UNIVERSIDADE ESTADUAL DO NORTE DO PARANÁ

***CAMPUS* LUIZ MENEGHEL**

DAYANNE OLIVEIRA DA SILVA

IDENTIFICAÇÃO DO PERFIL DAS VÍTIMAS DE *PHISHING* NA UNIVERSIDADE ESTADUAL DO NORTE DO PARANÁ (UENP)

Bandeirantes

2014

DAYANNE OLIVEIRA DA SILVA

IDENTIFICAÇÃO DO PERFIL DAS VÍTIMAS DE *PHISHING* NA UNIVERSIDADE ESTADUAL DO NORTE DO PARANÁ (UENP)

Monografia apresentada à Universidade Estadual do Norte do Paraná – *campus* Luiz Meneghel – como requisíto parcial para a obtenção do grau de Bacharel em Sistemas de Informação.

Orientador: Fábio de Sordi Júnior

Bandeirantes

2014

DAYANNE OLIVEIRA DA SILVA

IDENTIFICAÇÃO DO PERFIL DAS VÍTIMAS DE *PHISHING* NA UNIVERSIDADE ESTADUAL DO NORTE DO PARANÁ (UENP)

Monografia apresentada à Universidade Estadual do Norte do Paraná – *campus* Luiz Meneghel – como requisíto parcial para a obtenção do grau de Bacharel em Sistemas de Informação.

COMISSÃO EXAMINADORA

_____
Prof. Fábio de Sordi Júnior
UENP – *Campus* Luiz Meneghel

_____
Prof. Ricardo Gonçalves Coelho
UENP – *Campus* Luiz Meneghel

_____
Prof.Luiz Fernando Legore do Nascimento
UENP – *Campus* Luiz Meneghel

Bandeirantes, 07 de julho de 2014.

Dedico este trabalho aos meus pais e as minhas irmãs que me apoiaram em todos os momentos.

AGRADECIMENTOS

Agradeço a Deus em primeiro lugar, pois sem ele nada seria possível; Aos meus pais que incentivam cada escolha que faço; Aos meus amigos queridos que estiveram ao meu lado nas alegrias e tristezas; As minhas irmãs Fabiane, Patrícia e Beatriz por tornar meus dias mais felizes mesmo que longe; Ao professor Fábio De Sordi Júnior pela paciência que sempre teve comigo e ao Professor Fernando Legore do Nascimento por todo o apoio que me dedicou principalmente na fase final de minha graduação.

A persistência é o caminho do êxito.
Charles Chaplin.

RESUMO

Este trabalho identificou as vítimas de engenharia social *online*, em uma amostra de universitários. A engenharia utilizada foi uma fraude denominada *Phishing*, a qual vem aumentando significativamente nos últimos anos, mas muitos dos usuários da Internet ainda não conseguem reconhecê-la e acabam por se tornarem vítimas. A pesquisa usou um método de *Phishing* por meio de correio eletrônico contendo um falso *link* para alcançar os objetivos, tornando assim possível reconhecer os diferentes perfis das vítimas.

Palavras-chave: Engenharia social, fraude, *Phishing*.

ABSTRACT

This paper identified the victims of social engineering online in a sample of university students. The engineering used was a fraud known as Phishing, which has been growing significantly in recent years, but many internet users are still unable to recognize it and end up becoming victims. The research used a Phishing method by email containing a false link to reach the goals, this making it possible to recognize the different profiles of the victims.

Keywords: Social engineering, fraud, Phishing.

LISTA DE GRÁFICOS

Lista de Figuras

Lista de Tabelas

LISTA DE SIGLAS

APWG	- *Anti-Phishing Working Group*
CERT	- Centro de Estudos, Resposta e Tratamento.
DNS	- Sistema de Nomes de Domínio
HTML	- Linguagem de Marcação de Hipertexto
IBRAMERC	- Instituto Brasileiro de Inteligência de Mercado
MIS	- Movimento Internet Segura
RNP	- Rede Nacional de Ensino e Pesquisa
SMS	- Serviço de Mensagem Curta
UENP	- Universidade Estadual do Norte do Paraná
UTPE	- Universidade Federal de Pernambuco

SUMÁRIO

1 INTRODUÇÃO

Este Capítulo divide-se em cinco Seções com propósito de apresentar o trabalho. Na Seção 1.1 pretende-se contextualizar a pesquisa. Na Seção 1.2 enuncia-se o problema que motivou o trabalho. Na Seção 1.3 encontra-se a justificativa. Na Seção 1.4 são apresentados os objetivos que foram definidos contendo na subseção 1.4.1 os objetivos gerais e na subseção 1.4.2 os objetivos específicos. Na Seção 1.5 é descrita a organização do trabalho.

1.1 CONTEXTUALIZAÇÃO

A popularidade da comunicação pela I*nternet* tem aumentado consideravelmente nos últimos anos, o que trouxe benefícios para seus usuários como redução de tempo para conversação, comodidade e praticidade.

Juntamente com as vantagens incontestáveis surgiram também grandes ameaças de segurança.

As fraudes para obtenção de informações pessoais e corporativas via *e-mail* e rede social, estão cada vez mais frequentes. Segundo pesquisa realizada pelo Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br, 2013) corresponde a 64% das tentativas de fraudes notificadas.

Dentre muitos tipos de ataques cibernéticos, o *Phishing* tem ganho destaque, por utilizar indevidamente em uma de suas formas de atuação nomes de instituições conceituadas e conhecidas pelo público para aplicar golpes *online* (CALLAN, 2010).

O *Phishing* traz mensagens para o destinatário com *links* para páginas fictícias, que quando acessadas solicitam ao usuário inserção de dados pessoais e até bancários, estes quando fornecidos podem não aparentar agravo a primeiro momento, mas provavelmente acarretarão sérios prejuízos a vítima (FABENY apud BONFIETTI, 2007).

Segundo a Kaspersky (2013), no ano de 2013 houve um aumento de 87% nos casos *Phishing*, o Brasil ocupa a 4ª posição no *ranking* mundial em ataques. *E*stes números acabam por crescer graças a constante procura por serviços *online*, deixando os usuários mais vulneráveis.

Em pesquisa realizada pelo *Online Identify Risk Calculator*,(2013), os serviços bancários *online* são acessados por 67% do público analisado com uma regularidade mensal, e costumam realizar compras em *sites pelo menos 83% deste população.*

De acordo com Gastão Matos, integrante do Movimento *Internet* Segura (MIS), a ocorrência dessa ameaça coloca em risco a credibilidade da organização perante seus clientes.

Conforme relatório *Phishing ActivityTrendsReport* (2013), organizações financeiras e serviços de pagamento são os alvos principais das mensagens maliciosas as quais são enviadas às vítimas via correio eletrônico e redes sociais.

1.2 FORMULAÇÃO E ESCOPO DE PROBLEMA

A obtenção de ferramentas e programas capazes de detectar *Phishing* não é a solução completa para extinguir o perigo de roubo de dados, pois de acordo com Marcelo e Azevedo (2005), as pessoas são as principais responsáveis por permitir acesso as informações.

Entre usuários de correio eletrônico e redes sociais 63% não conseguem reconhecer uma mensagem falsa, conforme estudo feito pela Kaspersky (2012). As fraudes estão mais elaboradas, detalhadas, o que pode passar despercebido pela percepção do usuário sem uma observação mais criteriosa do conteúdo recebido.

Segundo pesquisa realizada pela *Check Point* (2011), em corporações os profissionais predisposto a serem potenciais vítimas representam 23% do pessoal da Tecnologia da Informação, 32% são lideres de negócios, 33% recursos humanos, 38% assistentes executivos e não há prevenção sobre técnicas de fraudes.

Profissionais de Tecnologia da Informação que deveriam possuir um conhecimento mais profundo sobre ataques *online* também estão suscetíveis em grande número à engenharia social por não conseguirem identificar a fraude (WEBSENSE, 2013).

1.3 JUSTIFICATIVA

A presente pesquisa justifica-se pela necessidade de identificar a descrição das possíveis vitimas de *Phishing* na Universidade Estadual do Norte do Paraná. A análise do perfil visa possibilitar uma futura elaboração de treinamento especifico para os usuários mais suscetíveis a sofrer com esse crime.

A identificação proporcionará encontrar uma correlação entre as reais vítimas de *Phishing.* Analisar a faixa etária, gênero, curso universitário para identificar possíveis diferenças.

Segundo o Deputado Federal Eduardo Azeredo, autor do Projeto para caracterizar *Phishing* como crime de estelionato (2013), as pessoas são vítimas desse tipo de fraude por falta de informação sobre o assunto, isto é não conhecem seu modo de atuação, o que influencia no crescimento desses incidentes.

*"*Pessoas devem estar cientes dos perigos do mundo virtual e da importância da segurança da informação, fazendo necessários treinamentos específicos para combater os ataques*"*, de acordo com Rogério Morais, vice-presidente da empresa de segurança RSA América Latina.

Pessoas novas em determinados ambientes representam uma maior chance de serem enganadas por fraudadores. Segundo Mitnick,(2006), não adianta os investimentos fortes em recursos de segurança, pois se apenas uma pessoa que possui acesso a dados for enganada de nada valerá as ferramentas de proteção.

Entender os fatores humanos que tornam as pessoas vulneráveis a criminosos *online* podem melhorar tanto o treinamento de segurança quanto o de tecnologia (CRANOR, 2008).

1.4 Objetivos

1.1.1 Objetivo geral

Reconhecer o perfil dos usuários vítimas de *Phishing*, que estudam na Universidade Estadual do Norte do Paraná (UENP – campus Luiz Meneghel).

1.1.2 Objetivos específicos

- Enviar mensagem eletrônica contendo *link* para o preenchimento de um formulário, com o tópico atualização de cadastro para todos os acadêmicos;
- Identificar possíveis diferenças entre os acadêmicos dos cursos oferecidos na Universidade em relação ao um ataque de *Phishing*;
- Constatar uma possível distinção na reação entre os gêneros dos alunos e faixa etária, perante uma engenharia social.

1.5 ORGANIZAÇÃO DO TRABALHO

O trabalho divide-se da seguinte forma: No Capítulo 2 é apresentado os conceitos de Segurança da Informação, Engenharia Social, Correio Eletrônico e Redes Sociais e Ataques e golpes na *Internet* e o *Phishing.*

A seguir, no capítulo 3 é apresentado o método seguido para o desenvolvimento do trabalho. Posteriormente, o Capítulo 4 contém o desenvolvimento do Trabalho, com a descriminação dos dados coletados, e por final, no Capítulo 5 é realizada a conclusão do Trabalho.

2 FUNDAMENTAÇÃO TEÓRICA

Este Capítulo divide-se em quatro Seções. Na Seção 2.1 será tratada a importância da Segurança da Informação. Na Seção 2.2 é abordada a Engenharia Social. Na subseção 2.2.1. é descrito o uso do correio eletrônico e das redes sociais, seguida da subseção 2.2.2 identificando os tipos de ataques e golpes na *internet.* Na subseção 2.3 é tratado o *Phishing.*

2.1 SEGURANÇA DA INFORMAÇÃO

Um dos fatores essências para o desenvolvimento e crescimento da sociedade em ritmo mais acelerado é a informação, que possui valores diferenciados para cada pessoa tornou-se parte importante no ambiente de negócios (DANTAS, 2011).

“A informação pode se expandir, ser completada, é capaz de ser substituída, transportável, difusa e pode ser compartilhada”. (Tarapanoff, Júnior e Cormier, 2000).

Segundo Carvalho (2011), a informação ocorre por meio de pessoas, seja de forma escrita, verbal ou qualquer outra maneira utilizada para propaga-la, é considerada tudo que tem relevância para um individuo ou para uma empresa.

Pessoas físicas ou grandes corporações estão sujeitos a sofrer invasões de dados importantes, o que pode acarretar prejuízos significativos, como exemplo, perdas financeiras e de registros (SILVA e STEIN, 2007 apud SIEBERG, 2005).

Os dados pessoais possuem alto valor para um indivíduo e são alvos constantes de ataques, que visam conseguir senhas, endereços, utilizar cartões de crédito das vítimas para realizar compras e operações bancárias.

A segurança da informação objetiva a proteção contra acessos sem consentimento, à preservação de dados, completude e defesa contra qualquer tipo de vulnerabilidade que a ameace (SILVA e STEIN, 2007 apud SIEBERG, 2005).

A vulnerabilidade é motivada por diversos elementos, incluindo armazenamento inapropriado e recursos humanos. As ameaças são formas de explorar as vulnerabilidades ocasionando estragos e extravios de informações (DANTAS, 2011).

Para Zapater e Suzuki (2005), a segurança da informação deve assegurar requisitos como:

- Integridade: visa certificar que as propriedades dos dados serão mantidas e não alteradas sem permissão;
- Confidencialidade: garante que apenas pessoas com autorização possam ter acesso aos dados;
- Disponibilidade: os dados devem estar acessíveis aos autenticados sempre que necessário;
- Autenticidade: assegura ao usuário a confirmação da origem da informação, para impedir intrusos, distingui os autorizados.
- Não repúdio: impossibilita que a autoria de determinada mensagem seja negada.

Na Figura 1 são apresentados os princípios essências para atingir o propósito da segurança da informação.

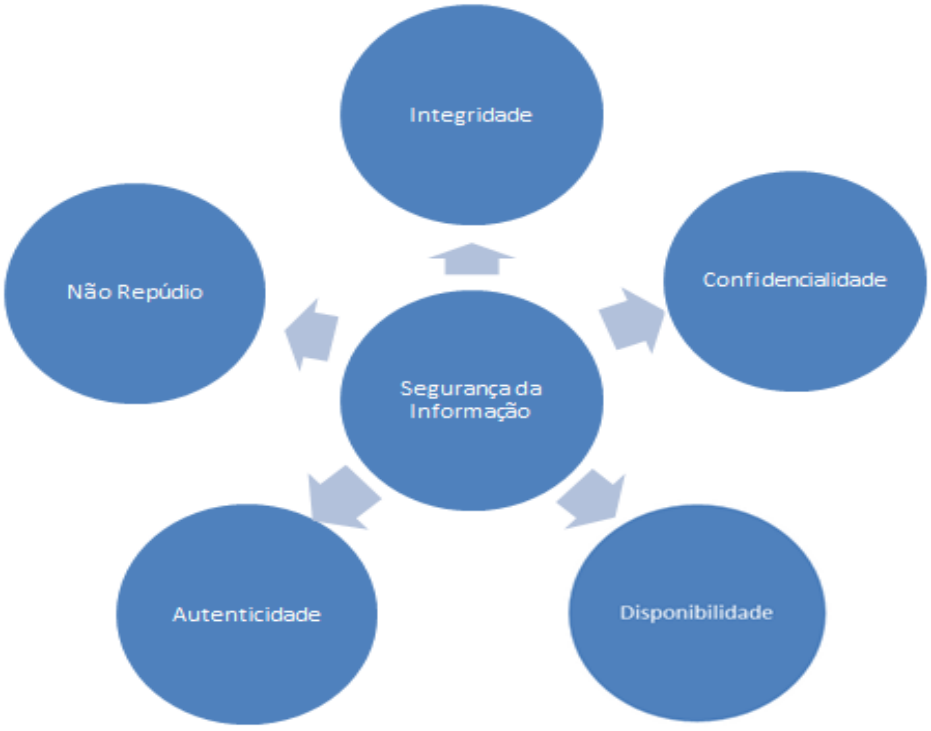

Figura 1: Princípios da Segurança da Informação
Fonte: Zapater e Suzuki (2005).

Pessoas, processos e ferramentas devem ser trabalhados para garantir a restrições de informações. As ferramentas responsáveis pela legitimidade do acesso, quais usuários são permitidos à determinada parte do sistema, por meio de autenticação preestabelecida.

Os processos são os métodos para a segurança, registro de monitoramento. As pessoas executam as ferramentas e os processos, dependendo delas o sucesso do funcionamento. (ZAPATER e SUZUKI, 2005).

Para Santo (s/d), o maior recurso para a segurança da informação são os seres humanos, pois operam o sistema que armazenam os conjuntos de dados. Nesse caso, a necessidade da conscientização sobre a importância em mantê-las protegidas, a fim de evitar que sejam dispersas.

Fonseca (2009) enfatiza que o usuário deve ter conhecimento sobre os tipos de informação que dispõe podendo ser ela pública na qual sua distribuição não acarreta danos ou confidenciais, bem como o número de documentos pessoais, que identificam um cidadão e são intransferíveis.

Para um cuidado frequente na proteção das informações é preciso que as pessoas mantenham-se atualizadas em relação às técnicas de engenharia social sejam elas virtuais ou não. Em muitos casos o ataque atinge sucesso por desatenção da vítima (MARCELO e PEREIRA, 2005).

2.2 ENGENHARIA SOCIAL

A engenharia social é a união de métodos praticados para conseguir ter acesso a informações relevantes, seja de pessoas físicas ou de empresas. Aplicação de meios ilícitos para adquirir informações aproveitando-se da confiança das pessoas (ALVES, 2010).

A atuação de um engenheiro social pode-se dar de formas distintas, em ambientes de lazer, de trabalho, ligação telefônica requisitando dados com identificação falsificada, mensagens por *e-mail* e redes sociais.

> Engenharia social usa a influência e a persuasão para enganar as pessoas e convencê-las de que o engenheiro social é alguém que ele não é, ou pela manipulação. Como resultado, o engenheiro social pode aproveitar-se das pessoas para obter as informações com ou sem uso da tecnologia. (MITNICK e SIMON, 2003).

Muitas das vezes as vítimas não tomam consciência que foram ou estão sendo usadas para fornecer dados que serão empregados contra elas. A ingenuidade e o formato de abordagem da fraude não permitem que percebam características de crime (Marcelo e Pereira, 2005).

O engenheiro social cria situações para controlar s eus abordados e levá-los a efetuarem ações que o ajude a chegar a seu objetivo ou fornecerem informações importantes que tragam benefícios ao fraudador.

De acordo com Cavalcanti (2012) os engenheiros sociais usam de abordagens que podem afetar o psicológico, o financeiro e a vida social de suas vítimas, desempenham personagens conforme a área que pretendem obter informações.

Expressam formas de tirar vantagens de conversas por meio de solicitações que a princípio não demostram interesses que possam ser preocupantes. Agem de modo solícito, com disposição a ajudar, manipulam as pessoas ardilosamente, conforme apresentado por (MITNICK e SIMON, 2006).

Segundo Marcelo e Pereira (2005) com foco no intuito de ter acesso a dados pessoais, empresariais e bancários, os fraudadores tendem a utilizar a seu favor fatores comportamentais das suas vítimas em potencial. Reproduzindo em si o modelo de comportamento que transmita credibilidade e confiança.

Silva (2012) define que aberturas comportamentais, como fragilidade emocional levam as pessoas a um risco maior de serem manipuladas, assim como vontade de demostrar eficiência, conhecimento e ou excesso de confiança.

A fraude é focada nos erros, desatenção e falta de discernimento humano, o que não é específico de máquinas. Para ter um desfecho satisfatório ao fraudador é preciso que a vítima o conceda as informações voluntariamente sem saber as reais condições que esta compartilhando seus dados, ou involuntariamente em caso de arquivos e programas maliciosos instalados em seus dispositivos.

Atualmente com o maior acesso as informações que podem ajudar as pessoas a se protegerem desse tipo de crime, supõem-se que seja praticamente impossível ser alvo dos engenheiros sociais, e que seus métodos seriam obsoletos para os dias modernos.

Guimarães e Júnior (2012) destacam os tipos de fraudes efetuadas:

- Pessoas desaparecidas: Objetiva obter da vítima uma lista de *e-mails* verdadeiros, ao clicar para conferir a notícia, a vítima passar a oferecer uma abertura para o criminoso;
- Fraudes Bancárias: Envio de mensagens para os usuários com *links* para páginas fictícias requisitando dados pessoais e bancários;

- Esquema de Ponzi: São feitos investimentos pela vítima considerado seguro, onde deve atrair mais pessoas a participar destes investimentos;
- Boatos: Falsos prêmios, brindes, pedido de ajuda a instituições filantrópicas, dentre outras;
- Envelope vazio: Envolve instituições bancárias, geralmente quando as agências estão período de recesso. O golpista realiza a negociação com comprovante de depósito em caixa eletrônico, onde na verdade não houve a transação;
- Análise do lixo: Documentos ou anotações descartados sem verificação da importância de seu conteúdo são alvos dos engenheiros sociais que coletam dados úteis para um futuro ataque.

Nas organizações, senhas, topologia de rede, sistema operacional e sua versão, nome de *hosts,* descrição de produtos, dados dos clientes, dentre outras, são alvos do interesse de pessoas que não possuem autorização para acessar estas informações (CERT, 2003).

Frank Abagnale Jr. (2014) sugere algumas ações para diminuir a vulnerabilidade em relação às fraudes:

1. Destruir documentos que contenham nome, endereço ou qualquer informação pessoal;
2. Monitoramento constante de cartões;
3. Evitar usar cheques;
4. Evitar uso de cartão de débito, para impedir acesso à conta bancária;
5. Controlar a exposição de dados pessoais nas redes sociais mesmo que parecem a primeiro momento inofensivo, como data de nascimento e cidade que reside, pois a divulgação destes torna a pessoa 98% mais suscetível.

Os fraudadores estão inovando em suas formas de procedimentos cada vez mais elaborados, em concordância com o ritmo dos avanços tecnológicos.

Na pesquisa realizada pela *Check Point Software Technologies* (2011), as fontes mais comuns de engenharia social *online* são *e-mails* contendo *Phishing* os quais representam 47% das ameaças, seguido pelas Redes Sociais com 39%.

2.2.1 Correio eletrônico e Redes Sociais

As ferramentas sociais na *Internet* ajudam o ser humano a suprir sua necessidade de interagir, fazer amizades, estabelecer um relacionamento de afeição com pessoas próximas ou mesmo as distantes fisicamente. Permitem compartilhar suas novidades e expressar opiniões, segundo Recuero (2009).

A primeira aplicação a surgir para auxiliar na comunicação por meio de mensagens transmitidas por computador foi o Correio Eletrônico aumentando a agilidade de envio e resposta de informações, de acordo com Santos (2007).

O *Hotmail* foi um dos primeiros correios eletrônicos gratuitos*,* onde o cliente poderia acessá-lo usando qualquer computador, em ambientes distintos com conexão a *internet*. O nome *HoTMaiL*, destaca o fato do Linguagem de Marcação de Hipertexto (HTML) ser usado na interface *WEB*.

Instrumento utilizado para manter contato com um grande número de pessoas se necessário, em um curto período de tempo, sem gastos para manter a comunicação, ou com baixo custo no caso de *e-mail* corporativo ainda conforme Santos (2007).

Com o passar dos anos houve o surgimento de outros grandes serviços de contas de *e-mail*, oferecendo aos usuários a possibilidade de escolher entre eles o que garanta o suprimento de sua conveniência.

Nas mensagens transmitidas é possível enviar anexos contendo imagens, fotos e documentos de textos, variando o tempo de carregamento dependendo da velocidade da *Internet*. A capacidade de espaço aumentou com o tempo, devido às necessidades dos usuários (KARANSINSKI, 2009).

O correio eletrônico é um dos serviços utilizados para manter a comunicação no ambiente acadêmico, garantindo o envio e resposta de informações entre discentes, docentes e pesquisadores.

Ao aproveitar dos benefícios que empregar esta ferramenta no ambiente corporativo, as organizações acabam ficando vulneráveis as invasões para obtenção de informações sigilosas e propensas a vírus que podem comprometer toda a rede, de acordo com Bernardinelli (2009).

O correio eletrônico também serve para o envio de mensagens contendo publicidade, *conhecido como E-mail Marketing,* ele é direcionado em nome de

empresas que oferecem serviços e produtos, com ou sem o consentimento do receptor (ZUINI, 2014).

As redes sociais também são alvos para exibir propagandas, aproveitando o aumento de seu público e as vantagens que a ferramenta proporciona. No Brasil 73% da população com acesso a *internet, possui* uma conta em alguma das mais populares plataformas (CAPUTO, 2014).

O sucesso das redes sociais reflete até mesmo nas empresas, 88% das organizações nacionais aderiram a alguma rede social em prol dos negócios, buscando maior visibilidade e almejando a expansão das conquistas empresariais (LATIN AMERICA SOCIAL MEDIA CHECK-UP, 2012).

Pessoas procuram ter contato com empresas que forneçam mercadorias ou serviços, para solucionar dúvidas, oferecer sugestões, criticar, elogiar, por estes fatores as empresas empregam algum tipo de serviço *online*, segundo o Instituto Brasileiro de Inteligência de Mercado (IBRAMERC, 2012).

A quantidade numerosa de usuários faz das redes sociais alvo de ataques cibernéticos em ritmo crescente, impulsionados pelas informações divulgadas no perfil destes usuários e visualização de mensagens fraudulentas por acreditar ser de um amigo confiável (INTERNET SECURITY THREAT REPORT, 2013).

Os golpes mais comuns nas redes sociais são promoções, jogos e testes, notícias inverídicas, curtidas arriscadas e extensões maliciosas (CAPUTO, 2014).

2.2.2 Ataques e golpes na *internet*

Ataque é uma ameaça proposital, planejada com o objetivo específico de obter informações restritas para serem negociadas pelo fraudador. Dessa forma ele poderá interferir na rede, modificar ou desviar documentos, capturar dados bancários para movimentação de contas, entre outros, conforme Pinheiro (2007).

Segundo o Kioskea (2014), um ataque visa explorar aberturas, erros nos sistemas e tirar proveito por meio de intercepção de mensagens, fraudar identidade, interromper serviços e fazer a contaminação com intrusos.

A Kaspersky (2014) descreve as características de alguns ataques:

- Cavalo de Tróia: Encontra-se em *sites* na *Internet*, incorporados a uma mensagem do correio eletrônico e em compartilhamento de arquivo. Para

atuar ele precisa ser executado explicitamente no computador hospedeiro. Em sua ação, elimina ou altera arquivos. O agressor passar a ter domínio da máquina;

- Vírus: Altera ou elimina os documentos contidos no computador e pode realizar cópias de si mesmo. Para estabelecer-se precisa ser executado no computador. Podem ser encontrados em *sites*, mensagens eletrônicas, redes sociais, ao realizar *downloads*, compartilhar arquivos e inserção de discos removíveis contaminados.
- *Worm*: Explora as vulnerabilidades da máquina, é transmitido por envio de mensagens no correio eletrônico, ação de códigos maliciosos, baixado de *sites* na *Internet,* mensagens instantâneas. Lança ataques *online e* instala códigos maliciosos.
- Spam: São mensagens não solicitadas, com conteúdos falsos, de imoralidades, publicidades, ofertas fictícias de emprego dentre outros. Ocorre o envio de mensagens com remetente falsificado, para aumentar a chance de ser aberto e não ser detectado pelo filtro.
- Spyware: Software recebido por mensagens eletrônicas, redes sociais, compartilhamento de mídias removíveis e arquivos, baixado de *sites*, rouba informações e mantem-se escondido.

Existem outros tipos de ataques como o *Backdoor* e *Rootki*t que são inseridos por um invasor, explora as vulnerabilidades e não multiplicam-se*. Rootkit* pode remover os arquivos existentes.

O *Scam* (golpe), são mensagens contendo produtos em oferta, propaganda de viagens, requisitando que o usuário preencha formulários, coletando assim informações e resultando no roubo destes dados.

> *"As mensagens que escondem o* scam *tem características próprias de instituições financeiras, sítios de cartões de mensagem, notificações de órgãos públicos, notícias de destaque,* downloads *de programas, promoções e eventos, temas pornográficos e mensagens pessoais, sempre com o intuito de deixar as vítimas curiosas ou instigadas" (MOURA, 2012).*

Os fraudadores abusam da vulnerabilidade dos usuários para ter acessos às informações que precisam. Os golpes mais comuns são os conhecidos *Hoax*, Furto

de identidade, golpes em *site* de compras coletivas e de comércio eletrônico (KASPERSKY, 2014).

- *Hoax*: São boatos enviados por mensagem eletrônica, oculta-se por traz de organizações governamentais e filantrópicas para garantir confiança ao remetente da mensagem e contém códigos perversos. Muitas vezes abusa de supostas tragédias para chamar a atenção das vítimas.
- Furto de Identidade: Os dados pessoais e bancários são roubados e os estelionatários usam destes dados coletados para cometer crimes em nome da vítima. Podem-se realizar compras, abrir empresas, realizar transações usando dos documentos furtados.
- Golpes em *site* de compras coletivas e de comércio eletrônico: São enviadas mensagens contendo *link* para supostas páginas de compras com preços atraentes e período de promoção limitado, estimulando o usuário a adquirir seus produtos. Em *sites* de comprar coletivas é uma oportunidade de conseguir um grande número de vítimas em um curto espaço de tempo.
- *Pharming*: Por meio de adulteração dos Sistema de Nomes de Domínio (DNS), ocorre o redirecionamento da página de navegação, ao tentar visitar um *website* o usuário é conduzido a outra página. Neste ambiente inseguro pode haver a tentativa de instalação de programas desnecessários e ou execução de arquivos. A segurança da conexão deve ser conferida principalmente em locais que necessitem de entrada com *login*.

O golpe em comércio eletrônico cresce de acordo com o aumento da popularidade de *sites* de compras e a quantidade de acessos. Os fraudadores preferem obter recursos abstratos, que não necessitem fornecer endereço para entrega, como jogos *online* por exemplo.

Páginas falsificadas representam um número expressivo das fraudes que são notificadas e assombram o ambiente virtual, ficando a frente de ataques de cavalo de Tróia.

No Figura 2, são apresentados os percentuais de incidência de ataques na *Internet,* de acordo com a CERT (2013).

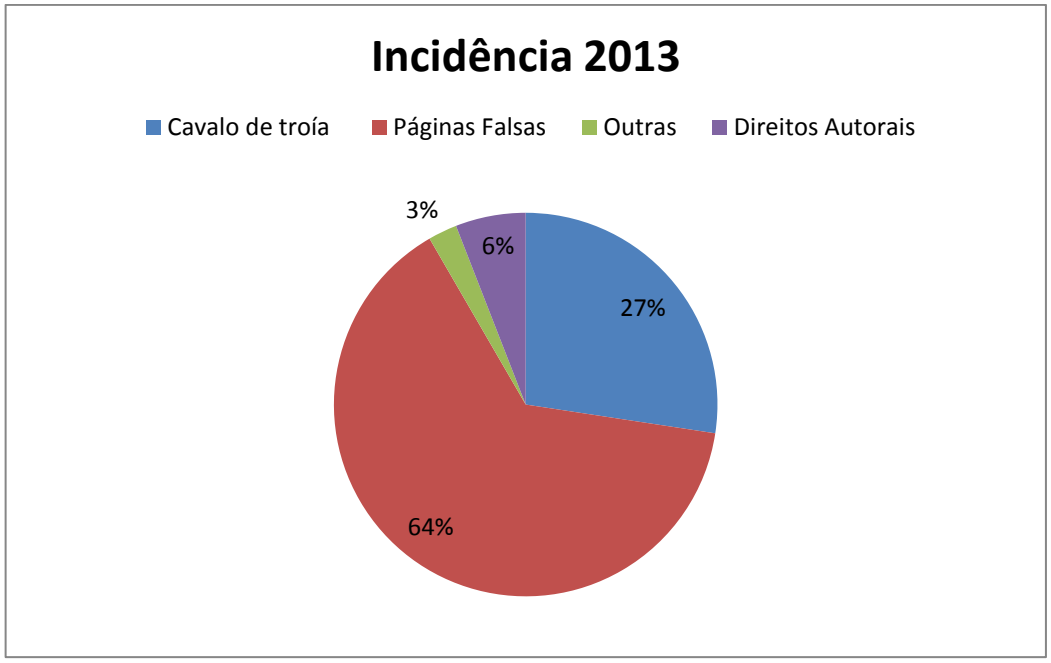

Figura 2: Incidência de Ataques na Internet

Fonte: CERT, 2013.

2.3 PHISHING

O termo *Phishing* deriva da palavra *fishing* (pescaria), em referência ao modo que o fraudador coleta os dados de suas vítimas. Lançando uma isca, utilizam do crédito que as pessoas atribuem às instituições autênticas (JAMES, 2005).

Phishing adota engenharia social e tecnologias para realizar fraudes por meio de mensagens endereçadas no *e-mail e* rede social. As mensagens trazem *links* para *sites* falsos que requerem fornecimento de informações sobre o usuário, assim define o relatório de tendências de atividades de *Phishing* realizado pelo *Anti Phishing Working Group* (APWG, 2013).

O *Phishing* é uma forma *online* de fraude, onde o invasor passa por outra pessoa ou instituição a fim de obter dados das vítimas. Estas informações normalmente são dados confidenciais como nome de usuários, senhas, número de documentos entre outros (DANHIEUX, 2013).

As identificações das mensagens falsas não são feitas de forma simples, já que os *sites* e mensagens de *Phishing* são similares ao máximo com a realidade. Devida a essa semelhança, é difícil que estas mensagens sejam identificadas como *spam* (PINHEIRO, 2007).

Os geradores de mensagens de *Phishing* podem alterar seu conteúdo assim que sua tentativa anterior tenha sido descoberta como fraude, resultando em um número elevado de pessoas que caem neste tipo de fraude por estar sempre em transição.

Segundo Danhieux (2013), há quatro objetivos a serem atingidos em um ataque de *Phishing,* sendo eles: Colher informações, infectar o computador com links maliciosos, infectar o computador com anexos maliciosos e fraudes.

- Colher informações consiste em induzir o usuário a fornecer seus dados, acreditando que esta interagindo com uma entidade idônea, sendo quase imperceptível notar diferenças significativas à primeira vista na página falsa comparada a original. Contém o mesmo conteúdo e características. Seu foco é pescar senhas e elementos cadastrais.
- Infectar o computador com links maliciosos, o fraudador busca ter controle total do computador da vítima, atacando o navegador WEB.
- Infecção por anexos maliciosos, também procuram o controle da máquina do usuário, mais em vez de utilizar de links, usam arquivos corrompidos, que ao baixar o documento e abri-lo, atinge o seu objetivo.
- Fraudes, os usuários são persuadidos por meio de mensagens com assunto que focam o psicológico da vítima, levando-a realizar depósitos em dinheiro para o fraudador, julgando estar contribuindo com ações altruístas, ou por ambicionar prêmios que supostamente exigem pagamento de taxas antecipadas.

A forma mais comum de *Phishing* ocorre por meio do envio de *e-mails*, onde o *hacker* se faz passar por uma organização de confiança, por exemplo, uma empresa conhecida, pedindo que a vítima insira informações pessoais em um site falso, que contém a aparência fiel do site original.

O fraudador aproveita da ignorância dos usuários para cometer o golpe. Muitos clientes não estão cientes que as agências bancárias não solicitam informações por *e-mail,* para fazer recadastramentos e preciso comparecer a agência.

Para o sucesso dessa fraude é preciso procedimentos do usuário, como baixar programas, clicar em links para ser direcionada a uma página *World Wide Web* (WEB), conceder permissão para o fraudador (EIRAS, 2004).

O *Phishing* pode ser elaborado para ser disparado para vários endereços distintos ao mesmo tempo, sem ter uma vítima em específico, coletando dados indiscriminadamente, este é conhecido como Pescaria cega *(Blind Phishing).*

O número de envios de *Blind Phishing* é alto, em formato de *spam*, não leva em consideração se a possível vítima tem ou não alguma relação com a instituição que teve sua página falsificada, apenas envia a mensagem e espera que alguém a acesse e fornece os dados.

Nas redes sociais a fraude ocorre em forma de solicitações de amizade, convite para visualização de vídeos e notícias, mensagens de pessoas conhecidas, promoções, pacotes de viagem, muitas vezes buscando roubar o nome de usuário e senha.

De acordo com Jacatic, Johnson e Menezer (2007).

> Phishing é uma forma de engano que um atacante tenta de forma fraudulenta adquirir informações confidenciais de uma vítima através da personificação de uma entidade confiável. Os ataques de Phishing normalmente empregam iscas genéricas. Por exemplo, um Phisher passa por uma grande corporação bancária ou popular site de vendas online terá um rendimento razoável, apesar de saber pouco ou nada sobre o destinatário.

No caso da vítima ser empresas ou órgãos públicos o golpe é mais elaborado. Nesse caso é necessário um estudo antecipado por parte do fraudador, para identificar os hábitos, formulando o conteúdo da mensagem de acordo com os interesses da empresa, este é conhecido com *Spear Phishing* (MARTINS, 2008).

O *Spear Phishing* (pesca com arpão) é encaminhado para um alvo predefinido. Os dados que se pretendem obter com o ataque são focalizados, requer uma minuciosa averiguação por parte do fraudador.

De acordo com o Muris (2008), *Spear Phishing*, não é apenas um crime, mas sim dois crimes, já que em alguns casos o fraudador, rouba dados de empresas, assim cometendo o primeiro crime, em seguida usa os dados dos clientes desta empresa para novos crimes.

Existem outros tipos de *Phishing*, sendo eles por telefone e por serviço de mensagem curta (SMS). Os fraudadores oferecem serviços que não existem ou se

passam por empresas onde o usuário teria uma pendência fictícia e pede para que a vítima entre em contato (MUSTHALER, 2013).

No relatório As palavras mais usadas em ataques de *Spear Phishing* (FireEye, 2012), expõem as fraudes por *e-mail* contendo arquivos perversos utilizando nome de serviços postais, pagamento de impostos, instituições financeiras, serviços aéreos e envio de faturas.

Na Cartilha de Segurança para *Internet* (CERT, 2013), são detalhados os tópicos e temas das mensagens enviadas em um ataque de *Phishing.* Na Tabela 1, são registrados todos os assuntos mais utilizados.

Tabela 1 - Exemplos de tópicos e temas de mensagens de *Phishing*

Tópico	Tema da mensagem
Álbuns de fotos e vídeos	Pessoa supostamente conhecida, celebridades algum fato noticiado em jornais, revistas ou televisão traição, nudez ou pornografia, serviço de acompanhantes.
Associações assistenciais	AACD Teleton, Click Fome, Criança Esperança.
Avisos judiciais	Intimação para participação em audiência comunicado de protesto, ordem de despejo.
Cartões de crédito	Programa de fidelidade, promoção.
Comércio eletrônico e Companhias aéreas	Cobrança de débitos, confirmação de compra, atualização de cadastro, devolução de produtos, oferta em *site* de compras coletivas e Promoção, programa de milhagem.
Eleições	Título eleitoral cancelado, convocação para mesário.
Empregos	Cadastro e atualização de currículos, processo seletivo em aberto.
Imposto de renda	Nova versão ou correção de programa consulta de restituição, problema nos dados da declaração.
Internet Banking	Unificação de bancos e contas, suspensão de acesso atualização de cadastro e de cartão de senhas lançamento ou atualização de módulo de segurança comprovante de transferência e depósito, cadastramento de computador.
Multas e infrações de trânsito	Aviso de recebimento, recurso, transferência de pontos.
Músicas, Notícias e boatos.	Canção dedicada por amigos e Fato amplamente noticiado, ataque terrorista, tragédia natural.
Prêmios e Promoções	Loteria, instituição financeira. Vale compra, assinatura de jornal e revista desconto elevado, preço muito reduzido, distribuição gratuita.

Tópico	Tema da mensagem
Programas em geral e Antivírus	Lançamento de nova versão ou de novas funcionalidades e Atualização de vacinas, eliminação de vírus lançamento de nova versão ou de novas funcionalidades.
Propagandas e *Reality shows*	Produto, curso, treinamento, concurso. Big Brother Brasil, A Fazenda, Ídolos.
Redes sociais	Notificação pendente, convite para participação aviso sobre foto marcada, permissão para divulgação de foto.
Serviços de Correios	Recebimento de telegrama *online*
Serviços de *e-mail*	Recadastramento, caixa postal lotada, atualização de banco de dados.
Serviços de proteção de crédito	Regularização de débitos, restrição ou pendência financeira.
Serviços de telefonia	Recebimento de mensagem, pendência de débito bloqueio de serviços, detalhamento de fatura, créditos gratuitos.
Solicitações	Orçamento, documento, relatório, cotação de preços, lista de produtos.

Fonte: Centro de Estudos, Resposta e Tratamento (CERT, 2013).

Para identificar casos de *Phishing* é necessário analisar alguns detalhes do *e-mail*, ou em caso de *links* em redes sociais. O primeiro e indiscutível passo a ser tomado é o discernimento da potencial vítima em relação à mensagem recebida.

O usuário deve estar alerta ao ser contemplado com prêmios, ofertas de empregos e negócios com pessoas que nem conhece, ajuda comunitária a outros países, requisição de atualização cadastrais de instituições em que nem possui conta, convite para promoções, atualização de título eleitoral, conforme Karasinski (2011).

Na área de psicologia afirma-se que a tomada de decisão segue uma trajetória mais complexa do que a de estímulo a resposta, através da interpretação. Os estímulos são sinais verbais e não verbais que ligam um enganador a um receptor (POWER E KIRWAN, 2013).

Em vez de *clicar* em cima dos *links* recebidos, o usuário deve realizar uma busca pelo *site* e conferir por meio dele se esta havendo algum tipo de promoção, oferta de serviços, ou a melhor atitude seria copiar o endereço e colar no navegador, para confirmar se é verdadeiro (FIREEYE, 2012).

A escrita da mensagem eletrônica deve ser observada, geralmente em situações de fraudes desta natureza são encontrados muitos erros gramaticais,

ortográficos e a presença de palavras estrangeiras soltas pelas frases sem muito sentido.

Os criminosos não têm medido esforços para alcançar mais vítimas e a Copa do Mundo 2014 tem sido uma isca para isso acontecer. Segundo resultados divulgados pela Kaspersky (2014), foram constatados vários domínios recentes com intuito de aplicar golpes.

De acordo com a divulgação citada acima, as páginas inverídicas induzem o usuário a baixar arquivos contendo bilhetes para participar do evento e prêmios enganosos. As empresas patrocinadoras estão sofrendo com seus *sites* sendo falsificados, abalando a confiança dos clientes nas instituições.

Diversos *sites* estão oferecendo ofertas improváveis, reduzindo os preços pela metade, com a desculpa de serem em estímulo as compras para as comemorações (Revista Exame, 2014).

Na Figura 3 é apresentado um exemplo de página falsificada com promoção da copa 2014.

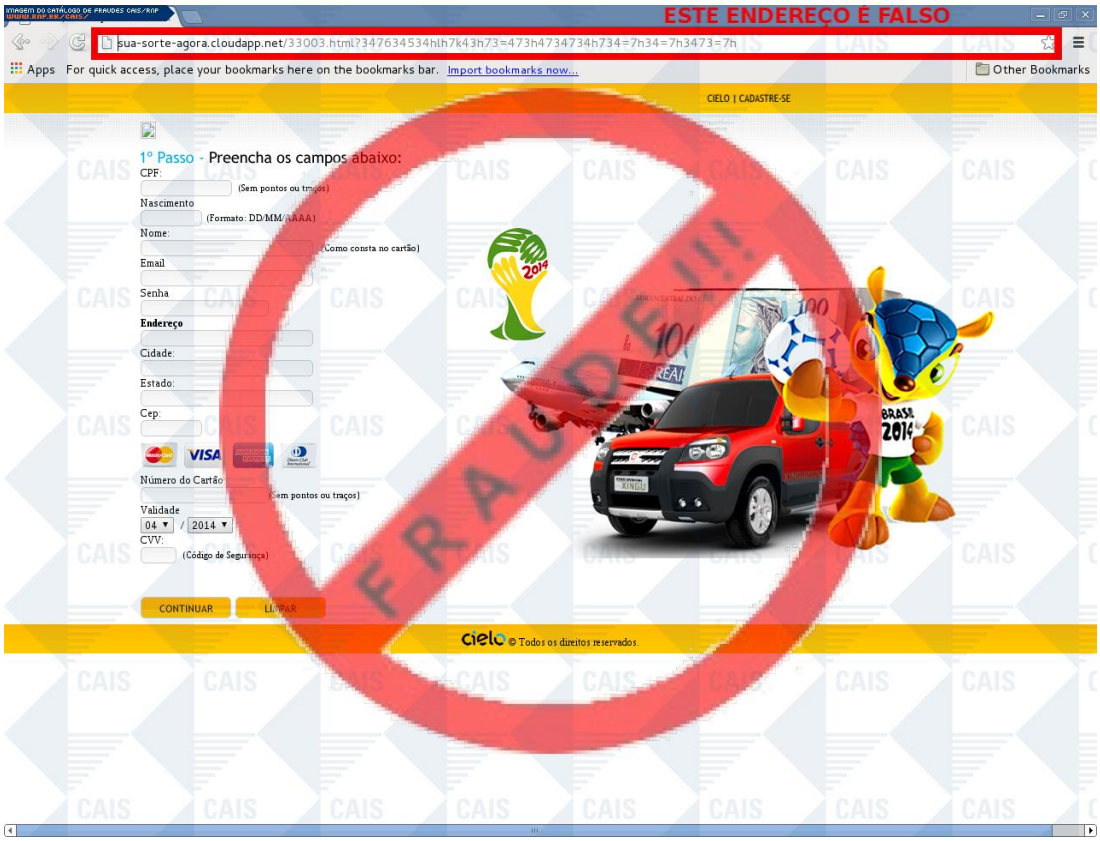

Figura 3: Fraude identificada
Fonte: Rede Nacional de Ensino e Pesquisa (RNP, 2014).

Em pesquisa realizada por Darwish e Aloul (2012), é feita uma comparação entre as potenciais vítimas de *Phishing* entre acadêmicos. Alguns fatores são analisados como áreas dos cursos universitários, faixa etária e gênero.

Na Tabela 2 são apresentados os resultados da pesquisa citada acima.

Tabela 2 - Características das potencias vítimas de *Phishing*

	Altamente suscetíveis	**Menos suscetíveis**
Idade	18-24 anos	25 anos ou mais
Gênero	Feminino	Masculino
Área da Educação	Humanas	Ciência da Computação

Fonte: Darwish e Aloul (2012).

No Brasil foi identificado por meio de pesquisa do VeriSign (2010) e divulgada na revista Fator Brasil, que as mulheres são 10% mais propensas do que os homens a não reconhecer uma página falsificada a responderem as solicitações feitas.

Em contraste aos resultados explanados por Darwish e Aloul, a faixa etária dos brasileiros analisados demostra um risco menor para os de 18 a 24 anos de serem enganados, ficando com o grupo de 35 a 44 anos a maior probabilidade.

A diferença encontrada na verificação das idades pode-se dar em função da cultura das populações estudadas. Segundo Rodrigues (2011) a cultura exerce influência nas atitudes e percepção das pessoas.

As regiões geográficas no Brasil também foram consideradas e a população que reside no Centro-Oeste é a que menos corre risco de ser fraudada. A região é composta por três estados e Distrito Federal.

Na Tabela 3 são expostos os resultados das análises feitas no Brasil.

Tabela 3 - Características de potenciais vítimas de Phishing no Brasil

	Altamente suscetíveis	**Menos suscetíveis**
Idade	35 a 44	18-24 anos
Gênero	Feminino	Masculino
Região	Não divulgado	Centro-Oeste

Fonte: Revista Fator Brasil (2010).

3 MÉTODOS E MATERIAIS

A natureza da pesquisa é descritiva que de acordo com Prodanov e Freitas (2013), visa reunir, analisar e classificar os dados coletados por meio de procedimento específico, sem a ocorrência de intervenções por parte do observador.

O procedimento técnico que foi empregado é o levantamento, pela necessidade da obtenção de informações, utilizando perguntas direcionadas a uma amostra de pessoas, das quais se pretende conhecer a descrição.

Os dados serão coletados por meio de um formulário desenvolvido utilizando a ferramenta de pesquisa *Lime Survey* que permite a coleta de dados. O Formulário possui um grupo de perguntas pessoais e acadêmicas, tendo questões fechadas e campos para respostas curtas.

Uma mensagem por correio eletrônico*,* com o assunto Atualização de dados cadastrais, foi enviada para os acadêmicos do Campus Luiz Meneghel, caracterizando um ataque de *Phishing,* contendo um *link* para direcionar ao formulário a ser preenchido*.*

O *e-mail* possui uma mensagem não tendenciosa a gênero ou curso, é voltada para o público que em comum possuem o fato de serem alunos da UENP. Os dados foram analisados com uma abordagem quantitativa.

A faixa etária estudada abrange uma amostra que possui em maioria, de 17 a 31 anos, sendo necessário dividir as idades em 4 classes. A primeira classe possui idade entre 17 a 21 anos. A segunda classe está entre 22 a 26 anos. A terceira são acadêmicos de 27 a 31 anos. Os que possuem idade acima de 31 estão contidos na quarta classe.

Para abranger um número expressivo de participante o Banco de dados da Universidade Estadual do Norte do Paraná (UENP- campus Luiz Meneghel), contendo os endereços de *e-mails* será utilizado.

Para expor os resultados, percentuais serão apresentados com ilustração de gráficos de Barra empilhados e tabelas.

4 DESENVOLVIMENTO

Para iniciar a pesquisa, primeiro teve-se acesso autorizado à lista de *e-mails* dos acadêmicos da UENP dos cursos de Agronomia, Ciência da computação, Ciências Biológicas, Enfermagem, Medicina Veterinária e Sistemas de Informação.

Com a base de dados em mãos, foi criado o endereço de *e-mail* “recadastramento.uenp2014@hotmail.com”, usado para enviar as mensagens, caracterizando *Phishing* explícito já que instituições não utilizam de contas populares de *e-mail* para contato, possuem um domínio próprio.

O suposto comunicado da Direção da Universidade solicitava que os acadêmicos realizassem uma atualização de cadastro *online*, e continha um *link* direcionando para o formulário a ser preenchido.

O assunto do e-mail foi “Informatização de serviços acadêmicos”, aproveitando-se do fato de não haver um sistema para rematrícula *online* e este ser um plano futuro que beneficiaria os alunos e todos os envolvidos em período de recadastramento que até então o fazem manualmente.

O fator que interferiu no número trabalhado foi o fato de vários dos acadêmicos relacionados não terem fornecido um endereço eletrônico para contato a secretária acadêmica no ato da matrícula diminuindo a quantidade de participantes.

Abaixo é representado o conteúdo do *e-mail*, comunicando os acadêmicos da nova forma de utilizar seus serviços, a partir de recadastramento em modo *online* e como os alunos deveriam proceder para não ter seu registro acadêmico cancelado ao não fornecer seus dados no tempo estabelecido.

Prezado acadêmico,

Para assegurar maior comodidade ao realizar as rematrículas dos cursos oferecidos na UENP, estamos modernizando nosso sistema de registros, antes feito por meio de formulário impresso.

A partir de agora pode-se realizar a matrícula ou a renovação da mesma sem sair de casa, sem filas e sem depender da disponibilidade de horário da secretária acadêmica.

Por não haver mais a necessidade da presença física do aluno ou de seu responsável legal, este não terá mais o benefício de justificar a não efetuação da rematrícula em prazo estabelecido.

No primeiro momento apenas a atualização de alguns dados serão solicitados, para confirmação de registros, envolvendo todos os alunos devidamente cadastrados.

Esta atualização de cadastro também permitirá a utilização de outros serviços que em breve serão oferecidos no site da UENP.

Para atualizar seu cadastro Clique aqui.

Atenção: Os acadêmicos que não efetuarem a atualização no período de 7 dias a partir do recebimento deste e-mail, não poderão realizar sua rematrícula, pois o preenchimento do formulário não poderá ser realizado na secretária acadêmica como em anos anteriores.

Evite transtornos, faça já sua atualização de cadastro.

Protocolo: A43RJHIU89IHGV9D

Esta é uma mensagem automática, não é necessário respondê-la.

Universidade Estadual do Norte do Paraná (UENP)
Campus Luiz Menheghel
Bandeirantes/PR

Conteúdo do *e-mail* enviado aos estudantes.

No formulário havia 10 campos a serem preenchidos, com dados do aluno que o acessasse. Nenhum dos dados requisitados ofereceu qualquer prejuízo para quem o forneceu.

Os campos para preenchimento eram os seguintes:

- Nome: Para identificar o acadêmico, por se tratar de um *e-mail* de recadastramento, tornou-se necessário para garantir a autenticidade do pedido. O nome não tem relevância para o trabalho.
- Sexo: O Gênero é importante para discriminar o perfil das vítimas e comparar com pesquisas anteriores.
- Data de nascimento: Para analisar a média da idade dos participantes;
- Curso: o objetivo da pesquisa é comparar a reação dos alunos dos diferentes cursos em relação ao *Phishing*, tornando-se necessário identificar o curso feito pelo graduando.
- Número de inscrição: Apenas para completar o formulário de acordo com informações básicas do discente, não tem relevância para o estudo.
- Ano de ingresso: Apenas para completar o formulário de acordo com informações básicas do discente.
- Semestre/Ano atual: Apenas para completar o formulário de acordo com informações básicas do discente, não tem relevância para o estudo.
- Usuário: Não é usado para a pesquisa, mas foi solicitado que os participantes criassem um usuário para ambientar um verdadeiro sistema com atualizações e simular um armazenamento onde apenas a pessoa a autorizada poderia ter acesso e alterar suas informações futuramente.
- Senha e redigitar a senha: Não são usados para a pesquisa, mas foi solicitado que os participantes criassem a senha para ambientar um verdadeiro sistema com atualizações acompanhando o usuário criado.

Os métodos usados em engenharia social foram aplicados na pesquisa, como a limitação de tempo disponível para realizar a atualização perante advertência de cancelamento de registro.

A atenção da vítima é um fator determinante também a suscetibilidade aos ataques. O estudo de Vishwanathet (2011) define 4 fatores relacionados a atenção do usuário e as chances desse ser vítimas destas fraudes.

- O nível de atenção para a fonte do e-mail será negativamente relacionada com a probabilidade do indivíduo para responder a e-mails de *Phishing.*
- O nível de atenção à gramática e ortografia no e-mail será negativamente relacionado com a probabilidade do indivíduo para responder a e-mails de *Phishing*.

  *Ex.: "**Campus Luiz Menheghel***" com o nome escrito com letras a mais.
- O nível de atenção para os sinais de urgência é relacionado com a probabilidade de responder a e-mails de Phishing.

  Ex.: ***"Atenção:*** *Os acadêmicos que não efetuarem a atualização no período de**7** dias a partir do recebimento deste e-mail, não poderão realizar sua rematrícula, pois o preenchimento do formulário não poderá ser realizado na secretária acadêmica como em anos anteriores".*
- O nível de atenção à linha de assunto será positivamente relacionado com a probabilidade de responder a *e-mails* de *Phishing*.

A atenção aos elementos específicos do e-mail (gramática, fonte, ortografia, sinais de urgência e assunto) está diretamente relacionada com as chances de a amostra fornecer uma resposta, impulsionada pelo incentivo de executar a atualização.

Com o encerramento da coleta de dados o formulário foi eliminado, impossibilitando visitas à ele, após o término. As informações contidas foram exportadas para um arquivo no *Excel*, onde os cálculos referentes aos números obtidos foram analisados.

Os cursos analisados pertencem a áreas distintas sendo elas, saúde, biológica, tecnológica e agrária.

- AGRONOMIA

Engenharia agronômica também conhecida como agronomia, desempenha grande papel na área de agronegócio. Estuda diversos métodos para melhoria da produtividade e a forma mais propicia de aplicá-la.

Os computadores ocupam espaço em várias áreas do conhecimento inclusive no setor agronômico, o que exige que os futuros profissionais tenham mais contato com os computadores e busquem conhecer mais sobre eles.

Em sua maioria os acadêmicos do curso de engenharia agronômica são do sexo masculino, embora tenha havido um aumento na procura feminina pelo curso nos últimos anos (CAMPANHA, 2013).

- Ciência da Computação

Curso da área tecnológica parte de conhecimento em exatas, seus alunos desenvolvem programas de computador em diversas áreas e desempenham funções importantes no campo de segurança para operações computacionais, segundo nota da Universidade Federal de Pernambuco (UTPE, 2012).

O número de acadêmicos do sexo masculino é superior a presença feminino que chega a apenas 18% nas salas de aulas, ainda de acordo com a Federal de Pernambuco.

- Ciências Biológicas

As Ciências Biológicas estuda toda forma de vida, genética, natureza, alimentos entre outros. Em controvérsia aos cursos discutidos anteriormente em Ciência Biológicas o número de acadêmicos do sexo feminino é superior à presença masculina nas aulas.

A área biológica envolve estudos em paleontologia, analises clínicas, produção de vacinas, pericias, bioenergia e desenvolvimento de produtos biotecnologias no campo de transgênicos, células tronco e clonagem.

O computador pode ser inserido nos estudos biológicos entre outras funções para realizar fórmulas matemáticas.

- Enfermagem

O curso de Enfermagem objetiva a promoção da saúde humana, auxiliar os médicos a alcançar e proteger o bem estar dos pacientes, tratando doenças e as prevenindo.

Seus profissionais atuam em hospitais, clínicas, ambulatórios, instituições de ensino infantil e atendimento domiciliar. Independente de onde oferecem seus

serviços são responsáveis pelas medicações, curativos, manutenção do ambiente e alimentação do paciente.

O uso do computador na área da saúde tornou-se essencial, é importante para execução de ferramentas para tratar dados coletivos e individuais dos pacientes (BORTOLI, 1999).

- Medicina Veterinária

*"*O Medicina Veterinária é a ciência dedicada ao estudo, prevenção e tratamento das doenças dos animais e pode atuar controlando a qualidade da produção nas industriais e também realizando pesquisas na área de zoonoses*",* de acordo com Mota (2012).

Para Martins e Moura (2011), utilizar o computador na área da veterinária é extremamente importante "A grande importância da Informática na Medicina Veterinária tem se justificado por diversos meios que atualmente podem ser vistos em clínicas, laboratórios e universidades de todo o país*".*

Estudos da Universidade do Kansas (2011) indicam que o curso de Medicina veterinária em geral é frequentado por um grande número de mulheres podendo chegar a 75% dos estudantes.

- Sistemas de Informação

O curso de Sistemas de Informação segundo descrição na página da UENP, "visa desenvolver profissionais que apresentem visão abrangente dos problemas organizacionais, encontrando soluções computacionais, seguras e confiáveis, eficazes e rápidas na informatização de empresas".

Assim como outros cursos que envolvem tecnologia, a maioria dos alunos são do sexo masculino, apesar de ter aumentado o interesse feminino na área o nível matrículas ainda é baixo.

- Resultados

O número de estudantes que receberam em seu *e-mail* uma notificação de recadastramento somam 555 alunos, o número de respostas obtidas com o devido preenchimento do formulário representam 141.

Um percentual de 25,40% da amostra pesquisada envolvendo todos os cursos forneceram seus dados ao suposto pedido da Universidade e 365 alunos ignoram o formulário.

São apresentados no Gráfico 1, o percentual de formulários preenchidos.

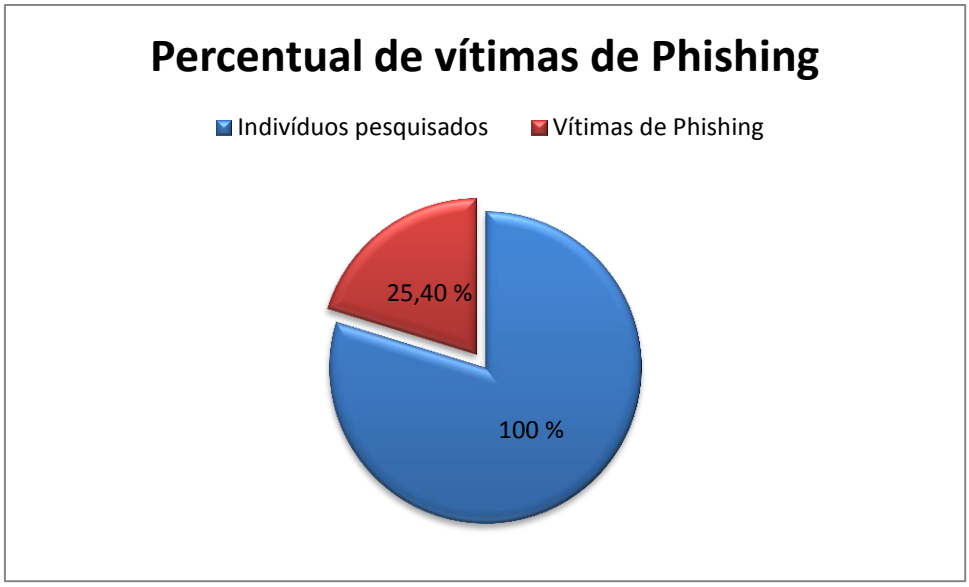

Gráfico 1: Percentual de vítimas de *Phishing*.

Além dos 141 formulários respondidos outros 49 acessos ocorreram, mas não houve preenchimento com os dados, apenas clicaram no *link* e visitaram a página. Estes números não interferem na pesquisa por não haver dados dos pesquisados para identificar o curso, gênero e idade da vítima.

Os *links* presentes em *e-mails* de *Phishing* podem instalar vírus infectando a máquina e programas espiões, assim podendo roubar as senhas sem a autorização do usuário, diferente das páginas falsas em que o usuário fornecer espontaneamente as informações sendo enganado.

Este grupo de 49 pessoas pode ser classificado como propensas a serem fraudadas, tendo instalações feitas em seus computadores sem permissão, já que clicam nos *links* sem verificar.

Entre o número total de vítimas, o estudo aponta a quantidade de alunos que responderam ao *e-mail* e quais seus respectivos cursos. Sendo eles: 50 alunos de Medicina Veterinária, 38 de Agronomia, 19 de enfermagem, 18 de Ciência da Computação, 11 de Ciências Biológicas e 5 de Sistemas de Informação.

No Gráfico 2, são representados a quantidades de estudantes pesquisados por curso e a quantidade de vítima de *Phishing* em cada um deles.

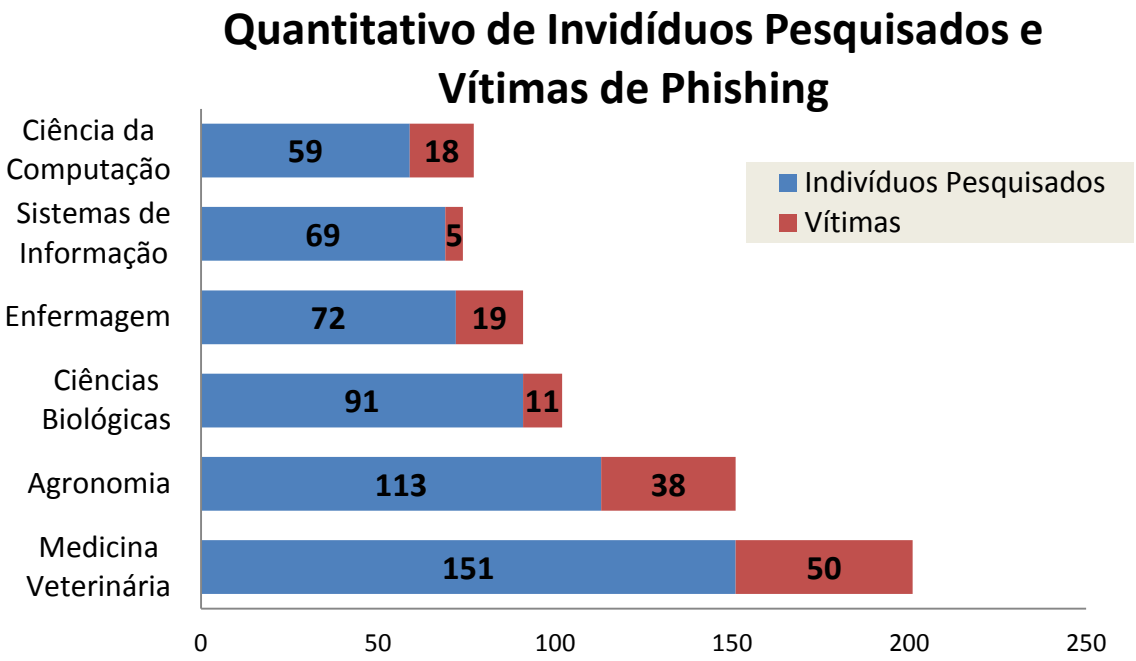

Gráfico 2: Quantitativo de Indivíduos pesquisados e vítimas de *Phishing*.

O percentual de vítimas de *Phishing em cada curso* é mostrado no Gráfico 3

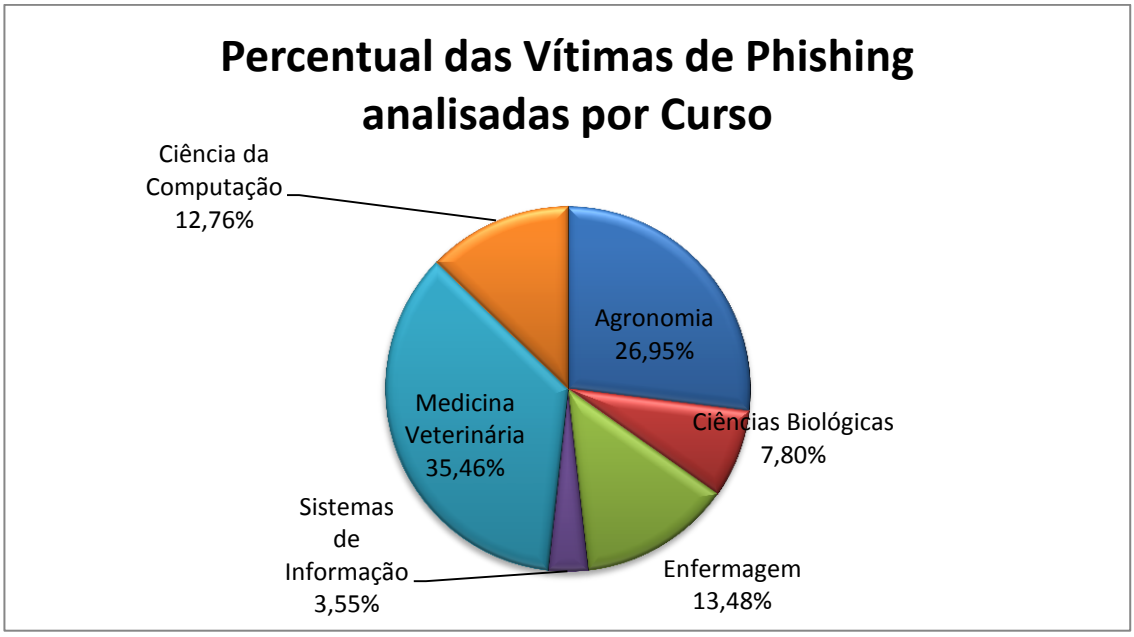

Gráfico 3: Percentual de vítimas de *Phishing* por curso.

No resultado encontrado houve um número maior de mulheres que não reconheceram que a mensagem não era verdadeira e aceitaram enviar seus dados sem verificar a integridade do *e-mail*.

As respostas vindas do sexo feminino resultaram em 75 respostas, cerca de 53,19% e as respostas masculinas, somaram 66 cerca de 46, 81%, comparadas ao número total de respostas alcançadas.

O percentual do gênero feminino e masculino que executaram a atualização simulada de cadastro é demonstrado no Gráfico 4.

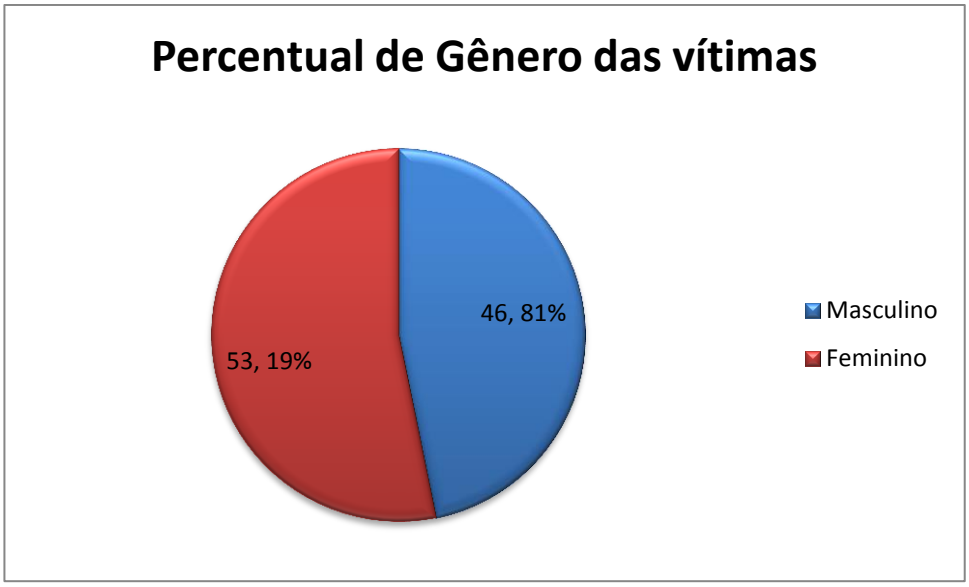

Gráfico 4: Percentual de gênero das vítimas.

Os pesquisados do sexo masculino somam 291, deste total, 66 foram vítimas, sendo representado por um percentual de 22,68%. O sexo masculino constitui 46,81% das vítimas totais. Nos cursos pesquisados o número de homens é retratado na Tabela 4.

Tabela 4- Quantidade de homens pesquisados e vítimas por curso

Curso	Quantidade de pesquisados	Quantidade de Vítimas
Enfermagem	7	6
Ciência da Computação	53	17
Agronomia	101	27
Medicina Veterinária	43	8
Ciências Biológicas	24	3
Sistemas de Informação	63	5
Total	**291**	**66**

No Gráfico 5 é representado o percentual de vítimas do sexo masculino em cada curso de acordo com os número expostos na tabela 4.

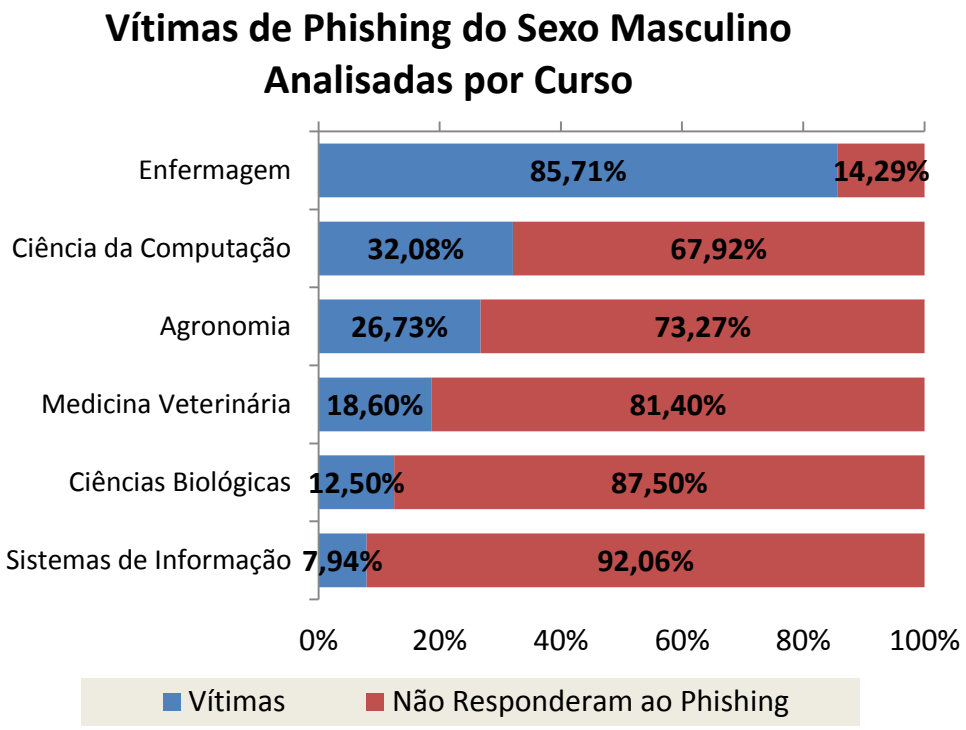

Gráfico 5: Vítimas masculinas por curso.

Os pesquisados do sexo feminino somam 264, deste total, 75 foram vítimas, sendo representado por um percentual de 28,40%. O sexo feminino constitui 53,19% das vítimas totais. Nos cursos pesquisados o número de mulheres é retratado na Tabela 5.

Tabela 5: Quantidade de mulheres pesquisadas e vítimas por curso**.**

Curso	Quantidade de pesquisados	Quantidade de Vítimas
Enfermagem	65	13
Ciência da Computação	6	1
Agronomia	12	11
Medicina Veterinária	108	42
Ciências Biológicas	67	8
Sistemas de Informação	6	0
Total	**264**	**75**

No Gráfico 6, é representado o percentual de vítimas do sexo feminino em cada curso de acordo com os número expostos na tabela 5.

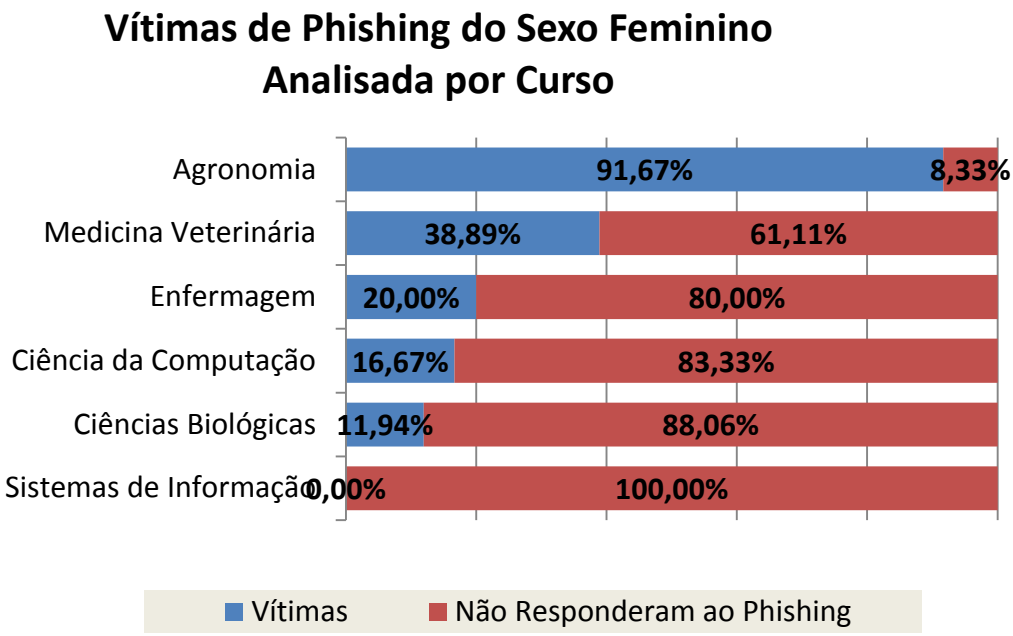

Gráfico 6: Vítimas femininas por curso.

A faixa etária esta dividida em quatro grupos envolvendo todos os pesquisados entre os 6 cursos. A idade é um fator importante no reconhecimento de uma fraude, pois envolve o senso de atenção e discernimento.

Na Tabela 6, é exposta a quantidade de vítimas por faixa etária.

Tabela 6: Faixa etária das vítimas

Classe	Número de Indivíduos
17 a 21 anos	83
22 a 26 anos	48
27 a 31 anos	8
acima de 31 anos	1
Total:	**141**

Na faixa etária de 17 a 21 anos teve-se 59% das vítimas, seguida pelos estudantes de idade entre 22 a 26 anos com 48%. As vítimas inseridas na faixa etária de 27 a 31 anos tiveram um percentual de 8% e apenas 1% possui idade maior que 31 anos.

No Gráfico 7, os percentuais de vítimas em cada classe de idade.

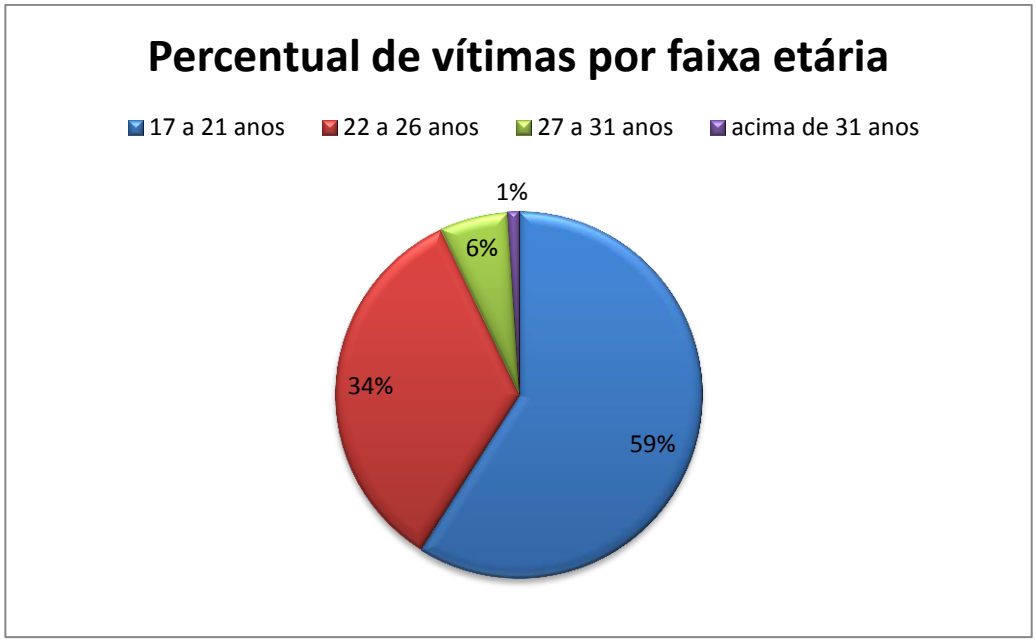

Gráfico 7: Percentual de vítimas por faixa etária

5 CONCLUSÃO

Em verificação aos dados coletados pode-se constatar as singularidades existentes em cada um dos cursos estudados, apresentando um público mais acometível em cada um deles.

Após análise individual dos cursos pode-se conhecer os grupos mais suscetíveis, levando em conta a faixa etária e o gênero dos graduandos.

Todas as faixas etárias pesquisadas possuíram usuários que não reconhecem a fraude de *Phishing*. Os acadêmicos com idade entre 17 a 21 anos representam um número maior de vítimas.

As mulheres são aproximadamente 6% mais propensas a serem vítimas analisando o total de pesquisados e vítimas por gênero.

Cada curso possui um resultado diferente em referência ao gênero mais suscetível como representado na Tabela 7.

Tabela 7 - Gênero mais suscetível por curso

	Mais suscetível	
Cursos	**Feminino**	**Masculino**
Medicina Veterinária	X	
Agronomia	X	
Enfermagem		X
Ciência da Computação		X
Ciências Biológicas		X
Sistemas de Informação		X

Nos cursos de agronomia e enfermagem ocorrem diferenças significativas no gênero, pois na agronomia a maioria dos acadêmicos são do sexo masculino e as vítimas identificadas são em maior número do sexo feminino.

Em enfermagem, acadêmicos no sexo masculino são minoria, mas a maior parte das vítimas são homens, mesmo sendo menos estudantes deste gênero.

Não há uma diferença considerável entre alunos da tecnologia com os graduando de outras áreas em relação a reconhecer um *Phishing.* O fato de estar envolvido com assuntos tecnológicos não ajudam os alunos a escapar de fraudes.

Conclui-se que as vítimas estão inseridas na faixa etária de 17 a 21 anos, são em maior parte do sexo feminino e o curso com maior número de respostas foi ao de Medicina Veterinária, que faz parte da área da saúde.

A identificação do Perfil das vítimas de *Phishing* no campus Luiz Meneghel, possibilita um futuro treinamento direcionado para este público discernir sobre o que são características de *Phishing*.

Em sugestão para trabalhos futuros, os outros *campis* da UENP localizado em Cornélio Procópio e Jacarezinho também poderiam ser utilizados para identificar as vítimas dessa fraude, já que possuem cursos diferentes dos oferecidos no campus Luiz Meneghel.

REFERÊNCIAS

ALOUL, A. E. Z. A. F.; DARWISH, A. **Towards Understanding Phishing Victims'**. 2012. 5f. Monografia (Bacharelado em Tecnologia) - American University of Sharjah, aloul, 2012. Disponível em: <http://www.aloul.net/Papers/faloul_iccsii12.pdf> Acesso em: 15 abr. 2014

ALVES, C. B. **Segurança de Informação VS. Engenharia Social**. 200. 63f. Monografia (Bacharelado em Sistemas de Informação) - Centro Universitário do Distrito Federal, udf, 200.

CARVALHO, I. R. F. **Segurança da Informação**. 2011. 18f. Monografia (Bacharelado em Ciência da computação) - Universidade Federal de Lavras, site, 2011.

CASTRO, A. E.; JÚNIOR, V. F. S.; VIEIRA, H. C. **O uso de questionário via e-mail em pesquisas acadêmicas sob a ótica dos respondentes**. 2010. 13f. Monografia (Bacharelado em administação) - Universidade Federal de Santa Maria, Santa Maria, RS, 2010.

CAVALCANTI, R. L. **Engenharia Social nas Redes Sociais** . 2011. 48f. Monografia (Bacharelado em Tecnologia da Informação) - Universidade Estadual de Maringá, Especialização na WEB, 2011.

DANTAS, M. L. **Segurança da Informação: Uma abordagem focada em gestão de riscos**. Olinda, pE: Livro rápido, 2011. 150p.

EIRAS, M. C. **Engenharia Social e Correio Eletrônico**. 2004. 40f. Monografia (Bacharelado em Segurança de Informação na Internet) - Universidade Federal do Rio de Janeiro, IBPI, 2004.

ESTRATÉGICOS, S. A. **Desafios estrategicos para a segurança e defesa cibernetica**. 1ª. ed. Brasília: Imprensa Nacional, 2011. 215p.

FABENY, G. **Fatores Geradores de Resitência ao Uso de Internet Banking no Banco do Brasil SC**. 2007. 58f. Monografia (Bacharelado em Administração) - Universidade Federal do Rio Grande Do Sul, UFRJ, 2007.

FREITAS, E. C.; PRODANOV, C. C. **Metodologia do Trabalho Científico: Métodos e Técnicas da Pesquica e do Trabalho Acadêmico**. 2ª. ed. Novo Hamburgo- RS: Feevale, 2013. 276p. Disponível em: <http://www.feevale.br/Comum/midias/8807f05a-14d0-4d5b-b1ad-1538f3aef538/E-book%20Metodologia%20do%20Trabalho%20Cientifico.pdf> Acesso em: 4 jun. 2013

GERHARDT, T. E.; SILVEIRA, D. T. **Métodos de Pesquisa**. 1ª .ed. Porto Alegre, RS: UFRGS, 2009. 114p. Disponível em: <http://www.ufrgs.br> Acesso em: 4 jun. 2013

GROUP, A. W. **Phishing Activity Trends Report** .APWG, Site PWG, n.1, p.2-5, 2013.Disponível em: <http://www.antiphishing.org/resources/apwg-reports/> Acesso em: 10 jun. 2013

MARCELO, A.; PEREIRA, M. A. A. **A arte de Hackear Pessoas**. 1ª. ed. Rio de Janeiro, RJ: Brasport, 2005. 86p. Disponível em: <http://books.google.com.br> Acesso em: 12 jun. 2013

MITNICK, K. D.; SIMON, W. L. **A arte de invandir**. São Paulo, SP: Prentice Hall, 2006. 235p.

PINHEIRO, J. M. S. **Ameaças e Ataques aos Sistemas de Informação**. Caderno UniFoa, Volta Redonda, v.5, n.2, p.21, 2007. Disponível em: <http://www.unifoa.edu.br/pesquisa/caderno/edicao> Acesso em: 10 jun. 2013

RECUERO, R. **Redes Sociais na internet**. 1ª. ed. Porto Alegre, RS: Meridional, 2009. 191p.

SANTO, A. F. S. E. **Segurança de Informação**. 0. 11f. Monografia (Bacharelado em Ciência da Computação) - Instituto Cuiabano de Educação, ICE, 0.

SANTOS, R. M. **Um comparativo entre o correio eletrônico e o correio tradicional**. Intercom, Barbacena, MG, n.1, p.15, 2007. Disponível em: <http://www.ufrgs.br> Acesso em: 11 jun. 2013

SILVA, P. A. L. **Análise das Redes Sociais aplicada à Engenharia Social**. 2012. 11f. Monografia (Bacharelado em Segurança da Informação) - Faculdade De Tecnologia de Guarantinguetá, googleacademico, 2012.

SILVA, D. R. P.; STEIN, L. M. **Segurança da Informação: uma refexão sobre o componente humano**. Ciência & Cognição, Porto Alegre, RS, n.10, p.46-53, 200.

SUZUKI, R.; ZAPATER, M. **Segurança da Informação, Um diferencial determinante na competitividade das corporações**. Rio de Janeiro: PROMO, 2005. 27p. Disponível em: <http://www.promon.com.br> Acesso em: 9 jun. 2013

A maioria das pessoas continuam sem identificar uma mensagem de phishing. Disponível em: <http://www.kaspersky.com> Acesso em: 11 jun. 2013

As palavras mais usadas em ataques de spear phishing para comprometer redes corporativas e roubar dados com sucesso. Disponível em: <http://www.fireeye.com/> Acesso em: 12 jun. 2013

Constitucionalidade do monitoramento de email. Disponível em: <http://www.boletimjuridico.com.br/doutrina/texto.asp?id=1238> Acesso em: 9 jun. 2013

Consultoria em ssegurança. Disponível em: <http://www.migdalconsulting.com.br> Acesso em: 18 jun. 2013

DMARC email standards help prevent brand abuse in phishing campaigns. Disponível em: <http://www.networkworld.com/article/2166372/infrastructure-> Acesso em: 21 jun. 2013

Falta de conhecimento sobre riscos adiam planos de segurança da informação. Disponível em: <http://computerworld.uol.com.br> Acesso em: 18 jun. 2013

Fast track to the future- The 2012 IBM Tech Trends Report. Disponível em: <http://public.dhe.ibm.com> Acesso em: 18 jun. 2013

Fraudes Identificadas.. Centro de Atendimento a Incidentes de Segurança Disponível em: <http://www.rnp.br/cais/fraudes.php> Acesso em: 9 abr. 2014

Fraudes na Internet e Engenharia Social. Disponível em: <http://www.aedb.br/seget/artigos12/27816233.pdf> Acesso em: 12 jun. 2013

Incidentes Reportados . Disponível em: <http://www.cert.br/stats/incidentes/2013-jan-mar/fraude.html> Acesso em: 3 jun. 2013

KIRWAN, G.; POWER, A. **Cybercrime**. Inglaterra: CAMBRIDGE UNIVERSITY PRESS, 2013. 280p. Disponível em: <http://books.google.com.br/books> Acesso em: 18 set. 2013

As palavras mais usadas em ataques de Phishing. Disponível em: <http://www.fireeye.com/pt-br/resources/pdfs/fireeye-top-spear-phishing-words.pdf> Acesso em: 15 mai. 2013

Mídias sociais nos negócios. Disponível em: <http://www.ibramerc.org.br> Acesso em: 14 jun. 2013

Página falsa do Walmart usa ofertas para roubar dados. Disponível em: <http://exame.abril.com.br/tecnologia/noticias/pagina-falsa-do-walmart-usa-ofertas-para-roubar-dados> Acesso em: 23 mai. 2014

Pesquisa revela que 73% dos usuários brasileiros da Web não conseguem reconhecer sites de phishing. Disponível em: <http://www.revistafatorbrasil.com.br/ver_noticia.php?not=124148> Acesso em: 15 mai. 2013

PHISHING ENVOLVED. Disponível em: <http://www.websense.com> Acesso em: 13 nov. 2013

Rede Social nas empresas. Disponível em: <http://informationweek.itweb.com.br> Acesso em: 19 jun. 2013

Scam, phishing e pharming: as fraudes praticadas no ambiente Internet Banking e sua recepção no Brasil.. Autor William Moura Disponível em: <http://www.egov.ufsc.br> - Acesso em: 16 jan. 2014

Social phishing.. om N. Jagatic, Nathaniel A. Johnson, Markus Jakobsson, Filippo Menczer Disponível em: <http://www.deri.ie/content/social-phishing> Acesso em: 17 jul. 2013

Tecnologia, Informação e Segurança. Disponível em: <http://www.prodeb.ba.gov.br> Acesso em: 10 jun. 2013