UNIVERSIDADE ESTADUAL DO NORTE DO PARANÁ

***CAMPUS* LUIZ MENEGHEL**

GUILHERME TAVARES BASSETTO

DESENVOLVIMENTO DE UMA FERRAMENTA DE TREINAMENTO ANTI-PHISHING

Bandeirantes
2014

Guilherme Tavares Bassetto

DESENVOLVIMENTO DE UMA FERRAMENTA DE TREINAMENTO ANTI-PHISHING

Trabalho de Conclusão de Curso submetido à Universidade Estadual do Norte do Paraná, como requisito parcial para a obtenção do grau de Bacharel em Sistemas de Informação.

Orientador: Prof. Fabio de Sordi Junior

Bandeirantes

2014

Guilherme Tavares Bassetto

DESENVOLVIMENTO DE UMA FERRAMENTA DE TREINAMENTO ANTI-PHISHING

Trabalho de Conclusão de Curso submetido à Universidade Estadual do Norte do Paraná, como requisito parcial para a obtenção do grau de Bacharel em Sistemas de Informação.

COMISSÃO EXAMINADORA

_____
Prof. Fabio de Sordi Junior
UENP – *Campus* Luiz Meneghel

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

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

Bandeirantes, 26 de junho de 2014

Agradecimentos

Primeiramente gostaria de agradecer a Deus por ter me dado força para minha persistência e capacidade para a superação das dificuldades apresentadas durante a realização desta formação deste trabalho e formação acadêmica

A meus pais José Carlos Bassetto e Valéria Pereira Tavares Bassetto, irmãos Rafaela T. Bassetto, Gustavo T. Bassetto e avós por ter me compreendido e me ajudado em todos os momentos, sempre me motivando.

Sem esquecer-se das grandes amizades dos meus parceiros de classe que começamos juntos o curso no segundo semestre de 2010, que são eles: Kelvin Horiuchi, Elielson Barbosa, Fernando Mossatto, Paulo César Barbieri, Victor Ronchi Garcia e Guilherme Zucato.

E finalizando deixo aqui meu muito obrigado ao Fabio de Sordi Junior pela troca de experiência durante a orientação deste trabalho final e a todos os professores que foram meus docentes no decorrer destes anos, com quem aprendi muitas coisas, assim me ajudando na minha vida profissional e pessoal.

RESUMO

O roubo de informação on-line é muito utilizado por indivíduos mal intencionados e se tem varias maneiras de se praticar este crime, um deles é o phishing que é um ataque que visa roubar informações sigilosas tanto de usuários comuns como de organizações, instituições e outros; esta prática é através de e-mails e páginas falsas. Nesse trabalho, é apresentado através da ferramenta desenvolvida, “Anti-Phishing”, de como identificar oque é *phishing* e suas técnicas por meio de um conteúdo dinâmico e interativo, assim com essa identificação os usuários pode navegar com mais segurança e cautela, sendo que esta ferramenta foi testada e validada conforme descrito no decorrer deste trabalho.

Palavras-chave: Phishing, Anti -Phishing.

ABSTRACT

The theft of private information online has been often used and there are many ways of practice this crime, one of these crimes is “Phishing” which has been more and more used as many as individual users and organizations or institutions in order to the theft of private information through e-mails and fake websites. In this paper,it will be presented what is “Phishing” and some techniques to avoid this crime, the main purpuse of this paper is creating and validating the developed tool, "Anti-Phishing". In this work we developed and presented through the Anti-Phishing tool to identify what it is and their phishing techniques trough a more interactive and dynamic content with this identification so the users can navigate more safety and caution, this ferramenta been tested and validadted as described during this.

Key-words: Phishing, Anti-Phishing.

Lista de Figuras

Lista de Gráficos

Lista de Tabelas

SUMÁRIO

1 INTRODUÇÃO

Atualmente com o avanço tecnológico se torna cada vez mais presente e desenvolve um papel primordial na comodidade das vidas das pessoas e a maneira de como elas realizam suas atividades rotineiras (Mayora et al.,2008).

Conforme o crescimento no acesso da Internet a mesma avança e a sociedade se adapta a este meio, assim surgindo cada vez mais tipos de fraudes, as quais a Internet não disponibiliza mas proporciona o crescimento desse crime.

O crime virtual tem vários arquétipos sendo que a ferramenta desenvolvida irá apresentar ao usuário como identificar *phishing*. O termo *phishing* é dado a pessoas que visam roubar informações pessoais, sendo que estas se passam por outras, sejam elas físicas ou jurídicas a fim de obter os dados ou informações por meio de páginas falsas, formulários e e-mails.

Um outro conceito segundo (KIRDA; KRUEGEL, 2005), *phishing* é o nome dado ao se praticar este tipo roubo de informações sensíveis, como senhas bancárias on-line, informações de cartão de crédito, senhas e e-mails, senhas de redes sociais e outras.

Conforme Yue e Wang (2008), os ataques de *phishing* são geralmente transmitidos via e-mails ou mensagens instantâneas, em uma tentativa de conquistar os destinatários através de sites falsos, que para serem acessados exigem informações credenciais ou algum tipo de cadastro. Porém, segundo E-gov (2013), o *phishing* também pode se promover através de banners falsos, IRC[1], programas e trojans, que levam o usuário a páginas falsas.

Com este conceito apresentado sobre oque é *phishing* e o meio que o mesmo utiliza para se propagar; a ferramenta desenvolvida se faz necessária para ajudar os usuários a aprender conceitos e dicas de como se identificar e se prevenir contra essas páginas falsas formulários e outros.

A mesma ensinará o usuário através de um modo interativo e dinâmico, onde o mesmo possa identificar páginas falsas, formulários e e-mails apenas analisando a URLs Layout e alguns detalhes.

[1] “Internet Relay Chat”

A ferramenta foi dividia em níveis para apresentar o conteúdo da melhor forma possível; a mesma foi testada através de métodos descrito neste trabalho, e após os testes da ferramenta grupo de usuários passaram por uma simulação de *phishing* através de passos dessa simulação que também é apresentado no decorrer deste. E com base nos resultados analisado desse treinamento é simulação do *phishing* é de onde surge a conclusão conforme descrita.

1.1 Contextualização

Os ataques de *phishing* está muito presente sendo que todos que utiliza a internet pode ser alvo a qualquer momento no decorrer do dia a dia que utilizam a Internet para trabalho e ou uso pessoal. O *phishing* é uma espécie de fraude na rede que tem como características tentar adquirir informações sigilosas de usuários com apresentação de páginas falsas da Internet. Com a mesma aparência de empresas, bancos ou instituições governamentais e não governamentais entre outros.

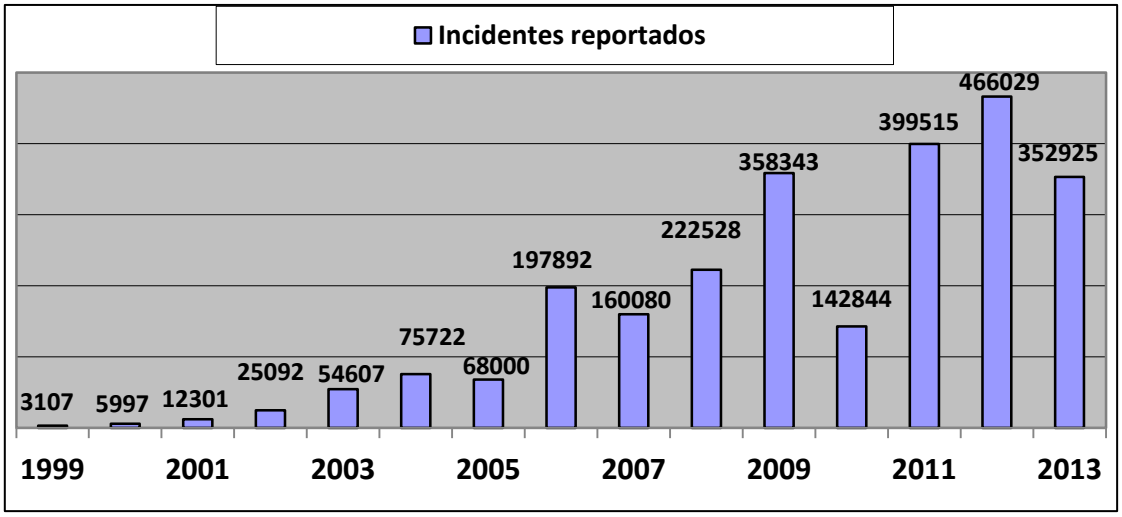
Um dos meios mais utilizados de transmissão, que leva os usuários a essas falsas páginas é via e-mail, que geralmente contém algum texto que exigirá uma rápida ação do usuário ou apresentará algo curioso e vantajoso, sempre pedindo para que esse acesse um link ou que clique nas imagens que a mesmo possui. Esses links e imagens sempre redirecionam para as páginas de *phishing*.

Os ataques por esse tipo de fraude vêm aumentando muito. Segundo Lab (2013) o número de ataques aumentaram em 87% nos últimos doze meses (Junho de 2012 à junho de 2013) passando de 19,9 milhões para 37,3 milhões.

Grandes empresas como o Facebook, Yahoo, Google e Amazon são os principais alvos, pois o e-mail que era a forma mais tradicional de transmissão obteve apenas 12% de todos ataques sendo que os 88% restantes são de links que levam os usuários a páginas de fraudulentas.

De acordo com Cert.br (2013) que é o “Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil”, os números de incidentes reportados por ano ao Cert.br vem tendo um aumento significativo ao passar dos anos, conforme no Gráfico 1

Gráfico 1 - (Cert.br, 2013), Total de Incidentes Reportados ao Cert.br por Ano.



Lembrando que esses números são os valores totais de incidentes no Brasil, são obtidos através da soma de diversos tipos de ataques que foram classificados em:

- Worm (são notificações de atividades maliciosas relacionadas com o processo de propagação de códigos maliciosos na rede);
- Dos (Denial of Service, notificações de negação de serviço);
- Invasão (em caso de acesso não autorizado a um computador ou rede);
- Web (quando os ataques visam o comprometimento de servidores Web ou reconfigurações dos mesmos);
- Scan (tem como característica identificar quais computadores e serviços estão ativos);
- Fraude (englobam as notificações de tentativa de roubo, com o objetivo obter vantagem);
- Outros (são incidentes que não se enquadram nas categorias anteriores).

A seguir, na Tabela 1, relacionada ao ano de 2013, podemos acompanhar os números dos ataques no brasil separados conforme a classificação acima citada.

Com base nos dados, pode-se perceber a evolução dos ataques representados em quantidades. Também observa-se que a cada ano os números tem uma variância porem com a tendência de aumento, ressaltando que no ano de dois mil e treze a análise está na faixa de trezentos e cinquenta mil, o que é relativamente é um numero alto.

Uma informação relevante que podemos observar na tabela é que 24% ou seja 84702 ataques é do tipo de fraude onde o *phishing* se encaixa isso somente aqui no Brasil e são a reportados. Segundo Cert.br (2013), estes 84702 mil ataques são divididos em:

64.25% Páginas Falsas (Tentativas de fraudes)

27.40% Cavalos de Tróia (Objetivo de fraude financeira)

5.92% Direitos Autorais (Cometendo violações)

2.44% Outras (Outras tentativas de fraude)

Tabela 1 - (Cert.br, 2013), Totais Mensais Classificados por TIpo de Ataque de Janeiro a Dezembro.

Mês	Total	Worn	Dos	Invasão	Web	Scan	Fraude	Outros
Jan	36067	6%	0%	5%	3%	52%	17%	14%
Fev	26471	5%	0%	4%	5%	47%	21%	15%
Mar	8090	6%	0%	6%	3%	49%	18%	15%
Abril	29943	6%	4%	5%	5%	44%	22%	14%
Mai	23409	5%	6%	4%	4%	44%	22%	15%
Jun	29713	6%	0%	6%	7%	52%	17%	12%
Jul	30874	9%	0%	1%	5%	44%	24%	13%
Ago	28531	7%	0%	1%	6%	43%	28%	12%
Set	31482	7%	0%	1%	5%	50%	27%	8%
Out	28842	9%	0%	2%	3%	45%	28%	9%
Nov	30213	9%	0%	1%	7%	43%	29%	8%
Dez	29290	10%	2%	1%	4%	40%	35%	5%
Total	352925	7%	3%	3%	5%	46%	24%	12%

Para obtermos um panorama mais abrangente de como vem aumentando esse tipo de crime vamos visualizar alguns dados globais, que Apwg (2013), *Anti-Phishing Working Group* que é uma coligação mundial de unificação da resposta global ao *cibercrime* em todos os setores da indústria, do governo e de aplicação da lei, que aconselha governos nacionais, organismos globais de governança, grupos de comércio do hemisférico global, entre outros.

Na Tabela 2 **– (APWG, 2013), países que hospedam sites de *phishing***, veremos uma relação de quais países estão hospedando sites de *phishing*.

Fazendo a analise percebe-se que o Brasil hospeda uma pequena parte na hospedagem dos sites fraudulentos que aparecem nos três meses do segundo trimestre de 2013 com algumas variações. Porém se realizarmos comparações com o relatório publicado em abril de 2012 que avaliou de julho a dezembro de 2011, e comparando o mesmo com os dados atuais é visível o aumento da hospedagem de sites de *phishing* no Brasil.

Tabela 2 – (APWG, 2013), países que hospedam sites de *phishing*.

Abril (%)		Maio (%)		Junho (%)	
United States	32.21	United States	44.03	United States	45.47
Hong Kong	19.38	Russian Federation	11.58	Kazakhstan	7.11
Russian Federation	7.67	United Kingdom	4.79	France	6.78
Germany	4.37	Germany	4.43	Germany	5.73
Canada	3.96	Finland	3.92	Canada	4.31
Brasil	3.54	Turkey	3.67	United Kingdom	3.11
Angola	2.68	Canada	3.38	Brasil	2.45
United Kingdom	2.42	Brasil	2.17	Turkey	1.70
France	2.33	Indonesia	1.90	Malaysia	1.58
Thailand	2.15	Ireland	1.56	Ukraine	1.40

Conforme Apwg (2013), os destaques estatísticos do mês de abril maio e junho de 2013 são conforme na Tabela 3.

Tabela 3 - (APWG, 2013) Destaques Estatísticos.

	Abril	Maio	Junho
Número de notificações de *phishing* por e-mail.	20,086	18,297	14,698
Número de sites de *phishing* detectados	36,480	44,511	38,110
Número de marcas alvo de campanhas de *phishing*	441	431	425
País que hospeda mais sites de *phishing*	USA	USA	USA
Contém algum tipo de nome de destino na URL	50.92%	57.45	51.52%
No hostname, endereço IP apenas	4.57%	5.23%	5.26%
Porcentagem de locais que não usam a porta 80	0.38%	0.45%	0.80%

Os ataques mais visados nos setores da indústria conforme Apwg (2013) estão divido em: serviços de pagamentos, 47.60%; varejo / serviço, 7.88%; ISP, 8.00%; redes sociais, 2.03%; leilões 2.19%; *gaming*, 2.03%; governo, 2.46% e classificados com 0.49%.

Com base em todos esses dados levantados acima conseguimos analisar que os números vêm aumentando com o decorrer do tempo.

1.2 Formulação e Escopo do Problema

A falta de informação e o modo de como a mesma é transmitida é o que faz a diferença. Atualmente muitos usuários não tem interesse em buscar

informação sobre como identificar um *phishing*, ou quando se tem o interesse, este acaba sendo desmotivado pelo fato de como o conteúdo é apresentado.

Para motivar este interesse em saber o que é o *phishing*, faltam ferramentas ou outros meios de apresentação deste conteúdo de forma interativa e prática.

Ou seja para contribuir com a redução em relação ao numero de incidentes de *phishing;* precisa ter além dos filtros e antivírus já existentes a melhora e investimento na engenharia social; a união destas duas formas de identificação de *phishing* a rede e seus usuários é menos vulnerável e estaria mais preparado para lidar com estas fraudes.

1.3 Justificativa

O mundo capitalista e a necessidade do consumismo por produtos, novas versões ou qualidade, fez com que o mercado de venda se tornasse mais tecnológico de modo que deixe o processo de compra ou venda mais ágil e simples. Assim as organizações e ou instituições começaram a utilizar deste meio tecnológico facilitando o funcionamento e promovendo também a satisfação dos clientes e das próprias empresas e instituições.

E através deste contexto, alguns indivíduos praticam crimes virtuais. Normalmente, se passam por grandes empresas, instituições e outros, com o intuito de pegar as informações para utilizá-la de forma ilícita.

O numero crescente de incidentes conforme abordado, se da por falta da disseminação de conteúdo, informação e falta de treinamento; sendo que estes deve abordar como deve-se agir para identificar um *phishing; sendo assim à necessidade da ferramenta desenvolvida*

1.4 Objetivo

Este trabalho tem como finalidade implementar e validar uma ferramenta de treinamento sobre *phishing* com o objetivo de capacitar os usuários e torna-los menos vulneráveis apresentando dicas para se identificar páginas falsas, formulários e outras formas de fraude..

1.4.1 Objetivos Específicos

- Criar uma ferramenta de treinamento Anti-Phishing;
- Validar a ferramenta simulando uma fraude através de um e-mail e um formulário falso;
- Verificar a eficiência da ferramenta.

1.5 Organização do Trabalho

Na continuidade deste trabalho, a fundamentação teórica irá tratar de questões das variadas fraudes na Internet, incluindo o *phishing* e seus tipos.

Será também apresentado o conceito e alguns exemplos de cada tipo de fraude.

Posteriormente, a seção métodos apresentará a metodologia de trabalho, a forma de realização do mesmo e as ferramentas utilizadas como o Lime Survey e o Construct2 e suas descrições.

E também no de correr deste será exibido o modelo de e-mail e de formulário que serão utilizados na pesquisa, assim como as informações sobre a ferramenta desenvolvida, resultados obtidos e conclusões.

2 FUNDAMENTAÇÃO TEÓRICA

Neste capítulo será apresentado conceitos de *phishing*, sendo que a ferramenta foi desenvolvida com base nos mesmos.

2.1 Fraudes na Internet

Segue abaixo algumas classificações de fraudes na internet e seus respectivos conceitos.

- **Furto de identidade:** O furto de identidade é caracterizado quando alguém assume uma identidade que não é a própria, segundo Cert.br (2013), é quando uma pessoa usufrui dos dados de outros para se passar por ela assim atribuindo-se uma falsa identidade. Esse furto de identidade tem como objetivo obter vantagens indevidas, e essas vantagens permite que terceiros possam abrir contas bancárias, compras com cartões de créditos, recebimento de benefícios, acesso a páginas pessoais e outros. Alguns dados como exemplo de furto de identidade conforme Microsoft (2013), são: senhas, nomes de usuários, informações bancárias, números de cartões de créditos e outros.
- **Fraude de antecipação de recursos:** É aquela que de alguma maneira o golpista procura induzir a fornecer informações confidenciais para realizar um pagamento adiantado, com promessa de futuramente receber algum tipo de benefício por exemplo.

Alguns exemplos mais comuns segundo a Cert.br (2013):

- “loteria internacional”, onde se recebe um e-mail informando que foi sorteado com uma quantia alta, porém para receber a mesma é necessário passar dados pessoais e informações sobre a conta bancária;
- “crédito fácil”, recebe via e-mail ou propagandas relâmpagos enquanto navega oferecendo empréstimos com boas quantias e juros baixos, assim ao se preencher um formulário de cadastro o crédito já é aprovado, em

seguida é solicitado a realização de depósitos para que as despesas sejam pagas despesas iniciais.

E outros do tipo em que solicitaria algum recurso próprio com promessa de rendimentos ou algum lucro futuro.

- **Golpes de comercio eletrônico:** esse golpe tem como objetivo conforme Cert.br(2013) apenas obter vantagens financeiras através das páginas fraudulentas. Os usuários são atraídos por questões de melhor preço, e realizam compras por este motivo, contudo, o principal problema é o não recebimento da mercadoria. Os mesmos são divulgados através de e-mails, anúncios e links patrocinados.

  Conforme o Guia de comércio eletrônico Procon (2013), é necessário obter alguns cuidados ao realizar compras ou contratações por meio da Internet, são eles: Refletir sobre seus interesses, não comprar por impulso; procurar identificar o fornecedor, procurar informações adicionais sobre a empresa e conferir os mesmos; buscar referências, com amigos e pesquisas e no SINDEC[2]; observar a segurança eletrônica; e outros.

2.1.1 Phishing

Segundo Irani et al.,(2008),"O *phishing* é uma forma on-line de fraude na internet, a qual o invasor ser passa por outra pessoa ou instituição a fim de obter informações das vítimas". Estas informações normalmente são dados confidenciais como, e também dados relacionados a instituições financeiras como os dados bancários e de transações financeiras. O fator comum a todos os ataques de *phishing* é que sempre as vítimas sofrem algum prejuízo.

Apesar de *phishing* ser classificado como *spam*, ele se difere de spam. O spam tenta vender um produto ou serviço, enquanto uma mensagem de *phishing* é olhada como de uma organização legítima. Devido à semelhança entre mensagens, algumas técnicas que são aplicadas para mensagens de spam não podem ser aplicadas para *phishing*. (IRANI et.al, pg.2 (2008).

[2] SINDEC: Sistema Nacional de Informações de Defesa do Consumidor.

De acordo com Apwg (2013), *phishing* é um mecanismo criminoso, onde usam técnicas para roubar informações de consumidores como dados de identificação pessoal e credencial da conta financeira e outras conforme já citadas. Usam e-mails se passando por empresas legítimas, agências, instituições e outros, onde o objetivo é levar os consumidores a falsos sites que acaba enganando os usuários assim roubando as credenciais diretamente, muitas vezes usam-se sistemas para interceptar nomes de usuários e senhas de contas online BB.

2.1.2 Tipos de *Phishing*

Segundo (Kirda, Kruegel 2005 p.2), "Os ataques de *phishing* se dividem em várias categorias. A mais antiga forma de ataques de *phishing* foram através de e-mail base em meados dos anos 90."

O Centro de Estudos, Respostas e Tratamento de Incidentes de Segurança no Brasil, Cert.br (2013), mostra que as pessoas são atraídas principalmente por: páginas falsas de comércio eletrônico ou Internet Banking; falsas redes sociais; mensagens contendo formulários; mensagens contendo links para códigos maliciosos; solicitação de recadastramento. E com base nesses exemplos a Cert.br desenvolveu a Tabela **4 – (Cert.br, 2013), Exemplos de tópicos e temas de mensagens de *phishing*** 4.

Tabela 4 – (Cert.br, 2013), 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.
Antivírus	Atualização de vacinas, eliminação de vírus lançamento de nova versão ou de novas funcionalidades
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
Cartões virtuais	UOL, Voxcards, Yahoo! Cartões, O Carteiro, Emotioncard
Companhias aéreas	Promoção, programa de milhagem

Continuando Tabela 4.

Tópico	Tema da mensagem
Comércio eletrônico	Cobrança de débitos, confirmação de compra atualização de cadastro, devolução de produtos oferta em site de compras coletivas
Comércio eletrônico	Cobrança de débitos, confirmação de compra atualização de cadastro, devolução de produtos oferta em site de compras coletivas
Comércio eletrônico	Cobrança de débitos, confirmação de compra atualização de cadastro, devolução de produtos oferta em site de compras coletivas
Comércio eletrônico	Cobrança de débitos, confirmação de compra atualização de cadastro, devolução de produtos oferta em site de compras coletivas
Comércio eletrônico	Cobrança de débitos, confirmação de compra atualização de cadastro, devolução de produtos oferta em site de compras coletivas
Comércio eletrônico	Cobrança de débitos, confirmação de compra atualização de cadastro, devolução de produtos oferta em site de compras coletivas
Comércio eletrônico	Cobrança de débitos, confirmação de compra atualização de cadastro, devolução de produtos oferta em site de compras coletivas
Comércio eletrônico	Cobrança de débitos, confirmação de compra atualização de cadastro, devolução de produtos oferta em site de compras coletivas
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
Músicas	Canção dedicada por amigos
Notícias e boatos	Fato amplamente noticiado, ataque terrorista, tragédia natural
Prêmios	Loteria, instituição financeira
Programas em geral	Lançamento de nova versão ou de novas funcionalidades
Promoções	Vale-compra, assinatura de jornal e revista desconto elevado, preço muito reduzido, distribuição gratuita.
Propagandas	Produto, curso, treinamento, concurso.
Reality shows	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.

Continuando Tabela 4.

Tópico	Tema da mensagem
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
Sites com dicas de segurança	Aviso de conta de e-mail sendo usada para envio de spam (Antispam.br) cartilha de segurança (CERT.br, FEBRABAN, Abranet, etc.).
Solicitações	Orçamento, documento, relatório, cotação de preços, lista de produtos.

O e-mail como já citado sendo umas das formas mais utilizadas para propagação do mesmo vem tendo uma caída conforme podemos observar na Tabela 3, essa recaída está relaciona aos serviços de identificação e de relatos dos *phishing* que algumas organizações disponibiliza, a APWG em sua página uma aba "*Report Phishing*"[3], neste local é coletado a mensagem suspeita que usuários colaborados identificam como *phishing* e enviam, por sua vez a APWG realiza uma análise com sua lista e verifica se é um possível nova mensagem de *phishing* ou não.

Assim com essas listas de mensagens de algumas empresas como a APWG, disponibilizam a mesma para melhoria e proteção principalmente junto com serviços de e-mail, para que o mesmo ao receber algumas mensagens já possa considerar a mesma como um *phishing* ou não de acordo com filtros que são feitos com base nesta relação.

Como o e-mail sendo umas das mais utilizadas ainda, Irani et al.,(2008), define que essas mensagens de *phishing* podem ser divididas em dois componentes principais sendo eles: o conteúdo e cabeçalhos da mensagem.

- O conteúdo é subdivido em duas partes que são os locais onde a mensagem se parecerá como a de uma organização legitima e a

[3] http://www.antiphishing.org/report-phishing/

segunda parte é onde o texto tem alguma URLs redirecionando para uma página web falsa.

- O cabeçalho é sub divido em três sendo como: 1) clientes de correio como: “Para:”, “De:”, “Assunto:”; 2) *relays* que adiciona cabeçalhos ao meio da mensagem que pode ser usado para determinar o IP e o caminho percorrido pela mensagem; 3) é onde os Spam-filtros agem e adicionam cabeçalhos a mensagem disponibilizando para o usuário determinar o que fazer.

Outros casos de classificações de *phishing* e seus conceitos seguem a baixo:

- ***Pharming*:** é quando acontece o redirecionamento através do DNS (Domain Name Service), que quando ao acessar um site verdadeiro o próprio navegador redireciona para uma falsa página**.**
- ***Spear Phishing*:** conforme o FBI (2013), *Federal Bureau Of Investigation,* é uma forma mais elevada de *phishing* ainda, pois os alvos são grupos de pessoas como, por exemplo, pessoas da mesma empresa, mesma instituição bancária, faculdade e outros do tipo que caracterizam um grupo de pessoas que realizam atividades rotineiras parecidas. Esses grupos de pessoas são identificadas conforme cada um envia informações para redes sociais e outras páginas que no cadastro solicitam informações que acabam descrevendo o perfil.

3 MÉTODOS

Esse capítulo apresentará os métodos e conceitos utilizados para a elaboração do presente trabalho.

3.1 Metodologia do Trabalho

O presente trabalho tomou como estudo de caso para cumprir os objetivos deste, professores e funcionários da Universidade Estadual do Norte do Paraná – Campus Luiz Meneghel. Este trabalho se enquadra na natureza explicativa com o intuito de propor e testar a ferramenta.

Para o desenvolvimento e a validação desta ferramenta proposta, foi utilizado o Construct2 sendo que a descrição do mesmo segue abaixo.

Após o desenvolvimento a mesma foi disponibilizada para o treinamento. A ferramenta tendo passado por esta etapa foi dado o inicio a simulação de *phishing*, onde dois grupos pessoas foram abordados sendo eles os que passaram pelo treinamento e o outro não.

Para obter os dados estatísticos deste trabalho, após treinamento foi feita uma simulação de fraude direcionada tanto para as pessoas que foram treinadas, quanto para algumas pessoas que não realizaram o treinamento.

Os resultados da simulação de *phishing* foram armazenados e hospedados no servidor da UENP que foi organizado por meio de um formulário que foi criado utilizando o Lime Survey que tem sua descrição abaixo.

Os dados que obtidos são:

- Total de e-mails enviados;
- Notas individuais de cada nível;
- Quantidade de repetição por nível;
- Quantidade de pessoas que realizou o treinamento;
- Pessoas que treinaram e não responderam o falso formulário;
- Pessoas que treinaram e responderam ao falso formulário;
- Pessoas que não realizaram o treinamento mas responderam;

E a conclusão sob a ferramenta e sua validação será extraída com base nestes resultados.

3.2 Lime Survey

O Lime Survey é um sistema de pesquisa online avançada para criar questionários on-line de qualidade. O software é baixado 10.000 vezes a cada mês e é utilizado em todo o mundo por empresas, universidades e indivíduos. O Lime Survey é *software open source* e completamente grátis. Os parceiros do Lime Survey é um grupo de empresas de serviços suportados pelos desenvolvedores do núcleo do Lime Survey.

A ferramenta oferece uma ampla gama de serviços comerciais opcionais para usuários da mesma, incluindo totalmente atendimento e até hospedagem, contratos de suporte remoto, desenvolvimento de código personalizado e consultoria. Os estilos de clientes variam de investigadores individuais até departamentos de formação de empresas e universidades, (LIMESURVEY.ORG, 2013)

3.3 Construct2

O construct2 é uma ferramenta desenvolvida pela empresa SCIRRA, que será utilizada para o desenvolvimento da ferramenta proposta por este trabalho. O mesmo permite a criação de jogos para várias plataformas como: Web(HTML5), iOS, Android, Windows Phone 8, Windows Desktop, Linux Desktop, Blackberry10, Firefox Marketplace, Tizen, Facebbok, Chrome Web Store, Amazon Appstore, (SCIRRA, 2013).

É um criador de jogo Drag-and-drop ou seja, é a ação de clicar em objetos e arrastá-lo para o local desejado e soltar, (arrastar e largar), que desta maneira não exige muito conhecimento técnico da ferramenta pois a mesma é de forma interativa e contém tutoriais em várias línguas. O construct consegue envolver aspectos de programação, design, matemática, colaboração, publicação e Marketing.

3.4 Story Board

Segundo GIED (2013), Story board é a descrição de todas as telas e detalhes que irão compor a ferramenta, pois o mesmo ajuda a visualizar o projeto final, e serve também como material que tem por finalidade servir e auxiliar como guia para o desenvolvedor.

Para melhor entendimento do layout fez-se necessário fazer a divisão do modelo em dois principais tipos, sendo eles conteúdo teórico e prático. Sendo que no teórico trata da questão da roteirização do contexto que contém conceitos e a teoria que refere ao tema abordado, segue como exemplo o modelo de layout na Figura 1, localizada na próxima página. Já no conteúdo prático aborda a questão das atividades em relação ao conteúdo, segue na próxima página o exemplo de layout na Figura 2.

Segue como Apêndice A, neste trabalho o Story board da ferramenta proposta de acordo com os conceitos mostrados pelo Grupo de Informática Educativa.

Figura 1 - Exemplo do conteúdo teórico.

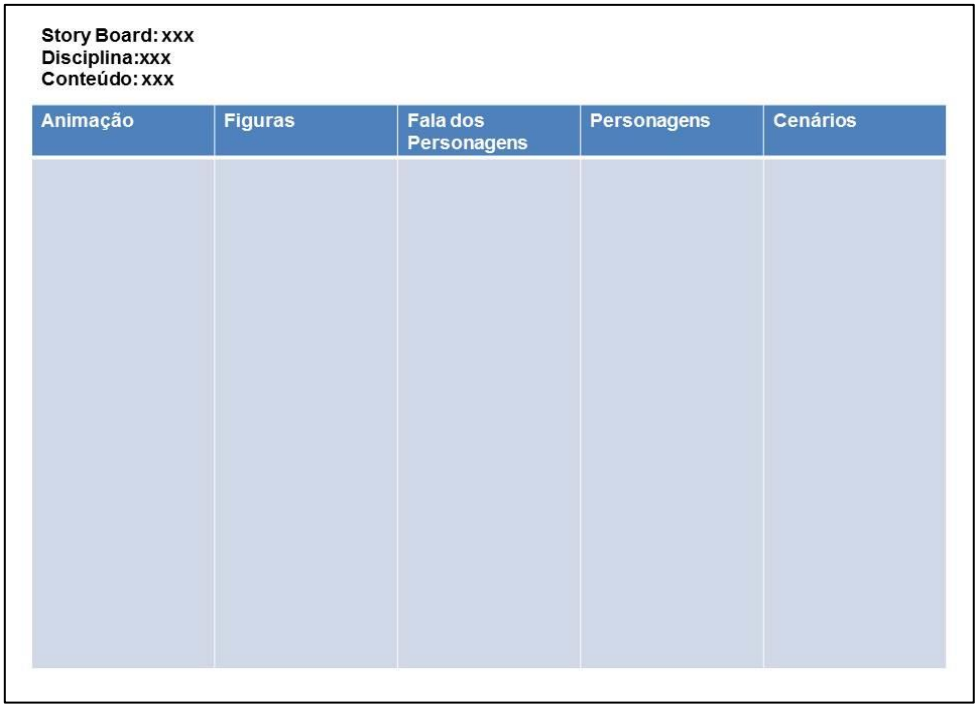
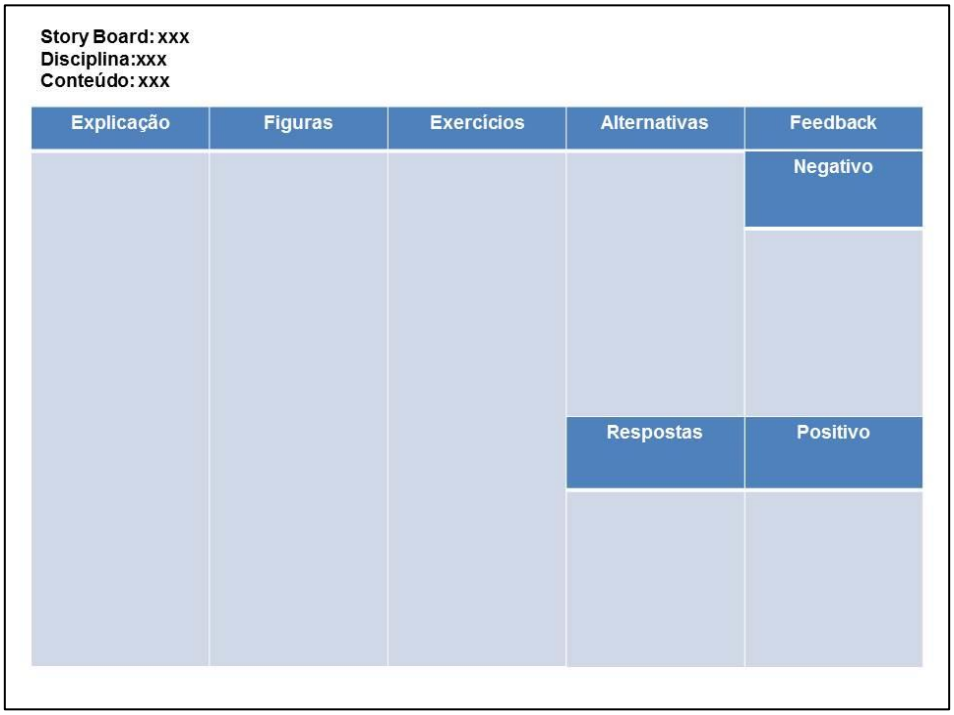


Figura 2 - Exemplo do conteúdo prático.



4 DESENVOLVIMENTO

Neste capítulo será apresentada a ordem que de como o trabalho foi feito e obtido os resultados seguindo um sequencia que está de acordo com dos tópicos abaixo.

4.1 A ferramenta

A mesma foi feita utilizando o Construc2 conforme já citado acima e também foi utilizado um servidor para alocação da mesma e um banco de dados Mysql também alocado ao mesmo servidor 200.195.132.228 que este pertence a UENP; o banco de dados está sendo utilizado para armazenar as seguintes informações: e-mail; pontuação por nível, quantidade que de vezes que fez cada nível, quantidade de ajuda que solicitou em cada nível e a nota de avaliação da ferramenta.

Os dados armazenados e solicitados na ferramenta são apenas estes pois serão estes analisados estatisticamente para obter resultados da validação ou não da ferramenta.

No **nível 01** a pontuação máxima do usuário pode ser de 90 pontos somando 10 pontos a cada acerto sendo que a média mínima é de 50 pontos ou seja para que se vá ao próximo nível tem que ter uma nota maior ou igual à que 55,55%.

Neste nível será abordado questões de URLS e detalhes nas páginas web. Onde as dicas que a ferramenta oferece são:

- Ao analisar a URL que é o endereço virtual de uma página, por exemplo: www.google.com.br , verifique se as imagens na página estão de acordo com ao que você procura.
- A URL do banco Sicredi é: http://sicredi.com.br porém uma página falsa da mesma poderia ser http://ssicredi.com.br
- Verifique se a página como um todo está com todas as imagens carregadas e sem falhas.
- Não se impressione com ofertas onde o valor é muito baixo comparado com vários concorrentes.

- Preste atenção em datas que estiverem na imagem, pois a mesma pode ser de dias ou meses anteriores..
- Procure pelo site em questão por um ferramenta de busca (ex: Google) e confira se a URL e o layout do site é atual.

No nível 01 é apresentada nove páginas diferentes onde seis são falsas contendo falhas conforme citado nas dicas e as outras três são verdadeiras; a pessoa que utilizar tem a opção de escolher entre Verdadeiro ou Falso e tem a opção de Ajuda a qualquer momento que a mesma mostra as dicas já citadas acima.

No **nível 02** o usuário já começa com 140 pontos porém a cada erro é descontado 10 pontos sendo que a média mínima é de maior ou igual á 80 pontos ou seja para ir ao próximo nível tem que ter uma nota maior ou igual à que 57,14%.

Neste nível será abordado questões de URLS similares e sub domínios e diretórios e agregando conhecimento adquirido no nível anterior. Onde as dicas que a ferramenta oferece são:

- Subdomínios são uma ramificação de um domínio, como por exemplowww.seublog.blogspot.com.br, porém podem existir página por exemplo: www.sicredi.algumacoisa.com.br.
- Evite acessar URLS através de propagandas na Internet e pesquise pelo site em questão em uma ferramenta de busca (ex: Google e confira se a URL e o domínio são os mesmos).
- E não estranhe se tiver domínios como por exemplo www.algumacoisa.eco ou com finais do tipo: emp.br; net.br; blog.br; flog.br; edu.br; acr.br; far.br; ind.br; rec.br e vários outros que estão disponíveis em https://registro.br/dominio/categoria.html que é o órgão responsável sobre essas questões.

Neste nível é apresentada quatorze links sendo que seis links são falsos e oito links são verdadeiros diferentes com a opção de escolha na frente se o mesmo é verdadeiro ou falso lembrando que a opção de ajuda esta disponível em qualquer momento da realização deste nível.

No **nível 03** o usuário poderá ter a pontuação máxima de apenas 70 pontos sendo contabilizados 10 pontos a cada acerto sendo que a média

mínima é de maior ou igual á 50 pontos ou seja para ir a tela de avaliação da ferramenta obrigatoriamente tem que ter uma nota maior ou igual à que 71,42% de acerto.

Neste nível será abordado questões de e-mails maliciosos e valores já agregados adquirido nos níveis anteriores. Onde as dicas que a ferramenta oferece são neste nível é:

- Verifique se quem está enviando o e-mail é mesmo a empresa onde trabalha ou onde efetue compras.
- Fique atento ao se cadastrar em sites e se foi permitido o envio de e-mails.
- Cuidado com URL que contém nos e-mails pois elas podem ser falsas conforme já discutido nos níveis anteriores.
- Bancos e lojas online jamais mandarão contas ou boletos para pagar a não ser que tenha permitido.
- Geralmente e-mails contem textos estranhos pedindo para clicar em URLs, verifique se esta URL não termina com .exe; .pif; .src; .bat; pois estas extensões são executáveis e podem fazer um download automático de algum vírus ou programa que não se faz necessário em seu computador pessoal.

Neste são apresentados sete e-mails onde seis são falsos e um é verdadeiro onde que na analise e com base nas dicas e conhecimento já adquirido anteriormente o usuário deve escolher entre o e-mail ser falso ou verdadeiro e também tem a disponibilidade de pedir ajuda caso o mesmo esqueça-se de alguma dica.

Após ter passado o terceiro e ultimo nível o usuário estará na pagina final onde o mesmo deve escolher uma nota para a ferramenta onde 0 é muito ruim e 5 é muito bom, após está escolha o mesmo pode escolher em realizar o treinamento novamente ou simplesmente sair.

Mais detalhes sobre a ferramenta, como sua arquitetura, descrição e designe podem ser encontrados no Story Board que se encontra no ‘Apêndice A’ deste trabalho.

4.2 Validação da ferramenta

Para validação da mesma foram feitas duas abordagens onde foi tradada a abordagem onde um determinado grupo de pessoas passou pelo treinamento e o outro grupo de pessoas não passou sendo assim temos pessoas que tem conhecimento sobre *phishing* adquirido por meio da ferramenta e pessoas que não tem conhecimento de *phishing* por meio da ferramenta.

4.2.1 Treinamento

Aplicação da ferramenta foi feita de forma presencial em um dos laboratórios de informática do Campus, porém realizada de forma totalmente online e individual. O objetivo de se realizar a aplicação desta maneira é identificar possíveis dificuldades de interação com a ferramenta por parte das pessoas que se inscreveram para utilizá-la.

A divulgação do treinamento foi feito através de um e-mail enviado pela administração do campus CLM contendo um link para um formulário de inscrição que permitia a escolha de uma data (11, 14, 15 ou 16 de maio de 2014) para a realização do treinamento.

Apesar de haver uma data para realização do treinamento, a ferramenta continuaria disponível para utilização em outros momentos, podendo ser acessada de qualquer local através do site: http://nti.uenp.edu.br/site/index.php?option=com_content&view=article&id=94&Itemid=97.

4.2.2 Simulação do *Phishing*

Para a criação dos formulários de *phishing* será utilizada a ferramenta Lime Survey. que possui diversas opções na criação de formulários, para o e-mail será utilizado o serviço disponibilizado na web pelo Hostinger descrito mais abaixo.

Para a realização da estatística dos dados foi disparado o total de 100 e-mails, sendo estes para professores e funcionários administrativo do campus CLM, o mesmo conteve o seguinte texto:

Recadastre Sua Conta E-mail da UENP

Devido ao grande numero de contas de e-mail cadastradas em nosso servidor, surgiu a necessidade de um recadastramento de usuários para termos a certeza das contas de e-mail que são realmente utilizadas, apagando todas as demais contas, para assim melhorarmos nosso serviço de e-mail.

Para efetuar recadastramento, clique aqui e preencha o formulário.

Atenção: Os usuários que não efetuarem o **recadastramento no prazo máximo de 5 dias** a partir do recebimento deste e-mail terão suas contas permanentemente apagadas dos nossos servidores. Evite transtornos, recadastre-se já.

Código de Verificação: UENP201465347856.

Este e-mail foi criado automaticamente pelo grupo de recadastramento dos e-mails institucionais da UENP.

Ao lermos o texto podemos perceber que ele trás um problema que a UENP está passando e pede a colaboração de todos. No decorrer do texto o mesmo utiliza um gatilho visceral que segundo WANG et al.(2012), tem por objetivo dar ênfase na urgência da resposta do mesmo, assim quem o lê o texto acaba sendo manipulado de certa forma e com isso os mesmos reduz a capacidade de processar a informação permitindo a ocorrência de erros de decisão.

O gatilho visceral é chamativo para que os destinatários respondam o mesmo imediatamente. Na palavra “clique aqui” que está como hiperlink redirecionando para o link[4].

O e-mail foi disparado com o seguinte endereço eletrônico: uenp_clm@uenp.esy.es que está hospedado em um servidor criado somente

[4] http://200.201.24.20/sistemas/survey/cct/index.php/736152/lang-pt-BR

para estes testes com o endereço: http://uenp.esy.es/ que esta utilizando o serviço do site da Hostinger (http://www.hostinger.com.br/) que oferece este serviço gratuitamente.

O e-mail disparado contém a seguinte falha no final do endereço sendo está @uenp.esy.es, lembrando que se fosse um e-mail verdadeiro da instituição, este seria com o final @uenp.edu.br.

O formulário conforme já citado acima foi criado utilizando a ferramenta Lime Survey que está instalada no servidor 200.201.24.20 que pertence a instituição UENP. Para que não fosse necessária a alocação em um servidor fora da instituição, foi utilizado o numero de IP do servidor ao invés do nome para que os usuários tratassem a mesma como uma URL suspeita.

O Formulário foi divido em duas partes: a primeira pede somente o endereço de e-mail e tem o símbolo da instituição assim como pode-se ver na Figura 3.

Esclarecendo que as informações solicitas não são confidenciais pois as mesma já estão disponível no site: http://clm.uenp.edu.br/.

Figura 3 - Primeira parte do formulário

A segunda parte do formulário pela seguintes questões:

- Escolha o grupo de Trabalho: Docente ou Administrativo

Se a resposta for docente então aparece a questão que pergunta em qual curso que o mesmo ministra aulas e se a respostar for administrativo aparecera a questão pedindo pra escolher qual a opção os serviços são prestados. Pode-se escolher em ser docente e administrativo ao mesmo tempo também, e após responder as questões é só clicar em enviar, segue abaixo Figura 4.

Figura 4 - Segunda Parte do falso formulário

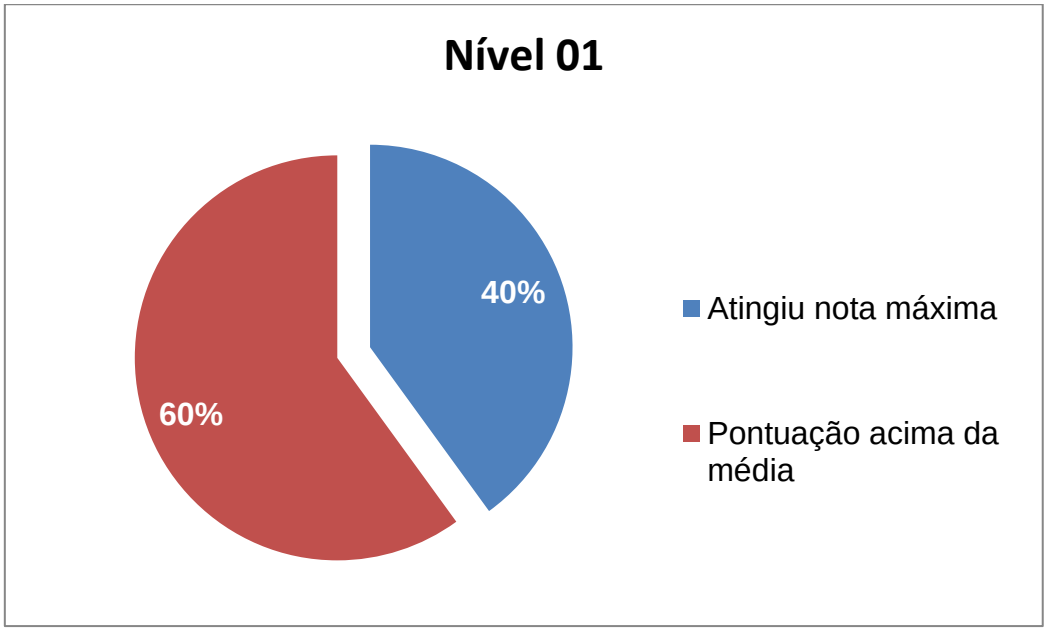
5 Resultados obtidos

Com a realização do treinamento e a simulação de *phishing* obteve-se os resultados que serão discutidos a partir deste momento.

5.1 Resultados do treinamento

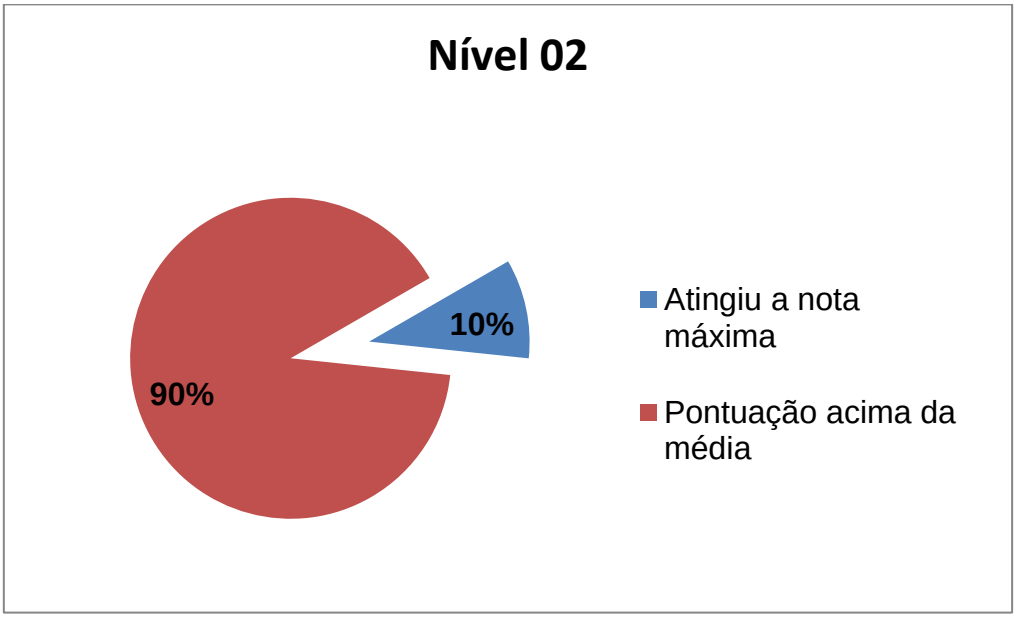
Ao final do treinamento no formato presencial, foram contabilizadas as participações de 20 pessoas. Os resultados desta fase serão descritos a seguir, organizados de acordo com os níveis da ferramenta.

Gráfico 2 - Pontuação nível 01



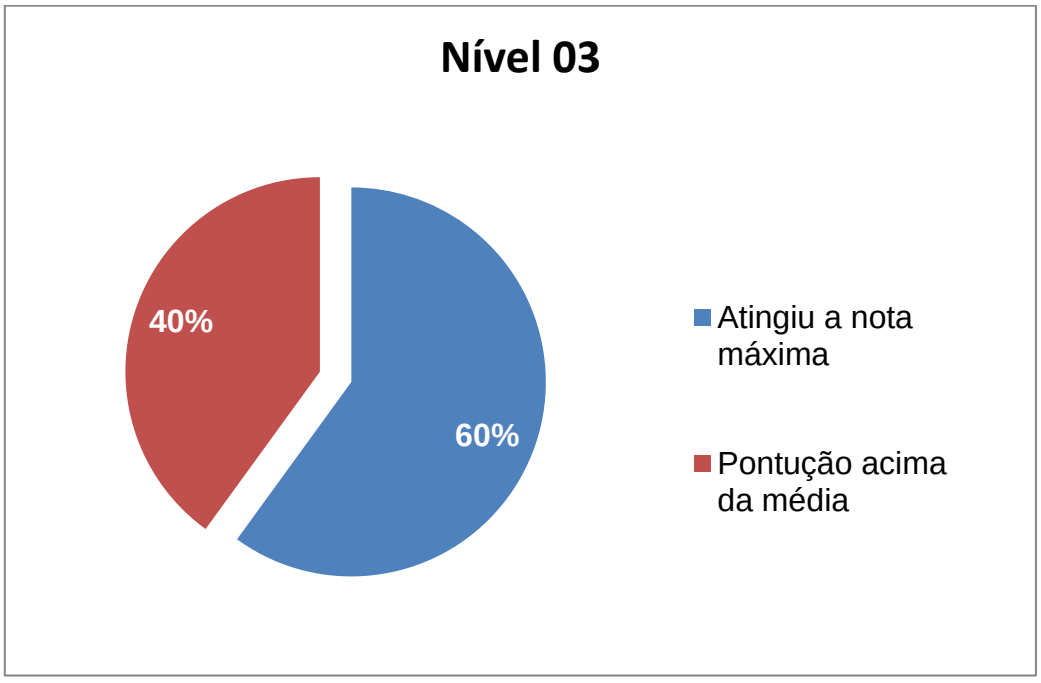
O nível 01 trata das questões de URLS e detalhes nas páginas conforme citado anteriormente, assim podemos perceber na Figura 6, que 40% dos participantes atingiram a nota máxima, sendo que o restante também conseguiu a pontuação exigida para mudar de nível.

Gráfico 3 - Pontuação nível 02



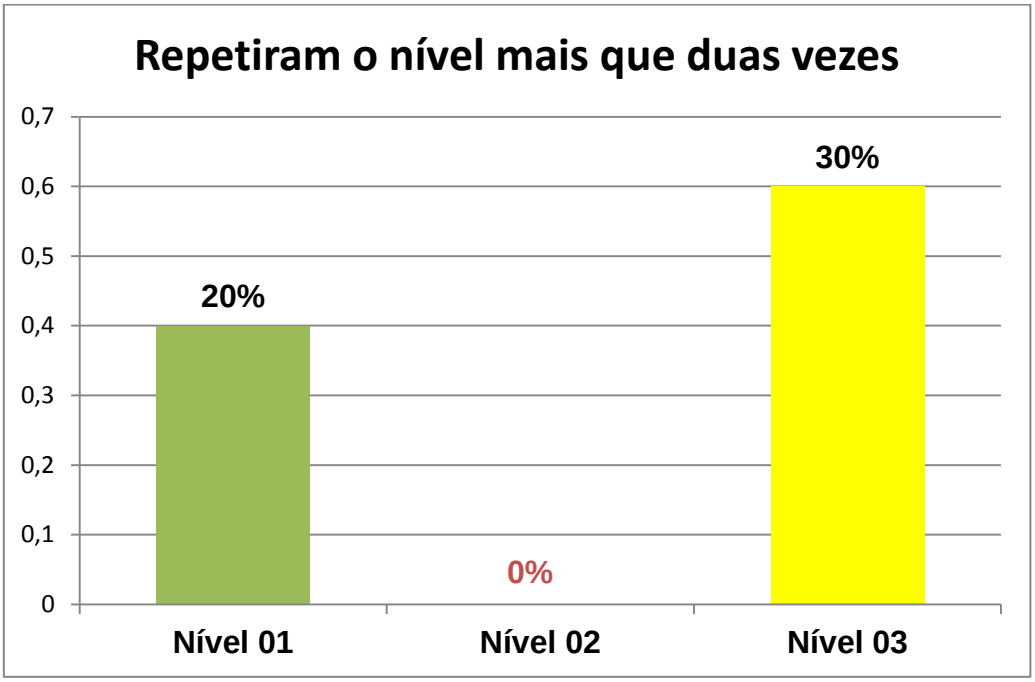
O nível 02 trata de questões de URLs, domínios e subdomínios conforme explicado anteriormente, assim podemos acompanhar na Gráfico 3, que houve uma porcentagem baixa de pessoas que atingiram a nota máxima neste nível, e a maioria dos participantes acabaram fazendo apenas os pontos necessários para avançar para o próximo nível.

Gráfico 4 - Pontuação nível 03



Por fim, o nível 03 trata de questões de e-mails falsos. De acordo com o Gráfico 4, podemos verificar que houve uma melhora na porcentagem relacionada a quantidade de pessoas que atingiram a nota máxima neste nível.

Gráfico 5 - Índice de repetição.



Conforme se pode ver no Gráfico 5, que este esta separado por nível foi extraída as seguintes informações. Para analise considere que 20 pessoas que realizaram o treinamento é igual a 100%.

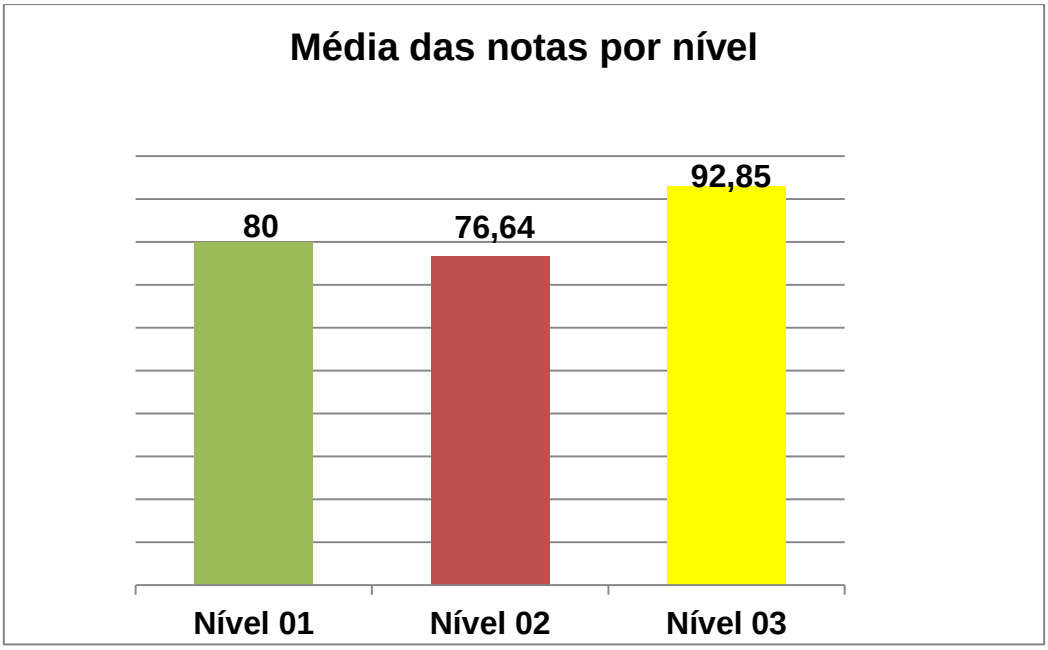
No primeiro nível 20% das pessoas não conseguiram atingir a nota mínima para mudar de nível, assim tiveram que refazer o mesmo até atingir a nota mínima ou superior. No segundo nível 0%, ou seja, ninguém que realizou o treinamento precisou refazer este nível, pois todos conseguiram obter uma nota para trocar de nível.

Já no terceiro foram 30% das pessoas que precisou refazer este nível para adquirir a nota mínima.

Com esta analise afirma que no nível 01 e 03 teve um índice maior de reprovas. Sendo que isso pode ser em decorrência do assunto que os níveis tratam, sendo assim os mesmos pode se tornar mais difícil em relação das pessoas que realizaram o treinamento, não ter conhecimento sobre o assunto.

Com o foco na analise das notas tiramos uma média de nota por nível conforme podemos perceber no Gráfico 6.

Gráfico 6 - Média das notas por nível



De acordo com os dados do Gráfico 6, percebemos que no nível 03 teve uma media de nota superior aos ostros níveis, mesmo ele tendo um índice de reprova maior conforme no Gráfico 5.

Após se passar pelo nível 03, os participantes avaliaram a ferramenta em uma escala de 0 a 5, onde 0 significa MUITO RUIM e 5 significa ÓTIMO. O resultado desta avaliação, obtido através da média das respostas foi 4.8, mostrando a aprovação da ferramenta por parte dos que utilizaram.

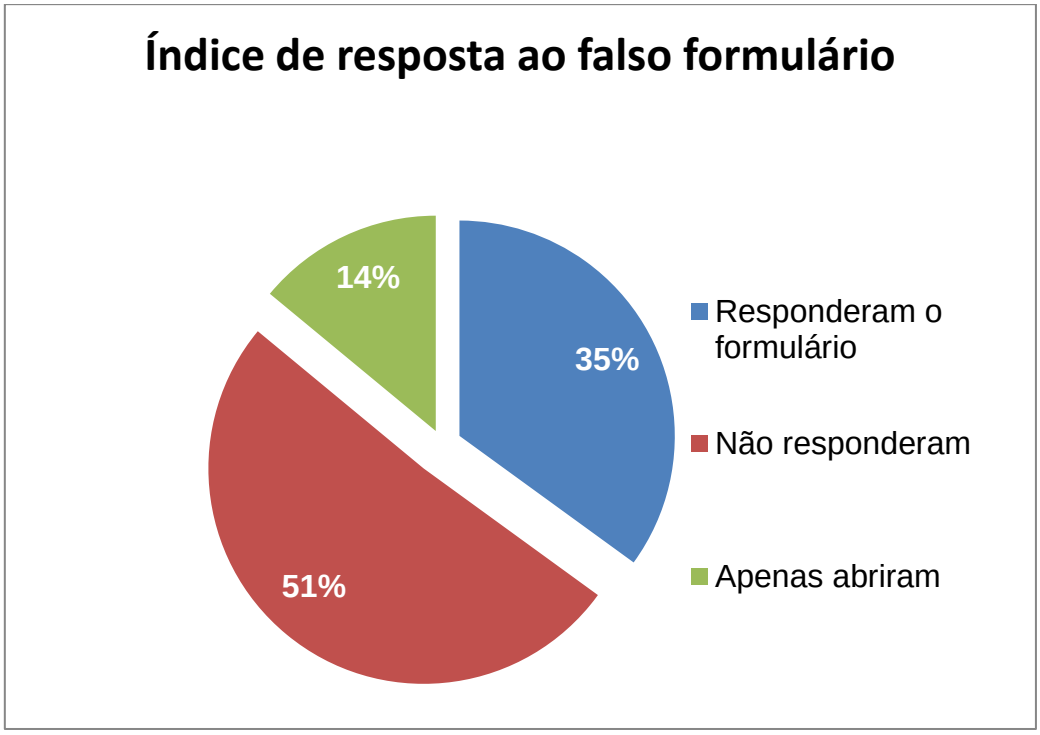
5.2 Resultados da Simulação

Como já citado, foi enviado um total de 100 e-mails utilizando o texto e endereço citado acima. Evocando que estes e-mail estão disponível na rede para qualquer pessoa acessar conforme já citado no item 4.2.2 acima.

O falso formulário foi respondido num total de 49 vezes, ou seja, o e-mail contendo o falso formulário (*phishing*) foi enviado para cem pessoas ou 100%, e 49% destas pessoas acessaram o falso formulário, porém apenas 35% responderam com dados validos preenchendo o formulário conforme o

mesmo solicitava e 51% não respondeu e nem abriu. Podemos visualizar isto no Gráfico 7.

Gráfico 7 - Índice de resposta ao falso formulário.



5.3 Resultados da validação

De acordo com os resultados acima apresentados e filtrando as informações alcançamos os índices que irá auxiliará chegar numa resposta precisa em relação a eficiência da ferramenta.

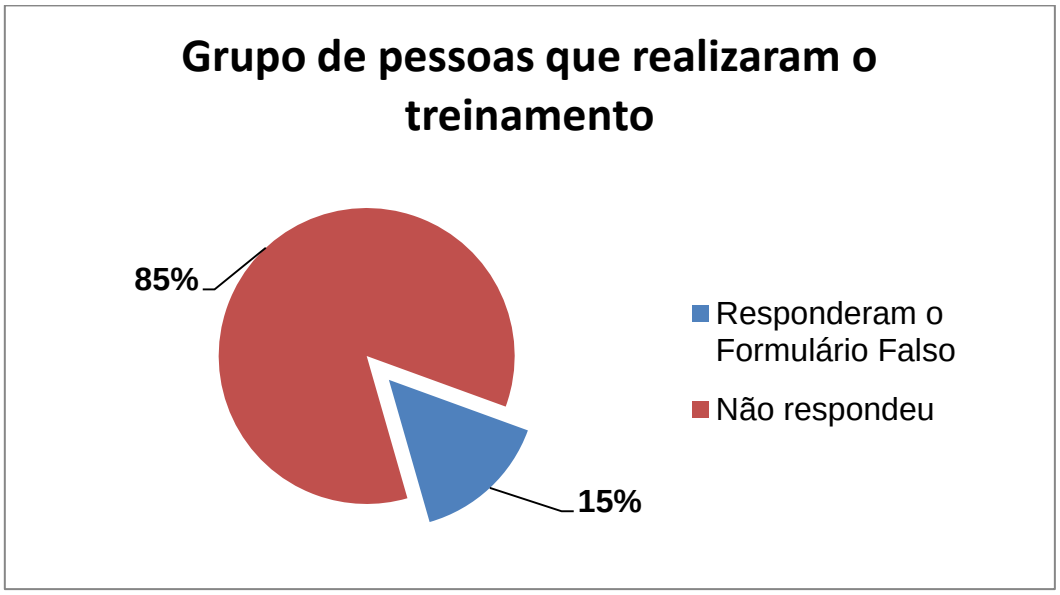
Observando o Gráfico 8, ou seja, num grupo total de cem pessoas ou 100%, oitenta pessoas ou 80% não realizaram o treinamento.

Destes 80%, a quantidade que respondeu o formulário com dados válidos foi de 40% e que não respondeu foi de 60%. Assim o numero de pessoas que não realizou o treinamento respondeu o formulário foi de trinta e duas.

Gráfico 8- Grupo de pessoas que não realizou o treinamento

No Gráfico 9, abaixo temos os dados de quem realizou o treinamento, ou seja, das 20 pessoas ou 20%. Destes que realizaram o treinamento 15% ainda responderam o formulário. Assim de um total de vinte pessoas três responderam o formulário.

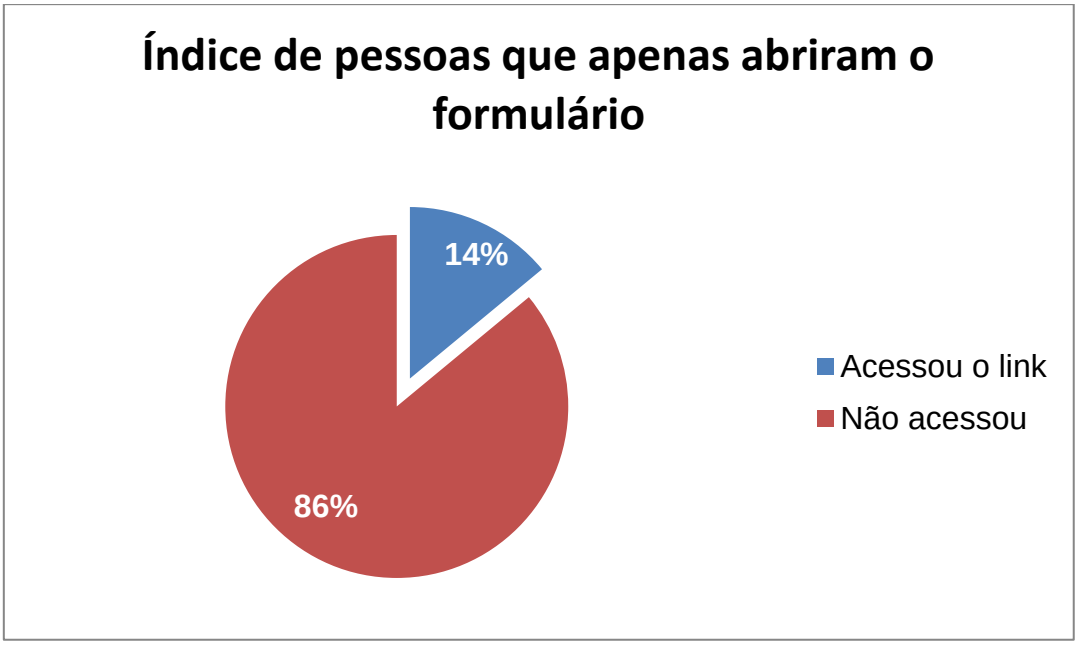
Gráfico 9 - Grupo de pessoas que realizou o treinamento



O Gráfico 10 mostra que 14% das pessoas que receberam o formulário apenas o abriram, ou seja, das cem pessoas que receberam o formulário quatorze pessoas identificaram a necessidade de abrir o mesmo, porem elas

não responderam, ou se responderam preencheram com dados inválidos, que não apresentavam informações coerentes, como e-mails válidos.

Gráfico 10 - Índice de pessoas que apenas abriu o formulário



6 CONCLUSÃO

Analisando os resultados obtidos e considerando as duas abordagens, que são o grupo de pessoas que realizou o treinamento e o grupo que não realizou, que foi necessária para a simulação do *phishing podemos* observar que quem não fez o treinamento teve um índice maior de resposta à simulação de *phishing* comparando com o grupo que realizou o treinamento.

Com base nessas afirmações e resultados apresentado podemos concluir que a ferramenta teve um desempenho mostrando uma redução de 37,5% na quantidade de pessoas vitimadas pela fraude tratada neste trabalho.

Além da redução na vulnerabilidade das pessoas que utilizaram a ferramenta, a avaliação desta, mostrou que seus utilizadores aprovam a forma que a ferramenta aborda o conteúdo.

Concluindo e comprovando que este tipo de ferramenta e ou treinamento se faz necessário em organizações ou apenas no âmbito pessoal para ajudar a diminuir a vulnerabilidade contra este tipo de ataque. Também se conclui que com a utilização desta ferramenta e/ou um pouco mais de conhecimento e prática, as organizações podem se tornar mais seguras e confiáveis.

Com base nas observações feitas durante o treinamento presencial percebe-se que como trabalho futuro a ferramenta deve ser mais dinâmica, podendo dar escolha para quem estiver utilizando-a para refazer o nível mesmo já tendo atingido a nota mínima para mudar de nível, com isso a notas e o aprendizado pode ser melhorado obtendo-se assim um desempenho ainda melhor da ferramenta.

Os acertos ou erros deveriam ser apresentados para que quem estiver utilizando-a possa ter um *feedback* no exato momento, como foi apresentado no nível 02. Este *feedback* poderia ser melhorado e implantado em todos os níveis da ferramenta. A mesma poderia tratar sobre a questão dos links que os e-mails de *phishing* contêm, explicando melhor e deixando claro que apenas abrindo-o já pode ser um risco.

Por fim, a validação feita neste trabalho poderia ser refeita em outros ambientes para se averiguar se a mesma obtém resultados equivalentes aos

obtidos neste trabalho, o que reforçaria ainda mais a importância da ferramenta criada.

Referências

APWG. **Phishing Activity Trensd Report**: Unifying the Global Response To Cybercrime. Disponível em: <http://docs.apwg.org/reports/apwg_trends_report_q2_2013.pdf>. Acesso em: 20 nov. 2013.

CERT.BR. **Cartilha de Segurança para Internet. Disponível** em: <http://cartilha.cert.br/golpes/>. Acesso em: 19 nov. 2013.

CERT.BR**. Estatísticas dos Incidentes Reportados ao CERT.br.** Disponível em: <http://www.cert.br/stats/incidentes/>. Acesso em: 10 nov. 2013.

E-GOV. Portal de e-governo, **inclusão digital e sociedade do conhecimento**. Disponível em: <http://www.egov.ufsc.br/portal/conteudo/scam-phishing-e-pharming-fraudes-praticadas-no-ambiente-internet-banking-e-sua-recepção-no->. Acesso em: 09 nov. 2013.

FBI. **Spear Phishing. Disponível** em: <http://www.fbi.gov/news/stories/2009/april/spearphishing_040109>. Acesso em: 21 nov. 2013.

Irani, Danesh,Webb, Steve, Giffin, Jonathon, & Pu, Calton. 2008. **Evolutionary Study of Phishing Security.**

LIMESURVEY.ORG. Official **LimeSurvey partners for professional solutions.** Disponível em: <www.limesurvey.com>. Acesso em: 13 nov. 2013.

LAB, Kaspersky. KASPERSKY INTERNET SECURITY 2014. Disponível em: <http://brazil.kaspersky.com/sobre-a-kaspersky/centro-de-imprensa/comunicados-de-imprensa/ataques-de-phishing-duplicam-no-último->. Acesso em: 16 nov. 2013.

KIRDA, Engin; KRUEGEL, Christopher**. Protecting Users Against Phishing Attacks** with AntiPhishing. Viena, 2005.

MICROSOFT (Org.). **Central de Proteção e Segurança.** Disponível em: <http://www.microsoft.com/pt-br/security/resources/identitytheft-whatis.aspx>. Acesso em: 19 nov. 2013.

Mayora, O, et al. User Centric Media in the Future Internet : Trends and Challenges, 2008. pg 441–446.

PROCON-SP. **GUIA DO COMERCIO ELETRONICO.** Disponível em: <http://www.procon.sp.gov.br/pdf/acs_guia_comercio_eletronico.pdf>. Acesso em: 20 nov. 2013.

SCIRRA. **Create games. Effortlessly**. Disponível em: <https://www.scirra.com/>. Acesso em: 13 nov. 2013.

WANG, Jingguo et al. Phishing Susceptibility**: An Investigation Into the Processing of a Targeted Spear Phishing Email**. Iee Transactions On Professional Communication, Eua, v. 55, p.345-362, 4 dez. 2012.

YUE, Chuan; WANG, Haining. **Anti-Phishing in Offense and Defense**. Annual Computer Security Applications Conference: The College Of William And Mary, 2008. 10 p.

APÊNDICE A

Este *Storyboard* tem como finalidade apoiar no desenvolvimento conforme já citado acima seguindo o modelo do GIED que é Grupo de Informática Educativa, que foi feito em 2009, descrevendo o conceito de como se criar o mesmo. E com base nesses conceitos descrito pela GIED segue a baixo as imagens contendo o *storyboard* desta ferramenta proposta.

StoryBoard: Ferramenta Anti-Phishing
Disciplina: Trabalho de Conclusão de Curso.
Conteúdo: Controle de tela e conteúdo.

Nº	Descrição
1.0	Tela Inicial ”login”
2.0	Explicando *phishing* e mostrando os níveis que será abordado na ferramenta.
3.0	Tela do nível 1 – Tratando de URLs e detalhes nas páginas. Tendo como sub páginas até a 3.10.
4.0	Tela do nível 2 – Tratando de URLs similares e sub domínios e diretórios. Tendo como sub página a 4.1.
5.0	Tela do nível 3 - Tratando de questões de e-mails maliciosos. Tendo como sub páginas até a 5.7.
6.0	Tela Final para à avaliação da Ferramenta

StoryBoard: Ferramenta Anti-Phishing
Disciplina: Trabalho de Conclusão de Curso.
Controle de tela e conteúdo. 1.0

Animação	Figuras	Fala dos personagens	Personagens	Cenários
Não houve animação.	Não teve figura pois o cenário já era necessário.	Aqui o jogador terá que digitar seu e-mail e clicar em "Iniciar". Texto contido: Está é uma ferramenta de treinamento para combater a questão de fraudes pela internet, principalmente o roubo de informações digitais. Digite seu e-mail do @uenp.edu.br abaixo e clique em iniciar para participar do treinamento.	É o próprio cursor do mouse e interage com a ferramenta por meio do mesmo.	O cenário é uma imagem de fundo personalizado e com relação a ferramenta mas que não influência na leitura de textos.

StoryBoard: Ferramenta Anti-Phishing
Disciplina: Trabalho de Conclusão de Curso.
Controle de tela e conteúdo. 2.0

Animação	Figuras	Fala dos personagens	Personagens	Cenários
Não houve animação.	Não teve figura pois o cenário já era necessário.	Aqui o usuário terá a opção de clicar em "Iniciar" Texto abordado: *Phishing* é nome dado à tecnica para efetuar o roubo de informações como senhas bancárias pn-line, informações de cartão de credito, senhas de e-mails, senhas redes sociais e outras do tipo. Atualmente os meios utiilizados para obter essas informações são páginas falsas, formulários e e-mails, sendo que essas três questões serão apresentadas em cada nível desta ferramenta. Primero nível será tratado a questão de Urls e detalhes das páginas de Internet. Segundo nível será tradado a questão de Urls similares Sub domínios e diretórios. Terceiro nível será tradado a questão dos e-mails.	É o próprio cursor do mouse e interage com a ferramenta por meio do mesmo.	O cenário é uma imagem de fundo personalizado e com relação a ferramenta mas que não influência na leitura de textos. .

StoryBoard: Ferramenta Anti-Phishing
Disciplina: Trabalho de Conclusão de Curso.
Controle de tela e conteúdo. 3.0

Animação	Figuras	Fala dos personagens	Personagens	Cenários
Não houve animação.	Não teve figura pois o cenário já era necessário.	Aqui o usuário terá a opção de clicar em "Continuar" Nivel1. Este Nível abordará questões de URLS e detalhes nas páginas web. Exemplo básico de URL é : www.google.com Dicas para saber se é uma página verdadeira ou não. 1 - Ao analisar a URL que é o endereço virtual de uma página, por exemplo: www.google.com.br, verifique se as imagens na página estão de acordo com ao que você procura. 2 – A URL do banco Sicredi é: www.sicredi.com.br porém uma página falsa da mesma poderia ser www.ssicredi.com.br 3 – verifique se a página como um todo está com todas as imagens carregadas sem falhas.	É o próprio cursor do mouse e interage com a ferramenta por meio do mesmo.	O cenário é uma imagem de fundo personalizado e com relação a ferramenta mas que não influência na leitura de textos.

StoryBoard: Ferramenta Anti-Phishing
Disciplina: Trabalho de Conclusão de Curso.
Controle de tela e conteúdo. 3.1

Animação	Figuras	Fala dos personagens	Personagens	Cenários
Não houve animação.	Não teve figura pois o cenário já era necessário.	4 – Não se impressione com ofertas onde o valor é muito baixo comparado com de vários concorrentes. 5 – Preste atenção em datas que estiverem na imagem, pois a mesma pode ser de doas ou meses anteriores. 6 – Procure pelo site em questão por uma ferramenta de busca (Ex: Google) e confira se a URL e o layout do site é atual ou que contenha poucas diferenças. Com base nessas dicas, defina como Verdadeira s ou falsas as páginas a seguir, e se esquecer de alguma dica, clique em ajuda O usuário terá opção de clicar em "Iniciar"	É o próprio cursor do mouse e interage com a ferramenta por meio do mesmo.	O cenário é uma imagem de fundo personalizado e com relação a ferramenta mas que não influência na leitura de textos.

StoryBoard: Ferramenta Anti-Phishing
Disciplina: Trabalho de Conclusão de Curso.
Controle de tela e conteúdo. 3.2

Animação	Figuras	Fala dos personagens	Personagens	Cenários
Não houve animação.	Não teve figura pois o cenário já era necessário.	Usuário terá opção de clicar em Verdadeiro, Falso ou Ajuda Caso o mesmo clique em ajuda mostrar as mesmas dicas apresentadas antes de iniciar o nível , e disponibilizar a opção de o mesmo fechar a Ajuda e continuar o treinamento. Falhas desta página: Url, imagem de como já estivesse feito o login.	É o próprio cursor do mouse e interage com a ferramenta por meio do mesmo. 	O cenário é uma imagem de fundo personalizado e com relação a ferramenta mas que não influência na leitura de textos.

StoryBoard: Ferramenta Anti-Phishing
Disciplina: Trabalho de Conclusão de Curso.
Controle de tela e conteúdo. 3.2

Explicação	Figuras	Exercícios	Alternativas	Feedback
• Terá que escolher entre verdadeiro e falso	• Não contém pois já está incluído no cenário	• Analisar a página e verificar se a mesma é falsa ou não de acordo com as dicas.	**Respostas corretas** • Clicar em Falso	**Negativo** • No final do nível se a nota mínima não for atingida o mesmo terá que refazer o nível.
			Respostas erradas • Clicar em Verdadeira	**Positivo** • Mensagem de motivação Ler as dicas com mais atenção

StoryBoard: Ferramenta Anti-Phishing
Disciplina: Trabalho de Conclusão de Curso.
Controle de tela e conteúdo. 3.3

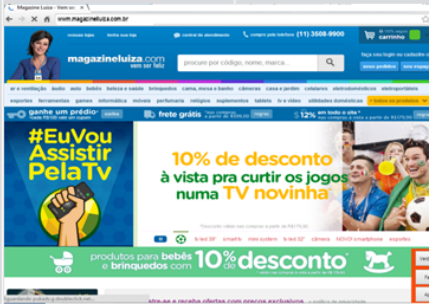
Animação	Figuras	Fala dos personagens	Personagens	Cenários
Não houve animação.	Não teve figura pois o cenário já era necessário.	Usuário terá opção de clicar em Verdadeiro, Falso ou Ajuda Caso o mesmo clique em ajuda mostrar as mesmas dicas apresentadas antes de iniciar o nível , e disponibilizar a opção de o mesmo fechar a Ajuda e continuar o treinamento. Falhas desta página: Url, imagens não carregadas, datas erradas.	É o próprio cursor do mouse e interage com a ferramenta por meio do mesmo.	O cenário é uma imagem de fundo personalizado e com relação a ferramenta mas que não influência na leitura de textos.

StoryBoard: Ferramenta Anti-Phishing
Disciplina: Trabalho de Conclusão de Curso.
Controle de tela e conteúdo. 3.3

Explicação	Figuras	Exercícios	Alternativas	Feedback
• Terá que escolher entre verdadeiro e falso.	• Não contém pois já está incluído no cenário	• Analisar a página e verificar se a mesma é falsa ou não de acordo com as dicas.	**Respostas corretas** • Clicar em Falso	**Negativo** • No final do nível se a nota mínima não for atingida o mesmo terá que refazer o nível.
			Respostas erradas • Clicar em Verdadeira	**Positivo** • Mensagem de motivação Ler as dicas com mais atenção

StoryBoard: Ferramenta Anti-Phishing
Disciplina: Trabalho de Conclusão de Curso.
Controle de tela e conteúdo. 3.4

Animação	Figuras	Fala dos personagens	Personagens	Cenários
Não houve animação.	Não teve figura pois o cenário já era necessário.	Usuário terá opção de clicar em Verdadeiro, Falso ou Ajuda Caso o mesmo clique em ajuda mostrar as mesmas dicas apresentadas antes de iniciar o nível , e disponibilizar a opção de o mesmo fechar a Ajuda e continuar o treinamento. Falhas desta página: Url.	É o próprio cursor do mouse e interage com a ferramenta por meio do mesmo.	O cenário é uma imagem de fundo personalizado e com relação a ferramenta mas que não influência na leitura de textos.

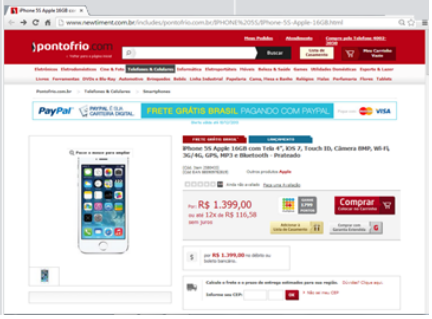


StoryBoard: Ferramenta Anti-Phishing
Disciplina: Trabalho de Conclusão de Curso.
Controle de tela e conteúdo. 3.4

Explicação	Figuras	Exercícios	Alternativas	Feedback
• Terá que escolher entre verdadeiro e falso	• Não contém pois já está incluído no cenário	• Analisar a página e verificar se a mesma é falsa ou não de acordo com as dicas.	**Respostas corretas**	**Negativo**
			• Clicar em Falso	• No final do nível se a nota mínima não for atingida o mesmo terá que refazer o nível.
			Respostas erradas	**Positivo**
			• Clicar em Verdadeira	• Mensagem de motivação Ler as dicas com mais atenção

StoryBoard: Ferramenta Anti-Phishing
Disciplina: Trabalho de Conclusão de Curso.
Controle de tela e conteúdo. 3.5

Animação	Figuras	Fala dos personagens	Personagens	Cenários
Não houve animação.	Não teve figura pois o cenário já era necessário.	Usuário terá opção de clicar em Verdadeiro, Falso ou Ajuda Caso o mesmo clique em ajuda mostrar as mesmas dicas apresentadas antes de iniciar o nível , e disponibilizar a opção de o mesmo fechar a Ajuda e continuar o treinamento. Falhas desta página: Url, preço muito baixo, layout por inteiro.	É o próprio cursor do mouse e interage com a ferramenta por meio do mesmo.	O cenário é uma imagem de fundo personalizado e com relação a ferramenta mas que não influência na leitura de textos.

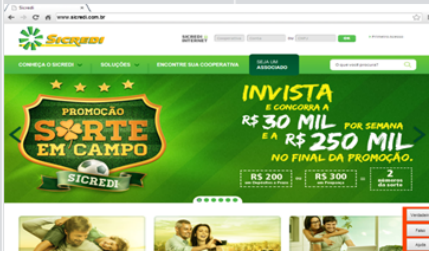


StoryBoard: Ferramenta Anti-Phishing
Disciplina: Trabalho de Conclusão de Curso.
Controle de tela e conteúdo. 3.5

Explicação	Figuras	Exercícios	Alternativas	Feedback
• Terá que escolher entre verdadeiro e falso	• Não contém pois já está incluído no cenário	• Analisar a página e verificar se a mesma é falsa ou não de acordo com as dicas.	**Respostas corretas** • Clicar em Falso	**Negativo** • No final do nível se a nota mínima não for atingida o mesmo terá que refazer o nível.
			Respostas erradas • Clicar em Verdadeira	**Positivo** • Mensagem de motivação Ler as dicas com mais atenção

StoryBoard: Ferramenta Anti-Phishing
Disciplina: Trabalho de Conclusão de Curso.
Controle de tela e conteúdo. 3.6

Animação	Figuras	Fala dos personagens	Personagens	Cenários
Não houve animação.	Não teve figura pois o cenário já era necessário.	Usuário terá opção de clicar em Verdadeiro, Falso ou Ajuda Caso o mesmo clique em ajuda mostrar as mesmas dicas apresentadas antes de iniciar o nível , e disponibilizar a opção de o mesmo fechar a Ajuda e continuar o treinamento. Falhas desta página: Não contem falhas, esta é verdadeira.	É o próprio cursor do mouse e interage com a ferramenta por meio do mesmo.	O cenário é uma imagem de fundo personalizado e com relação a ferramenta mas que não influência na leitura de textos.

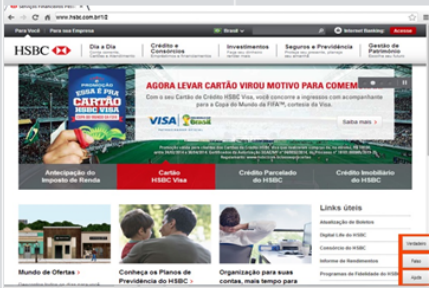


StoryBoard: Ferramenta Anti-Phishing
Disciplina: Trabalho de Conclusão de Curso.
Controle de tela e conteúdo. 3.6

Explicação	Figuras	Exercícios	Alternativas	Feedback
• Terá que escolher entre verdadeiro e falso	• Não contém pois já está incluído no cenário	• Analisar a página e verificar se a mesma é falsa ou não de acordo com as dicas.	**Respostas corretas**	**Negativo**
			• Clicar em Verdadeira	• No final do nível se a nota mínima não for atingida o mesmo terá que refazer o nível.
			Respostas erradas	**Positivo**
			• Clicar em Falso	• Mensagem de motivação Ler as dicas com mais atenção

StoryBoard: Ferramenta Anti-Phishing
Disciplina: Trabalho de Conclusão de Curso.
Controle de tela e conteúdo. 3.7

Animação	Figuras	Fala dos personagens	Personagens	Cenários
Não houve animação.	Não teve figura pois o cenário já era necessário.	Usuário terá opção de clicar em Verdadeiro, Falso ou Ajuda Caso o mesmo clique em ajuda mostrar as mesmas dicas apresentadas antes de iniciar o nível , e disponibilizar a opção de o mesmo fechar a Ajuda e continuar o treinamento. Falhas desta página: Não contem falhas, esta é verdadeira.	É o próprio cursor do mouse e interage com a ferramenta por meio do mesmo.	O cenário é uma imagem de fundo personalizado e com relação a ferramenta mas que não influência na leitura de textos.

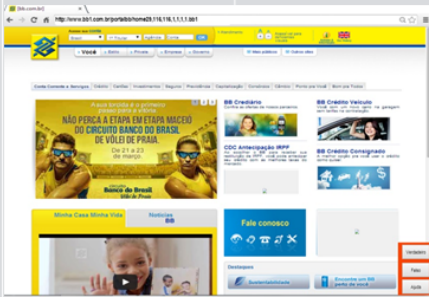


StoryBoard: Ferramenta Anti-Phishing
Disciplina: Trabalho de Conclusão de Curso.
Controle de tela e conteúdo. 3.7

Explicação	Figuras	Exercícios	Alternativas	Feedback
• Terá que escolher entre verdadeiro e falso	• Não contém pois já está incluído no cenário	• Analisar a página e verificar se a mesma é falsa ou não de acordo com as dicas.	**Respostas corretas** • Clicar em Verdadeira	**Negativo** • No final do nível se a nota mínima não for atingida o mesmo terá que refazer o nível.
			Respostas erradas • Clicar em Falso	**Positivo** • Mensagem de motivação Ler as dicas com mais atenção

StoryBoard: Ferramenta Anti-Phishing
Disciplina: Trabalho de Conclusão de Curso.
Controle de tela e conteúdo. 3.8

Animação	Figuras	Fala dos personagens	Personagens	Cenários
Não houve animação.	Não teve figura pois o cenário já era necessário.	Usuário terá opção de clicar em Verdadeiro, Falso ou Ajuda Caso o mesmo clique em ajuda mostrar as mesmas dicas apresentadas antes de iniciar o nível , e disponibilizar a opção de o mesmo fechar a Ajuda e continuar o treinamento. Falhas desta página: Url, imagens sem carregar, datas	É o próprio cursor do mouse e interage com a ferramenta por meio do mesmo.	O cenário é uma imagem de fundo personalizado e com relação a ferramenta mas que não influência na leitura de textos.



StoryBoard: Ferramenta Anti-Phishing
Disciplina: Trabalho de Conclusão de Curso.
Controle de tela e conteúdo. 3.8

Explicação	Figuras	Exercícios	Alternativas	Feedback
• Terá que escolher entre verdadeiro e falso	• Não contém pois já está incluído no cenário	• Analisar a página e verificar se a mesma é falsa ou não de acordo com as dicas.	**Respostas corretas** • Clicar em Falso	**Negativo** • No final do nível se a nota mínima não for atingida o mesmo terá que refazer o nível.
			Respostas erradas • Clicar em Verdadeira	**Positivo** • Mensagem de motivação Ler as dicas com mais atenção

StoryBoard: Ferramenta Anti-Phishing
Disciplina: Trabalho de Conclusão de Curso.
Controle de tela e conteúdo. 3.9

Animação	Figuras	Fala dos personagens	Personagens	Cenários
Não houve animação.	Não teve figura pois o cenário já era necessário.	Usuário terá opção de clicar em Verdadeiro, Falso ou Ajuda Caso o mesmo clique em ajuda mostrar as mesmas dicas apresentadas antes de iniciar o nível , e disponibilizar a opção de o mesmo fechar a Ajuda e continuar o treinamento. Falhas desta página: Url.	É o próprio cursor do mouse e interage com a ferramenta por meio do mesmo.	O cenário é uma imagem de fundo personalizado e com relação a ferramenta mas que não influência na leitura de textos.

StoryBoard: Ferramenta Anti-Phishing
Disciplina: Trabalho de Conclusão de Curso.
Controle de tela e conteúdo. 3.9

Explicação	Figuras	Exercícios	Alternativas	Feedback
• Terá que escolher entre verdadeiro e falso	• Não contém pois já está incluído no cenário	• Analisar a página e verificar se a mesma é falsa ou não de acordo com as dicas.	**Respostas corretas**	**Negativo**
			• Clicar em Falso	• No final do nível se a nota mínima não for atingida o mesmo terá que refazer o nível.
			Respostas erradas	**Positivo**
			• Clicar em Verdadeira	• Mensagem de motivação Ler as dicas com mais atenção

StoryBoard: Ferramenta Anti-Phishing
Disciplina: Trabalho de Conclusão de Curso.
Controle de tela e conteúdo. 3.10

Animação	Figuras	Fala dos personagens	Personagens	Cenários
Não houve animação.	Não teve figura pois o cenário já era necessário.	Usuário terá opção de clicar em Verdadeiro, Falso ou Ajuda Caso o mesmo clique em ajuda mostrar as mesmas dicas apresentadas antes de iniciar o nível , e disponibilizar a opção de o mesmo fechar a Ajuda e continuar o treinamento. Falhas desta página: Não contem falhas, esta é verdadeira.	É o próprio cursor do mouse e interage com a ferramenta por meio do mesmo.	O cenário é uma imagem de fundo personalizado e com relação a ferramenta mas que não influência na leitura de textos.

StoryBoard: Ferramenta Anti-Phishing
Disciplina: Trabalho de Conclusão de Curso.
Controle de tela e conteúdo. 3.10

Explicação	Figuras	Exercícios	Alternativas	Feedback
• Terá que escolher entre verdadeiro e falso	• Não contém pois já está incluído no cenário	• Analisar a página e verificar se a mesma é falsa ou não de acordo com as dicas.	**Respostas corretas**	**Negativo**
			• Clicar em Verdadeira	• No final do nível se a nota mínima não for atingida o mesmo terá que refazer o nível.
			Respostas erradas	**Positivo**
			• Clicar em Falso	• Mensagem de motivação Ler as dicas com mais atenção

StoryBoard: Ferramenta Anti-Phishing
Disciplina: Trabalho de Conclusão de Curso.
Controle de tela e conteúdo. 4.0

Animação	Figuras	Fala dos personagens	Personagens	Cenários
Não houve animação.	Não teve figura pois o cenário já era necessário.	Aqui o usuário terá a opção de clicar em "Iniciar" Nível 2. Este Nível abordará questões de URLS similares e sub domínios e diretórios. Dicas para saber se é uma URL verdadeira ou não: 1 – Subdomínios são ramificação de um domínio, como por exemplo www.seublogspo.com.br, porém, podem existir página por exemplo www.sicredi.algumacoisa.com.br 2 – Evite acessar URLs atráves de propagandas na Internet e pesquise pelo site em questão em uma ferramenta de busca(ex: Google) e confira se a URL e o domínio são os mesmos. 3 – E não estranhe se tiver domínios como por exemplo www.alguma .eco ou com finais do tipo: emp.br; net.br; blog.br e vários outros que estão disponíveis em http://registro.br/dominios /categoria.html que é o órgão responsável sobre essas questões. Com base nessas dicas, defina como VERDADEIRAS ou FALSAS as páginas a seguir, e se esquecer de alguma dica	É o próprio cursor do mouse e interage com a ferramenta por meio do mesmo.	O cenário é uma imagem de fundo personalizado e com relação a ferramenta mas que não influência na leitura de textos.

StoryBoard: Ferramenta Anti-Phishing
Disciplina: Trabalho de Conclusão de Curso.
Controle de tela e conteúdo. 4.1

Animação	Figuras	Fala dos personagens	Personagens	Cenários
Não houve animação.	Foram utilizadas para um feedback apresentado ao usuário.  	Aqui o usuário terá a opção de clicar em Verdadeiro, Falso ou ajuda. Para cada URL abaixo. • https://carrinho.pontofrio.com.br • http://www.terra.com.br/portal/ • http://www.amazon.anazoon.com.br/ • https://carrinho.extra.com.br/Checkout#login • http://hotmaill.net.br • http://www.newtiment.com.br/includes/pontofrio.com.br • http://idnorp.net.br • https://pt-br.facebook.com • http://bomnegocio.vendass.com • https://www.google.com.br • http://fcc.org.br/institucional/ • http://www.educacao.pr.gov.br/ • http://globotv.globo.com • http://www.faceboook.com.br	É o próprio cursor do mouse e interage com a ferramenta por meio do mesmo.	O cenário é uma imagem de fundo personalizado e com relação a ferramenta mas que não influência na leitura de textos.

StoryBoard: Ferramenta Anti-Phishing
Disciplina: Trabalho de Conclusão de Curso.
Controle de tela e conteúdo. 4.1

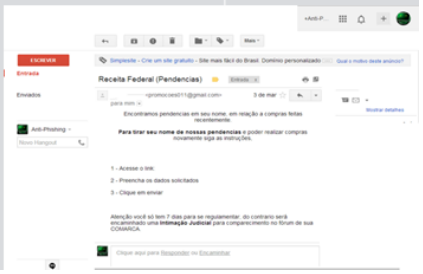
Explicação	Figuras	Exercícios	Alternativas	Feedback
• Terá que escolher entre verdadeiro e falso	 	• Analisar a página e verificar se a mesma é falsa ou não de acordo com as dicas.	**Respostas corretas** • Clicar em Verdadeira • Clicar em Falso Analisar de acordo com as dicas e conteúdo anterior.	**Negativo** • Frase de motivação para prestar mais atenção nas dicas.
			Respostas erradas • Clicar em Verdadeira • Clicar em Falso Analisar de acordo com as dicas e conteúdo anterior.	**Positivo** • Conforme faz a escolha mostra se acertou ou errou.

StoryBoard: Ferramenta Anti-Phishing
Disciplina: Trabalho de Conclusão de Curso.
Controle de tela e conteúdo. 5.0

Animação	Figuras	Fala dos personagens	Personagens	Cenários
Não houve animação.	Não teve figura pois o cenário já era necessário.	Aqui o usuário terá a opção de clicar em "Iniciar" Nivel3. Este Nível abordará questões de e-mails maliciosos.. Dicas para saber se é e-mail verdadeiro ou não: 1 – Verifique se quem está enviando o e-mail é mesmo a empresa onde tralha ou onde efetue compras. 2 – Fique atento se ao se cadastrar em sites e se foi permitido o envio de e-mails. 3 – cuidado com URL que contém nos e-mails pois elas podem ser falsas conforme já discutido nos níveis anteriores. 4 – Bancos e lojas online jamais mandarão contas ou boletos para pagar a não ser que tenha permitido. 5 – Geralmente e-mails contém textos estranhos pedindo para clicar em URLs, verifique se esta URL não termina com .exe; .pif; .bat; pois estas extensões são executáveis e podem fazer um download automático de algum vírus ou programa que não se faz necessário em seu computador pessoal.	É o próprio cursor do mouse e interage com a ferramenta por meio do mesmo.	O cenário é uma imagem de fundo personalizado e com relação a ferramenta mas que não influência na leitura de textos.

StoryBoard: Ferramenta Anti-Phishing
Disciplina: Trabalho de Conclusão de Curso.
Controle de tela e conteúdo. 5.1

Animação	Figuras	Fala dos personagens	Personagens	Cenários
Não houve animação.	Não teve figura pois o cenário já era necessário.	Usuário terá opção de clicar em Verdadeiro, Falso ou Ajuda Caso o mesmo clique em ajuda mostrar as mesmas dicas apresentadas antes de iniciar o nível , e disponibilizar a opção de o mesmo fechar a Ajuda e continuar o treinamento. Falhas deste e-mail: Quem enviou é um e-mail estranho, Pedindo pra acessar um link falso e erros de português.	É o próprio cursor do mouse e interage com a ferramenta por meio do mesmo.	O cenário é uma imagem de fundo personalizado e com relação a ferramenta mas que não influência na leitura de textos.



StoryBoard: Ferramenta Anti-Phishing
Disciplina: Trabalho de Conclusão de Curso.
Controle de tela e conteúdo. 5.1

Explicação	Figuras	Exercícios	Alternativas	Feedback
• Terá que escolher entre verdadeiro e falso	Não contém pois já está incluído no cenário	• Analisar a página e verificar se a mesma é falsa ou não de acordo com as dicas.	**Respostas corretas**	**Negativo**
			• Definir o e-mail como falso.	
			Respostas erradas	**Positivo**
			• Definir o e-mail como verdadeiro	

StoryBoard: Ferramenta Anti-Phishing
Disciplina: Trabalho de Conclusão de Curso.
Controle de tela e conteúdo. 5.2

Animação	Figuras	Fala dos personagens	Personagens	Cenários
Não houve animação.		Usuário terá opção de clicar em Verdadeiro, Falso ou Ajuda Caso o mesmo clique em ajuda mostrar as mesmas dicas apresentadas antes de iniciar o nível , e disponibilizar a opção de o mesmo fechar a Ajuda e continuar o treinamento. Falhas deste e-mail: Quem enviou é um e-mail estranho, Pedindo pra acessar um link falso e erros de português.	É o próprio cursor do mouse e interage com a ferramenta por meio do mesmo.	O cenário é uma imagem de fundo personalizado e com relação a ferramenta mas que não influência na leitura de textos.

StoryBoard: Ferramenta Anti-Phishing
Disciplina: Trabalho de Conclusão de Curso.
Controle de tela e conteúdo. 5.2

Explicação	Figuras	Exercícios	Alternativas	Feedback
• Terá que escolher entre verdadeiro e falso	Não contém pois já está incluído no cenário	• Analisar a página e verificar se a mesma é falsa ou não de acordo com as dicas.	**Respostas corretas**	**Negativo**
			• Definir o e-mail como falso.	
			Respostas erradas	**Positivo**
			• Definir o e-mail como verdadeiro	

StoryBoard: Ferramenta Anti-Phishing
Disciplina: Trabalho de Conclusão de Curso.
Controle de tela e conteúdo. 5.3

Animação	Figuras	Fala dos personagens	Personagens	Cenários
Não houve animação.	Não teve figura pois o cenário já era necessário.	Usuário terá opção de clicar em Verdadeiro, Falso ou Ajuda Caso o mesmo clique em ajuda mostrar as mesmas dicas apresentadas antes de iniciar o nível , e disponibilizar a opção de o mesmo fechar a Ajuda e continuar o treinamento. Falhas deste e-mail: Quem enviou o e-mail esta com endereço em branco estranho, Pedindo pra acessar um link falso e erros de português.	É o próprio cursor do mouse e interage com a ferramenta por meio do mesmo.	O cenário é uma imagem de fundo personalizado e com relação a ferramenta mas que não influência na leitura de textos.

StoryBoard: Ferramenta Anti-Phishing
Disciplina: Trabalho de Conclusão de Curso.
Controle de tela e conteúdo. 5.3

Explicação	Figuras	Exercícios	Alternativas	Feedback
• Terá que escolher entre verdadeiro e falso	Não contém pois já está incluído no cenário	• Analisar a página e verificar se a mesma é falsa ou não de acordo com as dicas.	**Respostas corretas** • Definir o e-mail como falso.	**Negativo**
			Respostas erradas • Definir o e-mail como verdadeiro	**Positivo**

StoryBoard: Ferramenta Anti-Phishing
Disciplina: Trabalho de Conclusão de Curso.
Controle de tela e conteúdo. 5.4

Animação	Figuras	Fala dos personagens	Personagens	Cenários
Não houve animação.	Não teve figura pois o cenário já era necessário.	Usuário terá opção de clicar em Verdadeiro, Falso ou Ajuda Caso o mesmo clique em ajuda mostrar as mesmas dicas apresentadas antes de iniciar o nível , e disponibilizar a opção de o mesmo fechar a Ajuda e continuar o treinamento. Falhas deste e-mail: Quem enviou é um e-mail estranho, Pede pra fazer um download de um arquivo.	É o próprio cursor do mouse e interage com a ferramenta por meio do mesmo. 	O cenário é uma imagem de fundo personalizado e com relação a ferramenta mas que não influência na leitura de textos.

StoryBoard: Ferramenta Anti-Phishing
Disciplina: Trabalho de Conclusão de Curso.
Controle de tela e conteúdo. 5.4

Explicação	Figuras	Exercícios	Alternativas	Feedback
• Terá que escolher entre verdadeiro e falso	Não contém pois já está incluído no cenário	• Analisar a página e verificar se a mesma é falsa ou não de acordo com as dicas.	**Respostas corretas** • Definir o e-mail como falso. **Respostas erradas** • Definir o e-mail como verdadeiro	**Negativo** **Positivo**

StoryBoard: Ferramenta Anti-Phishing
Disciplina: Trabalho de Conclusão de Curso.
Controle de tela e conteúdo. 5.5

Animação	Figuras	Fala dos personagens	Personagens	Cenários
Não houve animação.	Não teve figura pois o cenário já era necessário.	Usuário terá opção de clicar em Verdadeiro, Falso ou Ajuda Caso o mesmo clique em ajuda mostrar as mesmas dicas apresentadas antes de iniciar o nível , e disponibilizar a opção de o mesmo fechar a Ajuda e continuar o treinamento. Falhas deste e-mail: Quem enviou é um e-mail estranho, link falso contendo na imagem.	É o próprio cursor do mouse e interage com a ferramenta por meio do mesmo.	O cenário é uma imagem de fundo personalizado e com relação a ferramenta mas que não influência na leitura de textos.

StoryBoard: Ferramenta Anti-Phishing
Disciplina: Trabalho de Conclusão de Curso.
Controle de tela e conteúdo. 5.5

Explicação	Figuras	Exercícios	Alternativas	Feedback
• Terá que escolher entre verdadeiro e falso	Não contém pois já está incluído no cenário	• Analisar a página e verificar se a mesma é falsa ou não de acordo com as dicas.	**Respostas corretas** • Definir o e-mail como falso. **Respostas erradas** • Definir o e-mail como verdadeiro	**Negativo** **Positivo**

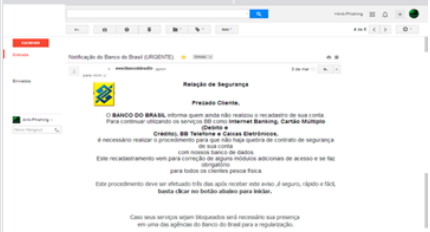
StoryBoard: Ferramenta Anti-Phishing
Disciplina: Trabalho de Conclusão de Curso.
Controle de tela e conteúdo. 5.6

Animação	Figuras	Fala dos personagens	Personagens	Cenários
Não houve animação.	Não teve figura pois o cenário já era necessário.	Usuário terá opção de clicar em Verdadeiro, Falso ou Ajuda Caso o mesmo clique em ajuda mostrar as mesmas dicas apresentadas antes de iniciar o nível , e disponibilizar a opção de o mesmo fechar a Ajuda e continuar o treinamento. Falhas deste e-mail: Este e-mail não contém falha.	É o próprio cursor do mouse e interage com a ferramenta por meio do mesmo.	O cenário é uma imagem de fundo personalizado e com relação a ferramenta mas que não influência na leitura de textos.

StoryBoard: Ferramenta Anti-Phishing
Disciplina: Trabalho de Conclusão de Curso.
Controle de tela e conteúdo. 5.6

Explicação	Figuras	Exercícios	Alternativas	Feedback
• Terá que escolher entre verdadeiro e falso	Não contém pois já está incluído no cenário	• Analisar a página e verificar se a mesma é falsa ou não de acordo com as dicas.	**Respostas corretas** • Definir o e-mail como falso.	**Negativo**
			Respostas erradas • Definir o e-mail como verdadeiro	**Positivo**

StoryBoard: Ferramenta Anti-Phishing
Disciplina: Trabalho de Conclusão de Curso.
Controle de tela e conteúdo. 5.7

Animação	Figuras	Fala dos personagens	Personagens	Cenários
Não houve animação.	Não teve figura pois o cenário já era necessário.	Usuário terá opção de clicar em Verdadeiro, Falso ou Ajuda Caso o mesmo clique em ajuda mostrar as mesmas dicas apresentadas antes de iniciar o nível , e disponibilizar a opção de o mesmo fechar a Ajuda e continuar o treinamento. Falhas deste e-mail: quem enviou o e-mail não é o banco, pedindo pra clicar num botão que levará a um link falso.	É o próprio cursor do mouse e interage com a ferramenta por meio do mesmo. 	O cenário é uma imagem de fundo personalizado e com relação a ferramenta mas que não influência na leitura de textos.

StoryBoard: Ferramenta Anti-Phishing
Disciplina: Trabalho de Conclusão de Curso.
Controle de tela e conteúdo. 5.7

Explicação	Figuras	Exercícios	Alternativas	Feedback
• Terá que escolher entre verdadeiro e falso	Não contém pois já está incluído no cenário	• Analisar a página e verificar se a mesma é falsa ou não de acordo com as dicas.	**Respostas corretas** • Definir o e-mail como falso.	**Negativo**
			Respostas erradas • Definir o e-mail como verdadeiro	**Positivo**

StoryBoard: Ferramenta Anti-Phishing
Disciplina: Trabalho de Conclusão de Curso.
Controle de tela e conteúdo. 6.0

Animação	Figuras	Fala dos personagens	Personagens	Cenários
Não houve animação.	Não teve figura pois o cenário já era necessário.	Usuário terá opção de selecionar a nota de avaliação e clicar em Enviar. Pro favor avalie esta ferramenta escolhendo de 0 a 5, onde zero é ruim e cinco é bom. Após a escolha clique em enviar. Obrigado por participar! Caso deseje refazer o treinamento clique em "Refazer".	É o próprio cursor do mouse e interage com a ferramenta por meio do mesmo.	O cenário é uma imagem de fundo personalizado e com relação a ferramenta mas que não influência na leitura de textos.