como principal meio de comunicação seria uma falha de grandes empresas, pois, na dúvida sobre a legitimidade daquela comunicação, os indivíduos tendem a procurar outra forma de contato, como ocorreu no caso do “Netflix”, ou, simplesmente, ignoram o conteúdo do e-mail.

O próximo capítulo conclui esta pesquisa, mostrando as conclusões tiradas acerca dos resultados obtidos e possíveis trabalhos futuros a serem realizados.

6. Considerações finais

O objetivo deste trabalho foi realizar um experimento como forma de avaliar a presença da segurança digital no contexto dos discentes do Centro de Informática. Então, a partir disso, surgiu a proposta de fazer tal avaliação por meio de um dos mais comuns, simples e abrangentes ataques cibernéticos: o phishing.

Por questões éticas, não seria possível realizar o ataque de forma direta. Assim, por meio de um questionário não muito extenso, com perguntas diretas acerca de casos fictícios de e-mails, os alunos foram indagados sobre suas ações diante de tais e-mails. Foram casos simples e com as principais características do ataque sem muitas sofisticações.

Os resultados se mostraram equilibrados, dos 414 respondentes, 212 não caíram em nenhum ataque, o equivalente a aproximadamente 51,2% dos participantes, o que não necessariamente indica que não cairiam em outras abordagens de phishing. Por outro lado, 202 podem ser considerados vítimas em potencial de pelo menos um dos e-mails, sem considerar que um único participante poderia cair em mais de um e-mail, totalizando 345 casos de sucesso de phishing.

Para um ataque de tão baixo custo e, geralmente, de tão pouca sofisticação, atingir nem que seja um indivíduo já pode ser considerado um sucesso para o atacante e possíveis prejuízos para a vítima. Para o phishing tradicional não importa o número de pessoas que não caíram e sim aquelas que forneceram suas informações para o atacante, mesmo que mínimas. No caso do Centro de Informática, ressaltando que as pessoas ali dentro já lidam ou irão lidar em algum momento com dados sensíveis de terceiros, se considerarmos que 202 discentes estão suscetíveis a ataques de phishing, também consideramos que muitos dados estão vulneráveis caso uma dessas pessoas caia em um phishing real. Não somente a suscetibilidade a um ataque pessoal, mas ser um instrumento de entrada para um atacante com objetivos muito maiores.

A preocupação com a segurança digital não está somente em proteger uma máquina contra acesso indevido, está em conhecer as portas de entrada, sabendo que uma delas, e a mais visada, é representada pelos próprios seres humanos.

Medidas de prevenção como as citadas na seção 2.3.2, são apenas o início e evitam os casos mais simples do phishing. No entanto, para os mais elaborados ataques, o que vale é a experiência e um pouco de desconfiança. Como dito por Schneir, citado na seção 2.1, damos muita credibilidade ao que lemos e, raramente, procuramos confirmação. Em um caso como o do exemplo do “Netflix”, acessar a conta para conferir a informação poderia evitar as consequências futuras do ataque, mas damos credibilidade em demasia e a urgência nos faz agir rapida e incorretamente.

No caso como o do Centro de Informática, é necessário que haja conscientização e inclusão de mais tópicos referentes à segurança ao longo das disciplinas para, desde o princípio, alertar os discentes do Centro, para fazê-los criar o interesse pelo tema e saberem se precaver de ataques, reduzindo, então, a porcentagem de discentes que se mostraram suscetíveis ao ataque de phishing neste trabalho.

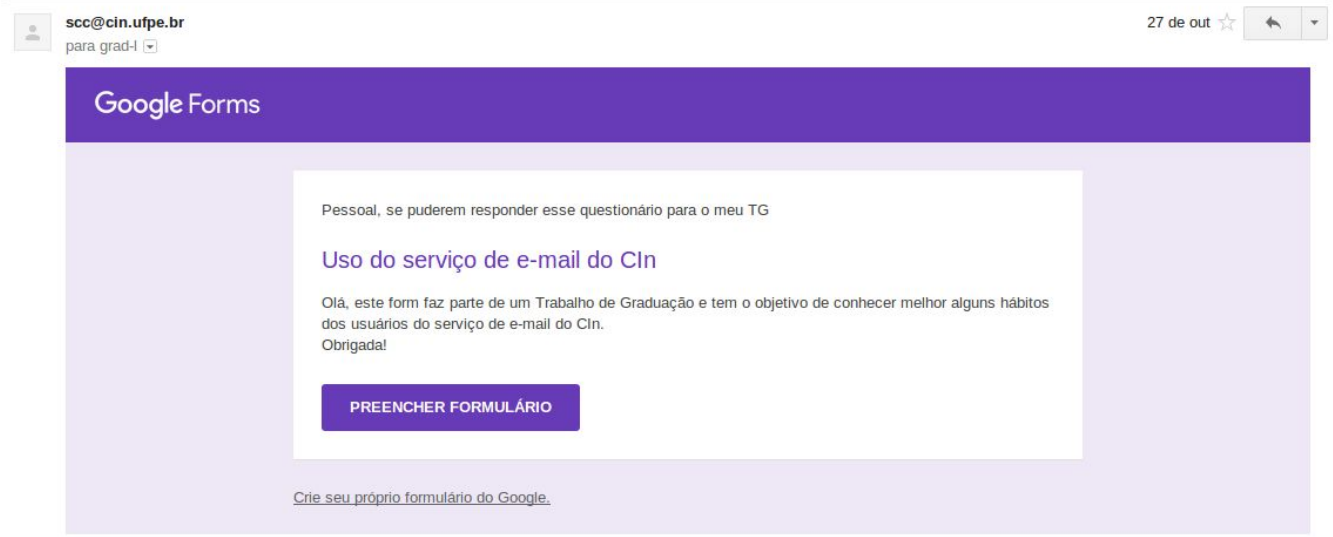
6.1. Trabalhos futuros

Devido ao curto período de realização deste trabalho, não foi possível um maior aprofundamento no assunto, como questionar a motivação de cada pessoa ao decidir por uma das ações em cada caso de e-mail. O phishing muitas vezes explora questões psicológicas dos humanos, podendo apelar para a boa vontade, o desespero, o medo, entre outros.

Por isso, em trabalhos futuros, poderiam ser avaliados esses quesitos a partir de questionários mais extensos e até entrevistas com questões tanto objetivas quanto subjetivas, com grupos não aleatórios de participantes de forma a obter resultados mais detalhados e com maior nível de precisão, inclusive para compreender melhor o modo de pensar de cada um dos participantes e os pontos que os levaram a dado comportamento. Também poderiam ser dadas mais opções de respostas para os participantes, mudando a abordagem de múltipla escolha para caixas de seleção, fazendo com que o indivíduo preenchesse com todas as suas possíveis ações diante do caso de e-mail mostrado no questionário.

Além disso, poderiam ser realizados treinamentos para aqueles que caírem no phishing para, posteriormente, reavaliar seu comportamento e verificar a eficácia desse tipo de ação paliativa.

Apêndice A - E-mail de convite



Apêndice B - O questionário

Uso do serviço de e-mail do CIn

Olá, este form faz parte de um Trabalho de Graduação e tem o objetivo de conhecer melhor alguns hábitos dos usuários do serviço de e-mail do CIn.
Obrigada!

1- Qual o seu curso? *

- ◯ Ciência da computação
- ◯ Engenharia da computação
- ◯ Sistemas de informação
- ◯ Pós-graduação, mestrado ou doutorado

2- Qual o seu período? *

- ◯ 1º ou 2º
- ◯ 3º ou 4º
- ◯ 5º ou 6º
- ◯ 7º ou 8º
- ◯ 9º ou 10º
- ◯ Depois do 10º
- ◯ Pós-graduação, mestrado ou doutorado

3- Você acessa o seu e-mail do CIn com que frequência? *

- ◯ Diariamente, observando-o pelo menos uma vez por turno ou sempre que chega um novo e-mail
- ◯ Diariamente, apenas uma vez ao acordar ou antes de dormir
- ◯ Ocasionalmente, para verificar se há um e-mail importante
- ◯ Quase nunca, apenas se estiver a espera de um e-mail de interesse
- ◯ Nunca, nem olho a caixa de entrada

4- Qual o principal meio utilizado para visualizar sua conta? *

- ◯ Cliente de e-mail (desktop)
- ◯ Cliente de e-mail (mobile)
- ◯ Webmail

Leia aqui!

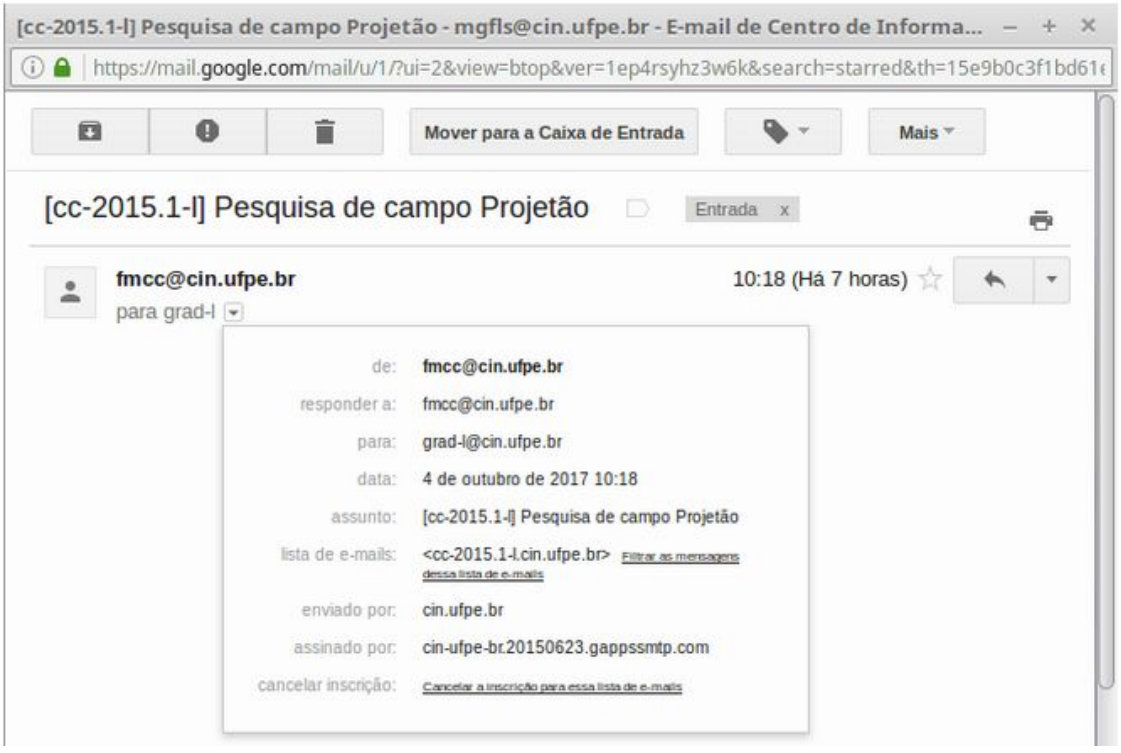
A seguir, serão mostrados casos de e-mails, segundo o contexto do Centro de Informática, em que você precisa avaliar suas ações, considerando-se no lugar de uma aluna fictícia do CIn, Maria Silva, em relação aos e-mails recebidos por ela.
Então, para cada questão, haverá CONSIDERAÇÕES sobra o contexto de Maria e, logo embaixo, a IMAGEM de um e-mail a ser avaliado.

OBS: as informações contidas nas imagens são todas fictícias e apenas imitam a realidade.

CONSIDERAÇÕES:

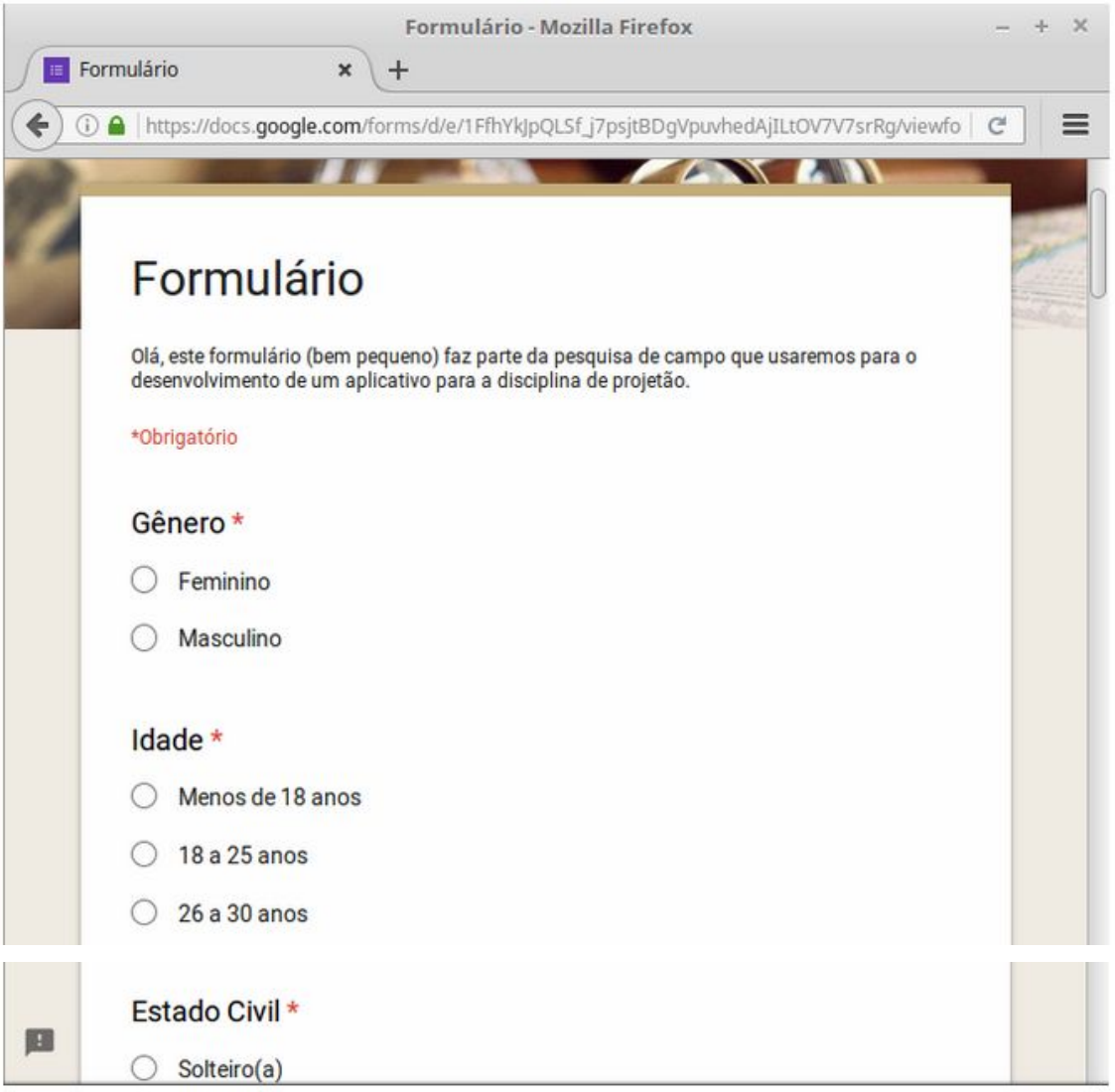
1- MARIA ACHA IMPORTANTE RESPONDER FORMULÁRIOS ACADÊMICOS

5- Marque a ação que você tomaria na seguinte situação: *



- ◯ Encaminharia o e-mail
- ◯ Apenas leria a mensagem e a deixaria em sua caixa de entrada
- ◯ Deletaria o e-mail
- ◯ Clicaria no link do e-mail
- ◯ Digitaria ou copiaria a URL no navegador

Dado que tenha acessado a página do link, qual ação tomaria? *

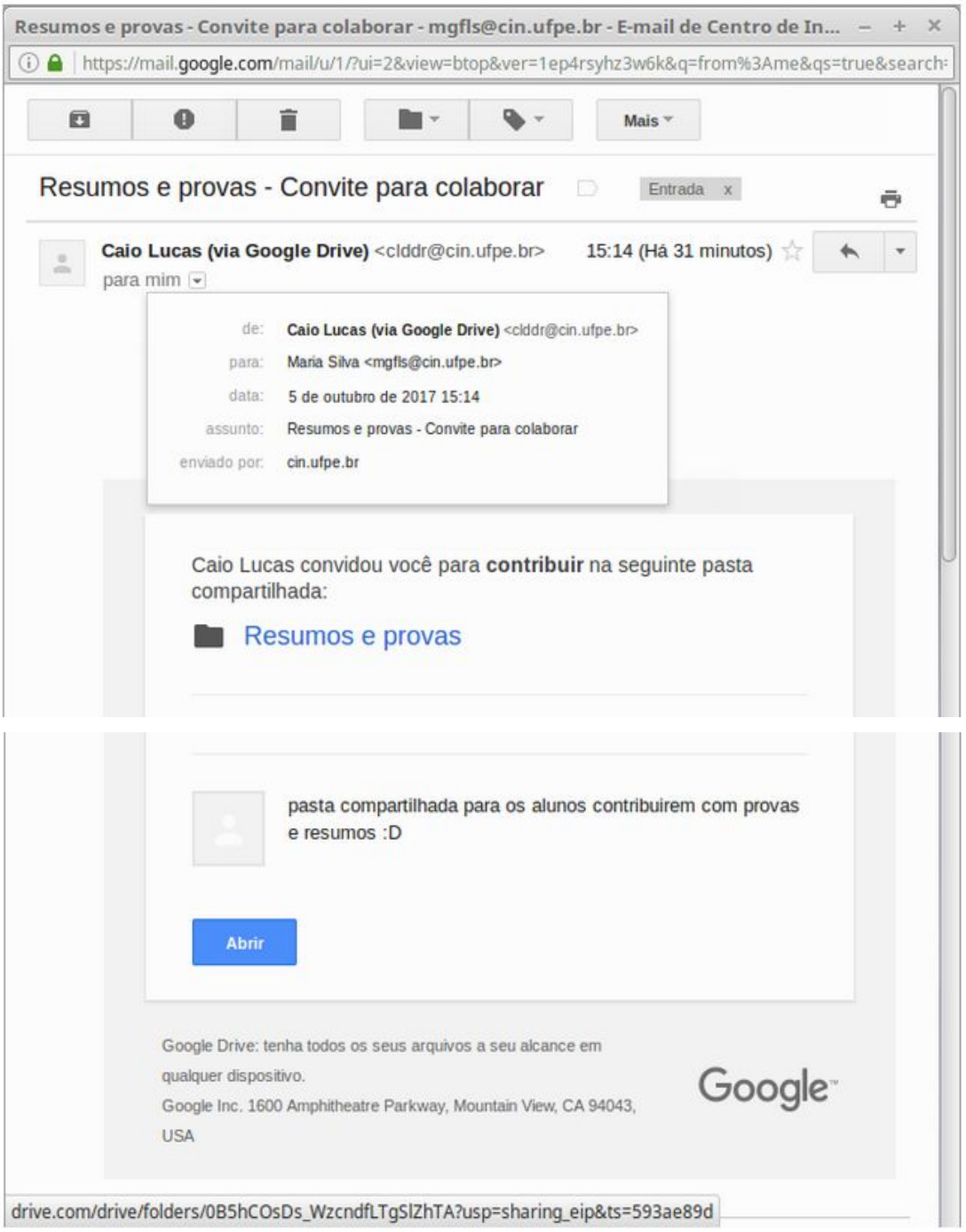


- ( ) Responderia o formulário
- ( ) Fecharia a janela e não responderia
- ( ) Fecharia a janela, mas responderia depois

CONSIDERAÇÕES:

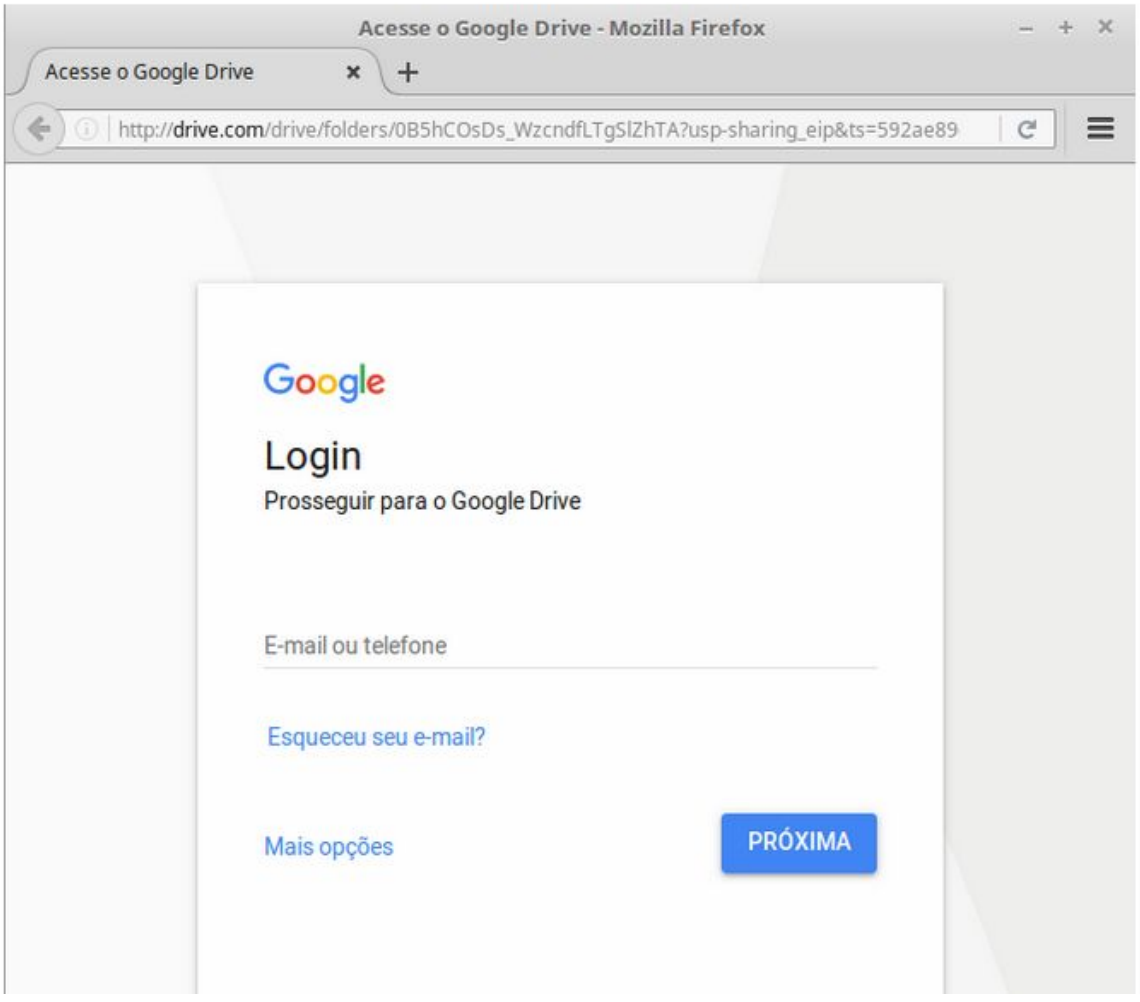
1- O REMETENTE É CONHECIDO

6- Marque a ação que você tomaria na seguinte situação: *



- ◯ Responderia o e-mail
- ◯ Encaminharia o e-mail
- ◯ Apenas leria a mensagem e a deixaria em sua caixa de entrada
- ◯ Deletaria o e-mail
- ◯ Clicaria no link do e-mail
- ◯ Digitaria ou copiaria a URL no navegador

Dado que tenha acessado a página do link, qual ação tomaria? *

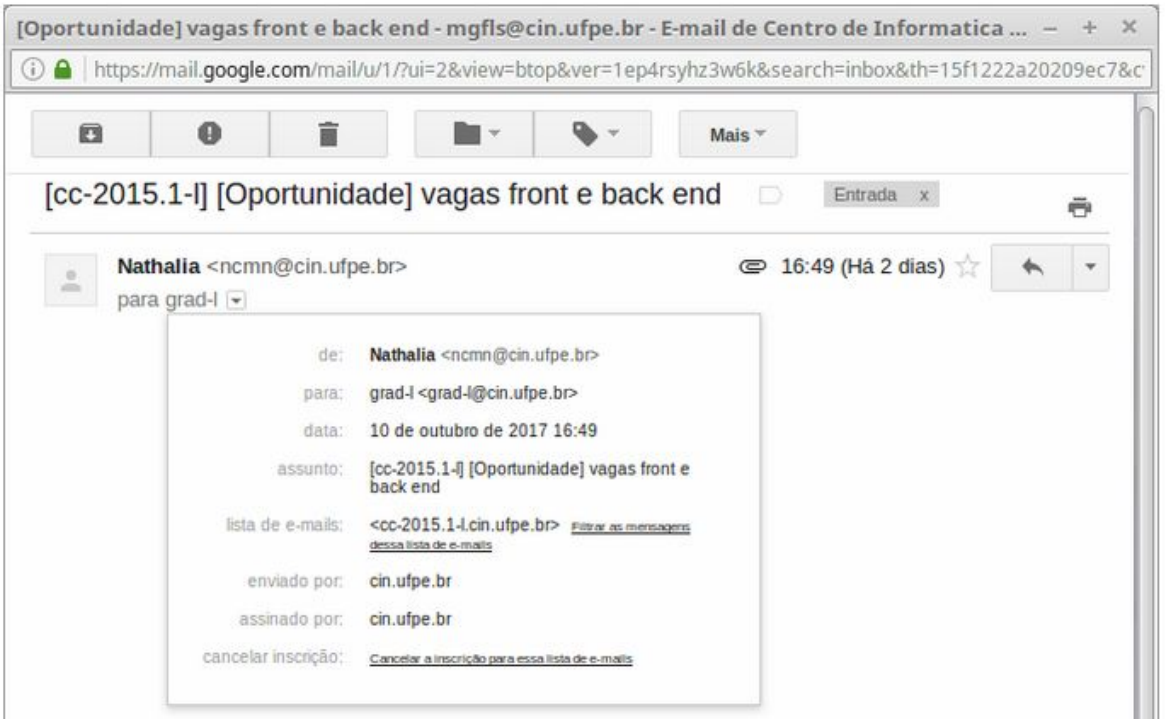


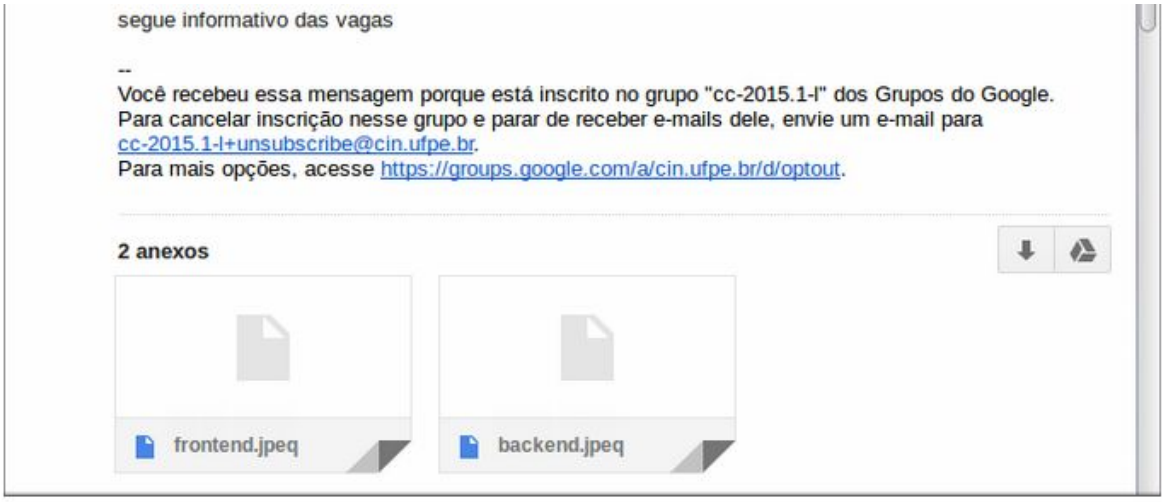
- ◯ Faria login
- ◯ Tentaria acessar o link novamente a partir do e-mail
- ◯ Não faria login

CONSIDERAÇÕES:

1- MARIA TEM INTERESSE EM VAGAS DE TRABALHO
2- O REMETENTE É CONHECIDO

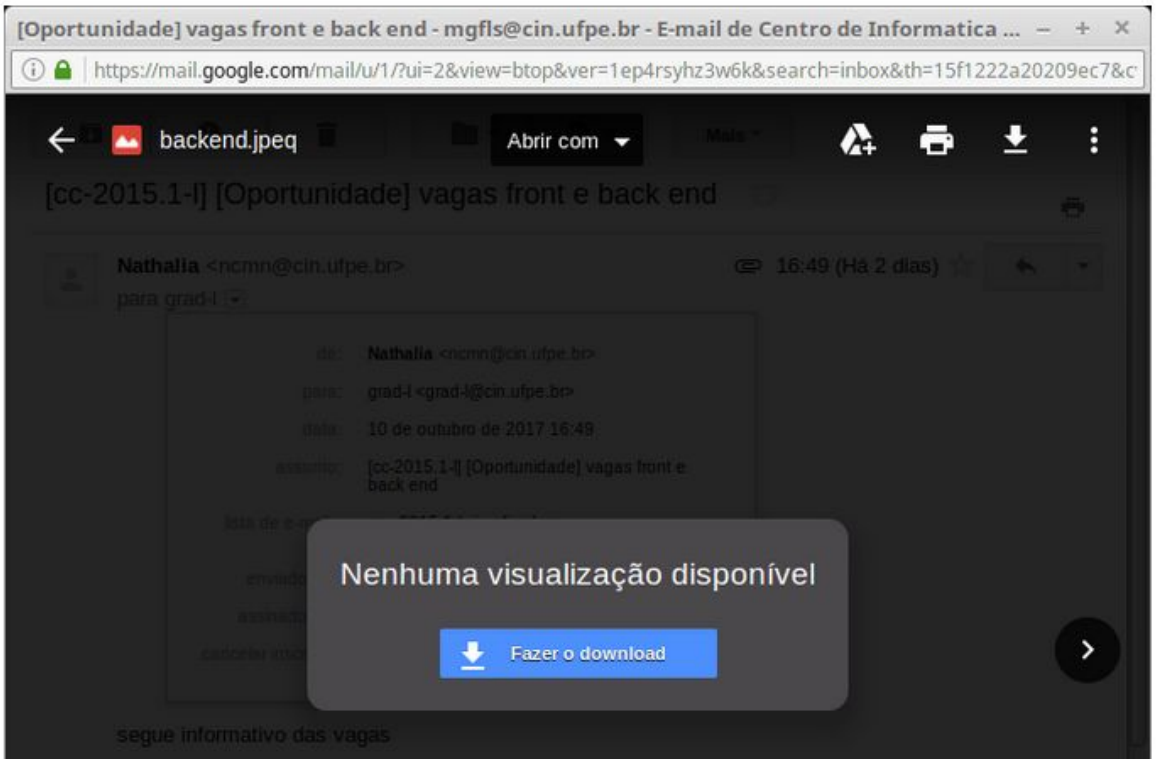
7- Marque a ação que você tomaria na seguinte situação: *

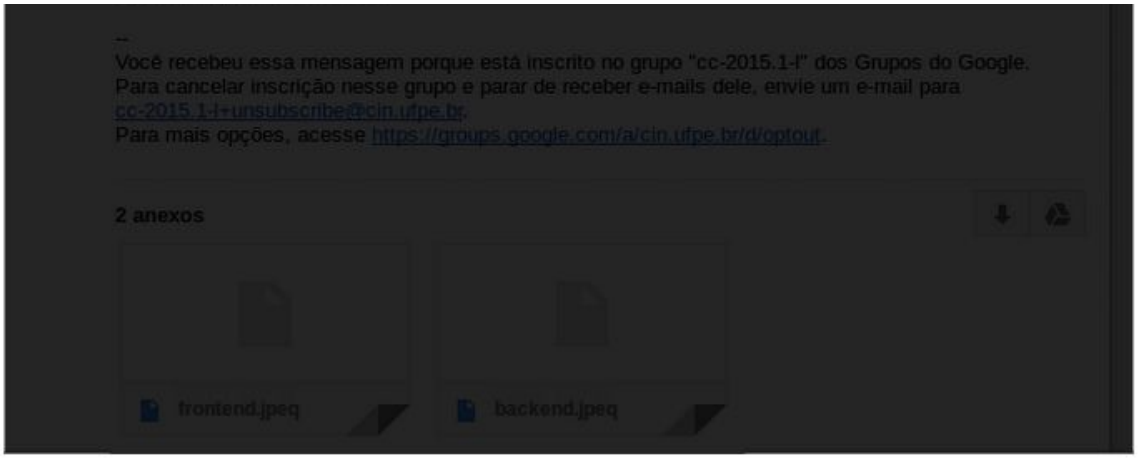




- ◯ Responderia o e-mail
- ◯ Encaminharia o e-mail
- ◯ Apenas leria a mensagem e a deixaria em sua caixa de entrada
- ◯ Deletaria o e-mail
- ◯ Clicaria no link do e-mail

Dado que tenha acessado a página do link, qual ação tomaria? *



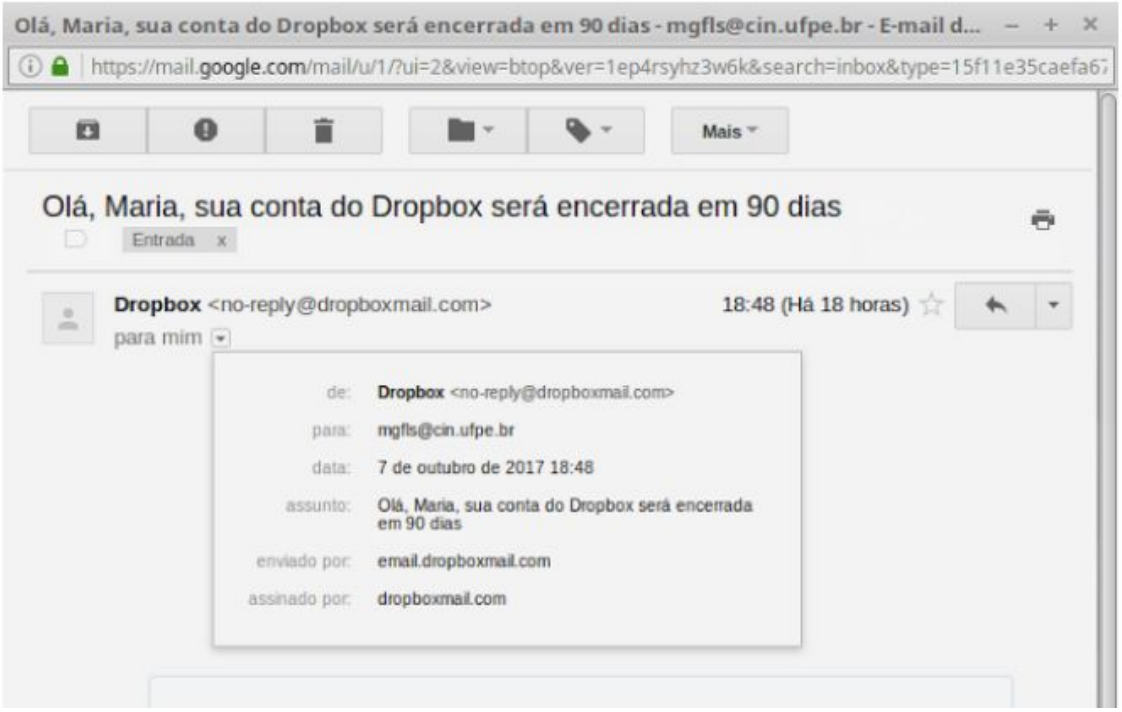


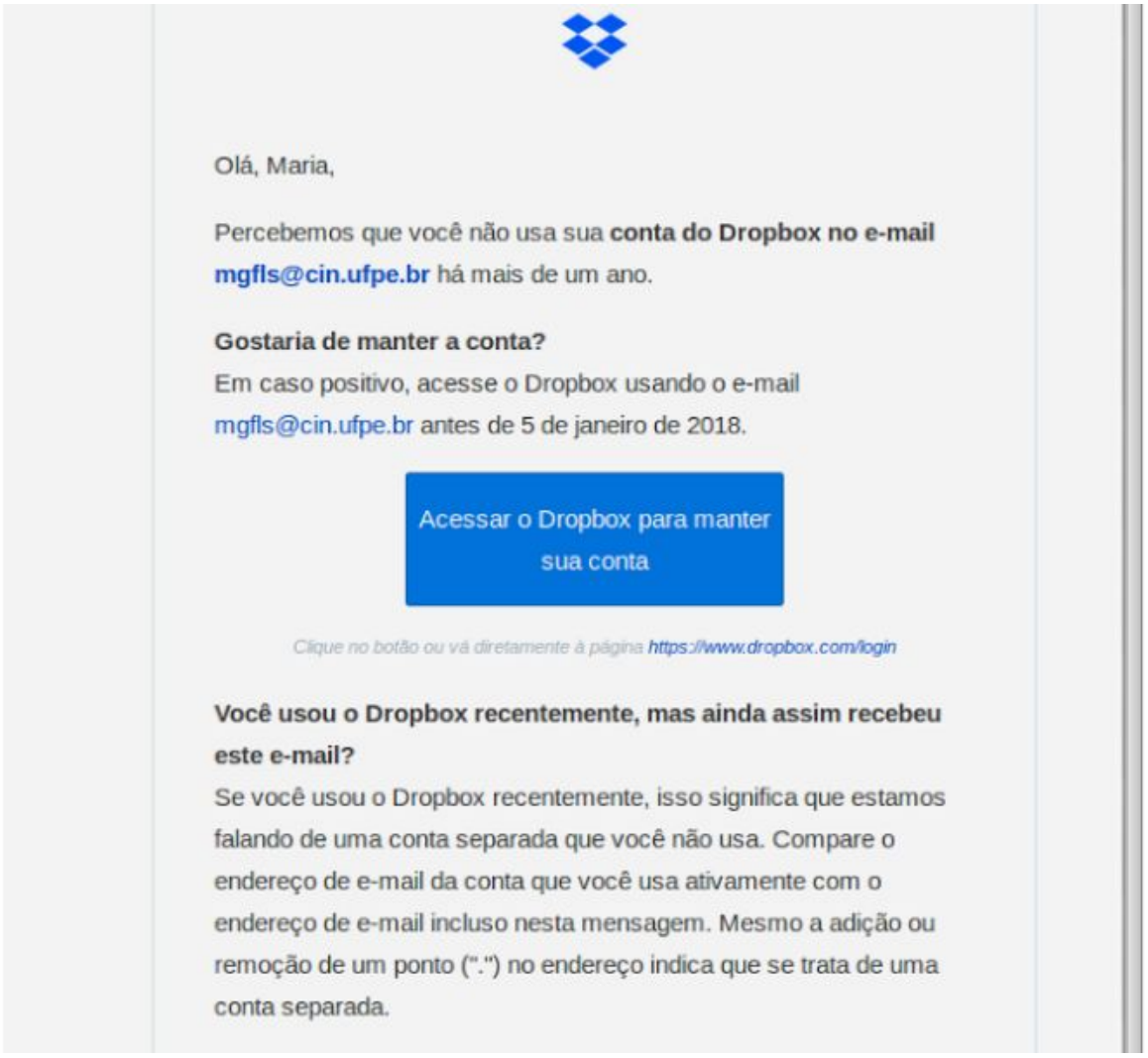
- ◯ Faria o download do arquivo
- ◯ Voltaria e responderia o e-mail por não conseguir ver o preview da imagem
- ◯ Deletaria o e-mail

CONSIDERAÇÕES:

1- MARIA POSSUI UMA CONTA DO DROPBOX CADASTRADA NESTE E-MAIL
2- MARIA ACHA POSSÍVEL TER ARQUIVOS IMPORTANTES ARMAZENADOS NO DROPBOX

8- Marque a ação que você tomaria na seguinte situação: *





Olá, Maria,

Percebemos que você não usa sua **conta do Dropbox no e-mail mgfls@cin.ufpe.br** há mais de um ano.

Gostaria de manter a conta?
Em caso positivo, acesse o Dropbox usando o e-mail mgfls@cin.ufpe.br antes de 5 de janeiro de 2018.

Acessar o Dropbox para manter sua conta

Clique no botão ou vá diretamente à página https://www.dropbox.com/login

Você usou o Dropbox recentemente, mas ainda assim recebeu este e-mail?
Se você usou o Dropbox recentemente, isso significa que estamos falando de uma conta separada que você não usa. Compare o endereço de e-mail da conta que você usa ativamente com o endereço de e-mail incluso nesta mensagem. Mesmo a adição ou remoção de um ponto (".") no endereço indica que se trata de uma conta separada.

Não quer mais sua conta?
Sua conta será automaticamente encerrada em 12 de janeiro de 2018. Para saber como salvar seus arquivos antes de sua conta ser encerrada, visite este artigo da Central de ajuda.

O que acontecerá com sua conta?
Depois que sua conta for encerrada, você não poderá mais acessar o Dropbox nem vincular dispositivos. Seus dados também estarão sujeitos à exclusão do serviço.

Se tiver alguma dúvida ou precisar de ajuda com sua conta, visite nossa Central de ajuda ou entre em contato pelo endereço inactives-help@dropbox.com.

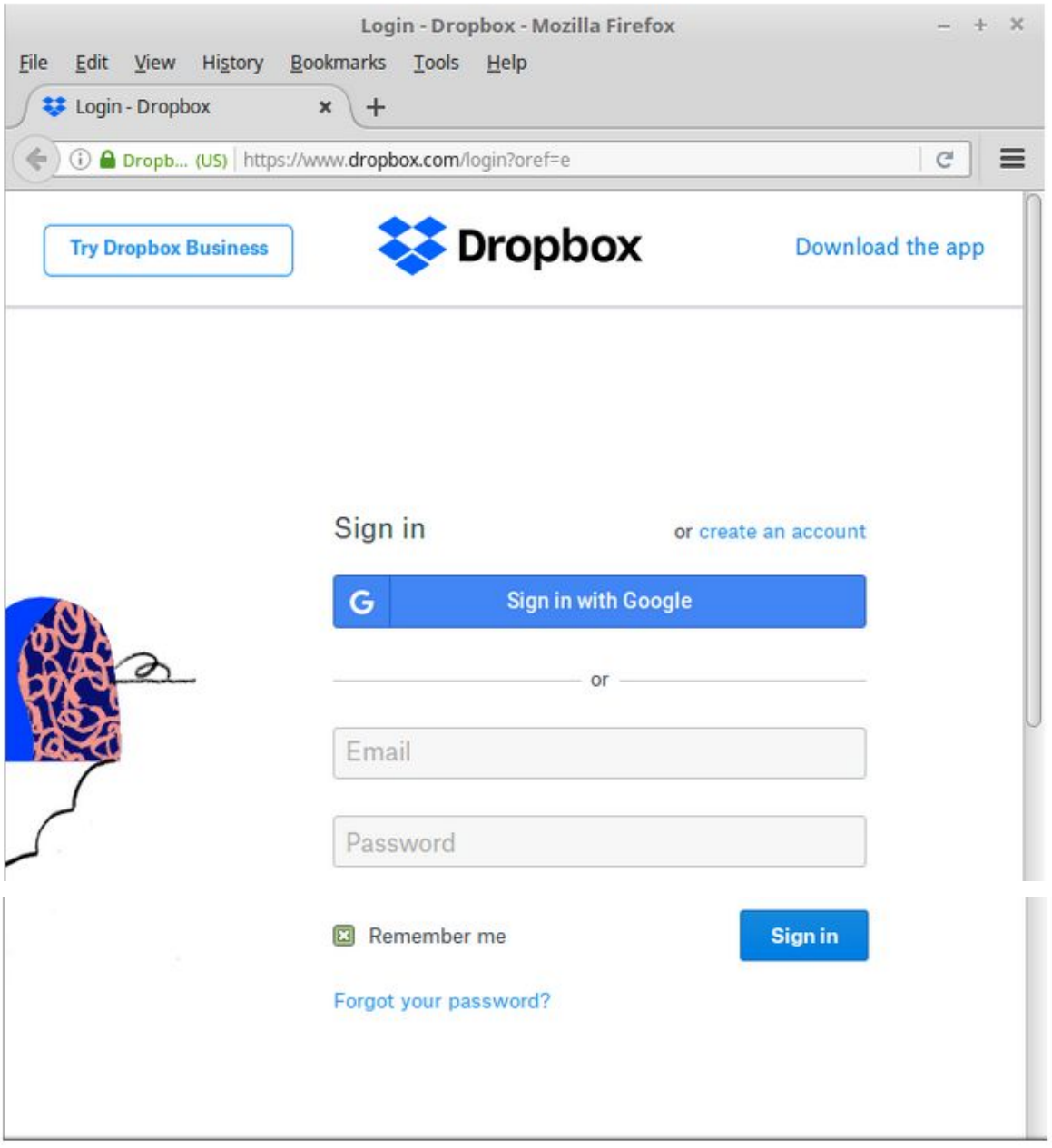
Atenciosamente,
- Equipe Dropbox

Proteja-se contra e-mails falsos.
O Dropbox nunca pede sua senha em e-mails. Se não confiar em um link de uma mensagem de e-mail, vá diretamente à página normal de login. Saiba mais sobre fraudes e roubo de informações

https://www.dropbox.com/l/AACbRMm0_1wU_6arhDKxYJ0gmNn9UHw/login

- ( ) Responderia o e-mail
- ( ) Encaminharia o e-mail
- ( ) Apenas leria a mensagem e a deixaria em sua caixa de entrada
- ( ) Deletaria o e-mail
- ( ) Clicaria no link do e-mail
- ( ) Digitaria ou copiaria a URL no navegador

Dado que tenha acessado a página do link, qual ação tomaria? *



- ◯ Faria login
- ◯ Tentaria acessar o link novamente a partir do e-mail
- ◯ Não faria login

CONSIDERAÇÕES:

1- MARIA POSSUI CADASTRO DO NETFLIX NESTE E-MAIL

9- Marque a ação que você tomaria na seguinte situação: *

Confirmação de cadastro

Olá!

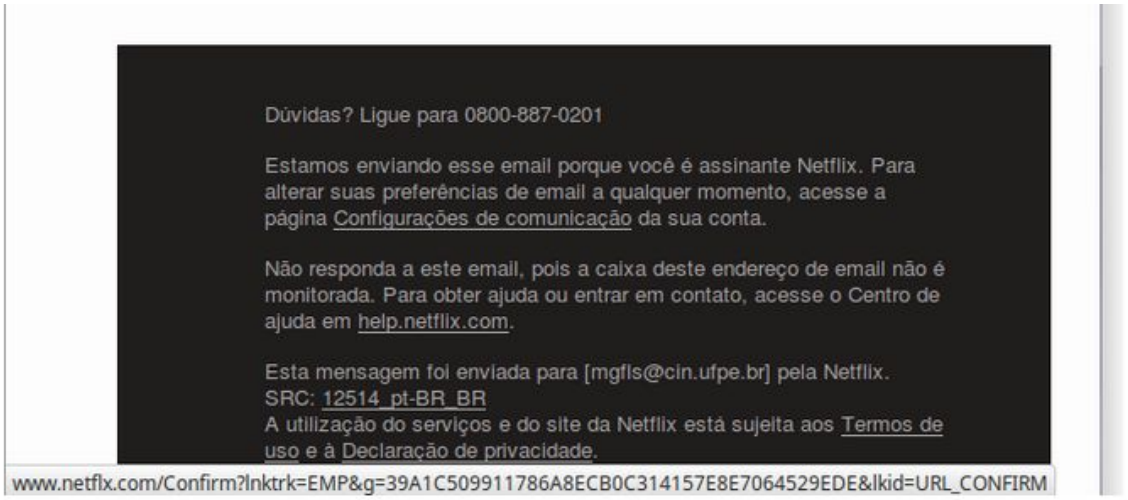
Recentemente, tivemos problemas ao verificar seus dados de pagamento cadastrados no nosso sistema e, por isso, precisamos revalidar essas informações.

Atualizar seus dados fará com que você continue aproveitando no próximo mês as melhores séries e filmes sem interrupções.

CONFIRMAR DADOS

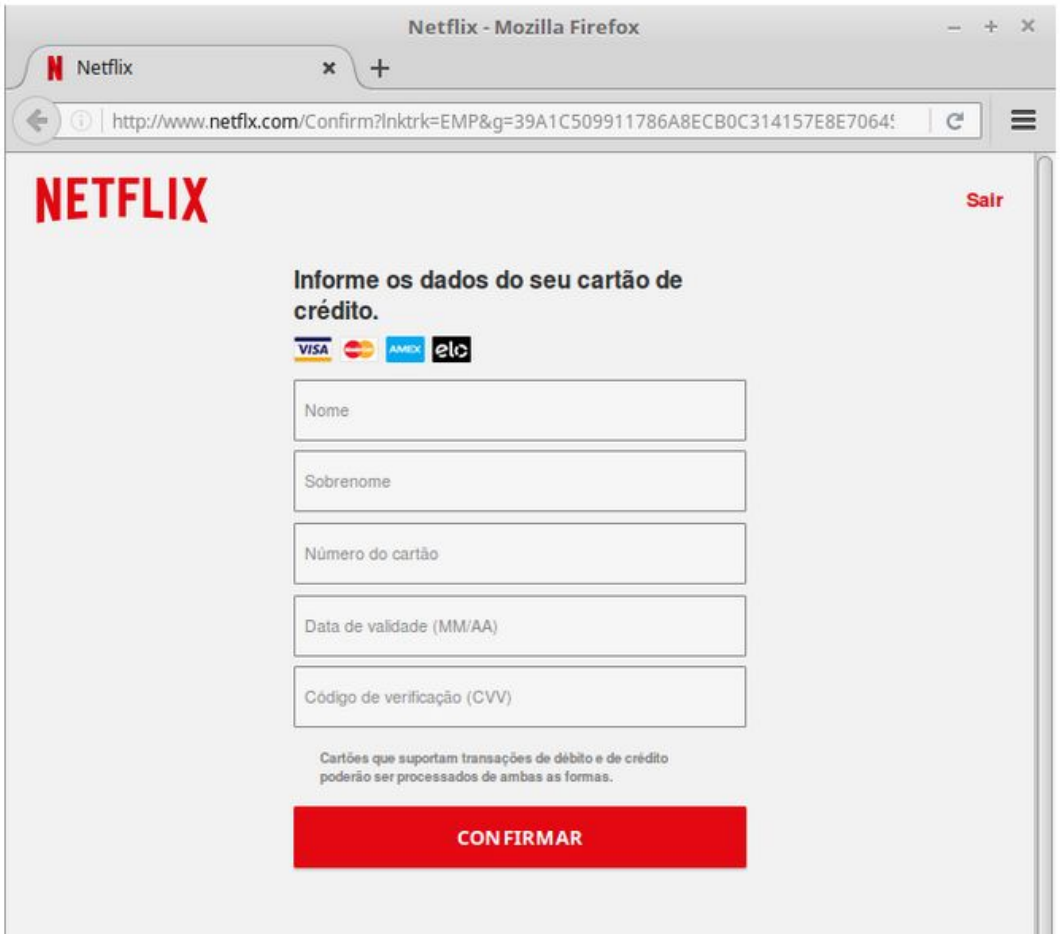
Estamos sempre prontos para ajudar. Acesse o Centro de ajuda para saber mais ou fale com a gente.

–Equipe Netflix



- ◯ Responderia o e-mail
- ◯ Encaminharia o e-mail
- ◯ Apenas leria a mensagem e a deixaria em sua caixa de entrada
- ◯ Deletaria o e-mail
- ◯ Clicaria no link do e-mail
- ◯ Digitaria ou copiaria a URL no navegador

Dado que tenha acessado a página do link, qual ação tomaria? *



- ◯ Preencheria com seus dados
- ◯ Entraria em contato por telefone
- ◯ Verificaria direto da conta

Referências

[1] [Infográfico] – História dos principais ataques de Phishing. Disponível em: <https://www.elpescador.com.br/blog/index.php/infografico-historia-dos-principais-ataques-de-phishing/>. Acesso em: 3 out. 2017.

[2] **20 Eye-Opening Cybercrime Statistics**. Security Intelligence. Disponível em: <https://securityintelligence.com/20-eye-opening-cybercrime-statistics/>. Acesso em: 11 nov. 2017.

[3] **The Attack Cycle**. Security Through Education. Disponível em: <https://www.social-engineer.org/framework/attack-vectors/attack-cycle/>. Acesso em: 7 out. 2017.

[4] AVELLAR E DUARTE - CLAUDIA DUARTE. **Internet no Brasil 2017 (estatísticas)**. Avellar e Duarte. Disponível em: <http://www.avellareduarte.com.br/fases-projetos/conceituacao/demandas-do-publico/pesquisas-de-usuarios-atividades-2/dados-sobre-o-publico-alvo/internet-no-brasil-2017-estatisticas/>. Acesso em: 1 out. 2017.

[5] **Baixe o guia completo sobre ataques de phishing.** El Pescador - Ebook. Disponível em: <https://www.elpescador.com.br/ebook/>. Acesso em: 1 out. 2017.

[6] BAUNFIRE.COM, SparkCMS by. **APWG Phishing Attack Trends Reports**. APWG Reports | APWG. Disponível em: <https://www.antiphishing.org/resources/apwg-reports/>. Acesso em: 14 out. 2017.

[7] **CERT.br Stats (janeiro a dezembro de 2016)**. CERT.br. Disponível em:

<https://www.cert.br/stats/incidentes/2016-jan-dec/tipos-ataque.html>. Acesso em: 1 out. 2017.

[8] CERT.BR. **Cartilha de Segurança -- Golpes na Internet**. Cartilha de Segurança para Internet. Disponível em: <https://cartilha.cert.br/golpes>. Acesso em: 4 nov. 2017.

[9] DARYA GUDKOVA, MARIA VERGELIS, NADEZHDA DEMIDOVA, TATYANA SHCHERBAKOVA ON FEBRUARY 20, 2017. 10:57 AM. **Spam and phishing in 2016**. Securelist - Information about Viruses, Hackers and Spam. Disponível em: <https://securelist.com/kaspersky-security-bulletin-spam-and-phishing-in-2016/77483/>. Acesso em: 4 nov. 2017.

[10] DARYA GUDKOVA, MARIA VERGELIS, NADEZHDA DEMIDOVA, TATYANA SHCHERBAKOVA ON MAY 2, 2017. 8:57 AM. **Spam and phishing in Q1 2017**. Securelist - Information about Viruses, Hackers and Spam. Disponível em: <https://securelist.com/spam-and-phishing-in-q1-2017/78221/>. Acesso em: 4 nov. 2017.

[11] DHAMIJA, Rachna; TYGAR, J. D. and HEARST, Marti. Why phishing works. **Proceedings of the SIGCHI conference on Human Factors in computing systems - CHI '06**, 2006.

[12] **Digital in 2017: Global Overview**. We Are Social. Disponível em: <https://wearesocial.com/special-reports/digital-in-2017-global-overview>. Acesso em: 30 set. 2017.

[13] DOWNS, Julie S.; HOLBROOK, Mandy and CRANOR, Lorrie Faith. Behavioral response to phishing risk. **Proceedings of the anti-phishing working groups**

2nd annual eCrime researchers summit on - eCrime '07, 2007.

[14] EDITOR, By: Sophos News. Disponível em: <https://news.sophos.com/en-us/2016/12/14/consumers-fear-a-cyberattack-over-a-physical-attack-but-what-are-they-doing-about-it/> Acesso em: 24 nov. 2017

[15] **Estatísticas do CERT.br -- Incidentes**. CERT.br. Disponível em: <https://www.cert.br/stats/incidentes/>. Acesso em: 4 nov. 2017.

[16] FELIX, Jerry; HAUCK, Chris. **System Security: A Hacker's Perspective**. 1987 Interex Proceedings. Acesso em: 14 nov. 2017.

[17] FINN, Peter and JAKOBSSON, Markus. Designing ethical phishing experiments. **IEEE Technology and Society Magazine**, vol. 26, no. 1, p. 46–58, 2007. Acesso em: 1 out. 2017.

[18] GIDDENS, Anthony. **The consequences of modernity**. [s.l.]: Polity Press, 2015.

[19] HALDER, Debarati and JAISHANKAR, K. **Cyber crime and the victimization of women: laws, rights and regulations**. [s.l.]: Information Science Reference, 2011.

[20] **IBM's CEO on hackers:** IBM Digital Nordic. Disponível em: <https://www.ibm.com/blogs/nordic-msp/ibms-ceo-on-hackers-cyber-crime-is-the-greatest-threat-to-every-company-in-the-world/>. Acesso em: 15 nov. 2017.

[21] JAGATIC, Tom N.; JOHNSON, Nathaniel A.; JAKOBSSON, Markus; *et al.* Social phishing. **Communications of the ACM**, vol. 50, no. 10, p. 94–100, 2007.

[22] KIZZA, Joseph Migga. **Guide to Computer Network Security**. [s.l.]: Springer-Verlag, 2015.

[23] KOYUN, Arif; JANABI, Ehssan Al. Social engineering attacks. **Journal of multidisciplinary engineering science and technology (jmest)**

[24] **Language Log**. Language Log: Phishing. Disponível em: <http://itre.cis.upenn.edu/myl/languagelog/archives/001477.html>. Acesso em: 7 out. 2017.

[25] OWASP. **OWASP Top 10 2017**. Disponível em: <https://www.owasp.org/images/b/b0/OWASP_Top_10_2017_RC2_Final.pdf>. Acesso em: 23 nov. 2017.

[26] **Phishing Activity Trend Report 2016 APWG**. Disponível em: <https://docs.apwg.org/reports/apwg_trends_report_q4_2016.pdf> Acesso em: 4 nov. 2017.

[27] **Phishing Activity Trend Report H1 2017 APWG**. Disponível em: <http://docs.apwg.org/reports/apwg_trends_report_h1_2017.pdf> Acesso em: 4 nov. 2017.

[28] **PhishTank > What is phishing? (definition of phishing, with examples)**. PhishTank - Out of the Net, Into the Tank. Disponível em: <https://www.phishtank.com/what_is_phishing.php>. Acesso em: 5 nov. 2017.

[29] REIS, Miguel and JOIA, Isabelle. **Ataques de Engenharia Social: tudo que você precisa saber!** PROOF. Disponível em: <http://www.proof.com.br/blog/ataques-de-engenharia-social/>. Acesso em: 28 out. 2017.

[30] **Schneier on Security**. Blog. Disponível em: <https://www.schneier.com/crypto-gram/archives/2000/1015.html>. Acesso em: 21 out. 2017.

[31] SHENG, Steve; HOLBROOK, Mandy; KUMARAGURU, Ponnurangam; *et al.* Who falls for phish? **Proceedings of the 28th international conference on Human factors in computing systems - CHI '10**, 2010.

[32] SILVA, Edna Lúcia Da; MENEZES, Estera Muszkat. **Metodologia da pesquisa e elaboração de dissertação/**. 4 ed. Florianópolis: UFSC, 2005.

[33] SOCIAL-ENGINEER. **2017 Verizon DBIR Social Engineering Breakdown**. Social-Engineer.Com - Professional Social Engineering Training and Services. Disponível em: <https://www.social-engineer.com/2017-verizon-dbir-social-engineering-breakdown/>. Acesso em: 28 out. 2017.

[34] GRANGER, Sarah. Social Engineering Fundamentals, Part I: Hacker Tactics | **Symantec Connect**. Disponível em: <https://www.symantec.com/connect/articles/social-engineering-fundamentals-part-i-hacker-tactics>. Acesso em: 28 out. 2017.

[35] TRAINING, Focus; OLSON, Chris; ROOSENRAAD, Chris; *et al.* **The Secret History of Cyber Crime**. Information Security Buzz. Disponível em: <http://www.informationsecuritybuzz.com/articles/the-secret-history-of-cyber-crime/>. Acesso em: 18 out. 2017.

[36] UNION, International Telecommunication. **Understanding cybercrime**: A guide for developing countries. [S.L.: s.n.], 2009.

[37] **What is Information Technology (IT)? - Definition from Whatls.com**. SearchDataCenter. Disponível em: <http://searchdatacenter.techtarget.com/definition/IT>. Acesso em: 25 nov. 2017

[38] **Where Does Cyber Crime Come From? History of Cyber Crime**. Le VPN. Disponível em: <https://www.le-vpn.com/history-cyber-crime-origin-evolution/>. Acesso em: 18 out. 2017.

[39] WOODWARD, Prof Alan. **Viewpoint: How hackers exploit 'the seven deadly sins'**. BBC News. Disponível em: <http://www.bbc.com/news/technology-20717773>. Acesso em: 11 nov. 2017.

[40] ZETLIN, Minda. **Highly Successful Netflix Scam Fools Even Sophisticated Users--and Security Software**. Inc.com. Disponível em: <https://www.inc.com/minda-zetlin/highly-successful-netflix-scam-fools-even-sophisticated-users-and-security-software.html>. Acesso em: 11 nov. 2017.