INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO RIO GRANDE DO NORTE
CAMPUS NATAL – ZONA NORTE
CURSO TÉCNICO INTEGRADO EM INFORMÁTICA

PEDRO VICTOR DA COSTA FREIRE
VIVIAN GABRIELLA BARROSO DA SILVA

DESENVOLVIMENTO DE MATERIAL DIDÁTICO E CAPACITAÇÃO EM SEGURANÇA DA INFORMAÇÃO, VOLTADOS PARA COMUNIDADE NO ENTORNO DO IFRN CAMPUS NATAL – ZONA NORTE

NATAL/RN
2016

PEDRO VICTOR DA COSTA FREIRE
VIVIAN GABRIELLA BARROSO DA SILVA

DESENVOLVIMENTO DE MATERIAL DIDÁTICO E CAPACITAÇÃO EM SEGURANÇA DA INFORMAÇÃO, VOLTADOS PARA COMUNIDADE NO ENTORNO DO IFRN CAMPUS NATAL – ZONA NORTE

Trabalho de Conclusão de Curso apresentado ao Curso Técnico em Informática do Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte, em cumprimento às exigências legais como requisito parcial à obtenção do título de Técnico em Informática.

NATAL/RN
2016

PEDRO VICTOR DA COSTA FREIRE
VIVIAN GABRIELLA BARROSO DA SILVA

DESENVOLVIMENTO DE MATERIAL DIDÁTICO E CAPACITAÇÃO EM SEGURANÇA DA INFORMAÇÃO, VOLTADOS PARA COMUNIDADE NO ENTORNO DO IFRN CAMPUS NATAL – ZONA NORTE

Trabalho de Conclusão de Curso apresentado ao Curso Técnico em Informática do Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte, em cumprimento às exigências legais como requisito parcial à obtenção do título de Técnico em Informática.

Aprovado em: ___/___/___

COMISSÃO EXAMINADORA

_____

Prof. Cesimar Xavier de Souza Dias – Avaliador
Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte

_____

Prof. Edmilson Barbalho Campos Neto – Coordenador do Curso de Informática
Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte

_____

Prof. Rodolfo da Silva Costa – Orientador
Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte

NATAL/RN
2016

AGRADECIMENTOS

Neste percurso acadêmico de 4 anos que está se encerrando gostaríamos de agradecer as pessoas que fizeram parte direta ou indiretamente dessa longa jornada cheia de obstáculos como alunos do curso Técnico Integrado em Informática. Primeiramente ao Instituto Federal de Educação de Ciência e Tecnologia do Rio Grande do Norte, em seu campi localizado na Zona Norte, que nos proporcionou toda a infraestrutura, apoio e por confiar em projetos e pesquisas dos alunos como principal prioridade na atual gestão, além dos mestres e doutores altamente qualificados que nos deu toda a base nesse período. Em seguida agradecemos ao nosso orientador, Professor Rodolfo Costa, pela orientação, comprometimento e paciência dedicada a esse projeto no ano letivo de 2015, contribuindo para nossa formação acadêmica e pessoal. Por fim agradecemos a todos os nossos amigos e familiares que nos apoiaram de forma considerável nessa longa jornada acadêmica, tanto de forma emocional quanto moral. Igualmente, somos gratos por todos os professores que passaram neste preâmbulo, pois todos contribuíram de forma singular na nossa formação básica e técnica.

RESUMO

Os computadores e a internet estão cada vez mais presentes em nossa vida, além de nos auxiliarem nas tarefas cotidianas eles estão cada vez mais ligados ao nosso entretenimento e no nosso meio de comunicação. O que esquecemos, ou desconhecemos, é o universo de riscos e ameaças que estamos sujeitos ao fazer uso dessa enorme rede chamada internet. Além disso surgem as redes sociais, plataformas de interação em que são partilhadas inúmeras informações entre seus usuários, os quais disponibilizam seus dados, alguns deles sensíveis, e estes ficam à disposição de outros membros da rede

Com isso da mesma maneira que existe a necessidade de segurança e privacidade no mundo real, no mundo virtual não é diferente. O que precisamos compreender ao lidar com esse mundo é que nenhuma informação pode ser considerada completamente segura. Este trabalho objetiva à tentativa de investigar, explicar, questionar e esclarecer as formas de utilização dos usuários dessa grande rede mundial de computadores, seja nas redes sociais ou em dispositivos computacionais e móveis, procurando esclarecer os tipos de ameaças e, através de métodos práticos de segurança da informação, estas sejam evitadas.

Palavras-chave: Segurança da Informação. Internet. Redes Sociais. Ameaças;

ABSTRACT

Computers and the internet are increasingly present in our lives, and we assist in daily tasks they are increasingly connected to our entertainment and our means of communication. What we forget, or do not know, is the universe of risks and threats that are subject to make use of this huge network called the Internet. Also arise sociais networks, interaction platforms that are shared lots of information between its members, which provide their data, some of them sensitive, and these are made available to other network members

With it the same way that there is a need for security and privacy in the real world, the virtual world is no different. What we need to understand when dealing with this world is that no information can be considered completely secure. This work aims to attempt to investigate, explain, question and clarify the forms of use that users of large global computer network, or in social networks or computing devices and mobile, seeking to clarify the types of threats and, through practical methods information security, these are avoided.

Keywords: Information Security. Internet. Sociais networks. threats;

SUMÁRIO

1. INTRODUÇÃO

No dia 2 de julho de 2015 foram iniciadas as atividades referentes ao projeto de extensão sobre voltados para comunidade no entorno do IFRN campus Natal- Zona Norte. O projeto foi desenvolvido para que a comunidade interna e externa do campus tivesse acesso ao conhecimento mínimo necessário de como se prevenir de diversas ameaças do mundo cibernético

Nos últimos anos os dispositivos computacionais, em especial os smartphones, em conjunto com a rede mundial de computadores, a Internet passaram por um processo de grande popularização, fazendo com que o homem ficasse dependente dessas ferramentas. Muitas de nossas informações estão em smartphones, computadores e alguns dizem que toda nossa vida está depositada em pequenos e portáteis dispositivos.

O avanço da tecnologia, a popularização da internet na década de 90 e a Web idealizada por Tim Berners-Lee (criador da WWW - World Wide Web), proporcionou à sociedade atual a oportunidade de comunicar-se e obter informações com maior agilidade e eficiência. Nesse mundo virtual destacam-se as redes sociais – ferramentas utilizadas, principalmente pelos jovens, para esses e outros inúmeros fins quando conectados à rede

Ocorre que com a facilidade de acesso à rede, adicionada à mobilidade da Internet cada vez mais independente de aparelhos enormes e fixos, a informação está sendo disseminada a todo momento, de praticamente qualquer lugar pelos usuários, seja através do compartilhamento de informações e entretenimento ou da difusão de conhecimento representando o principal meio de expressão da nossa era. Isso vem gerando um volume imenso de compartilhamento de informações através da Internet, podendo causar diversos problemas relacionados à segurança da informação, esta que segue a 4 princípios segundo o comitê gestor de Internet no Brasil: integridade, disponibilidade, privacidade e confidencialidade , que precisam ser preservados, a fim de que sejam evitados fraudes, violações, acessos, uso e divulgação indevida.

Em contrapartida quanto mais a tecnologia e os dispositivos de segurança evoluem dificultando assim a exploração de vulnerabilidades, mais os invasores explorarão o fator humano, pois de acordo com Kevin Mitnick, o ser humano é o elo mais fraco da segurança, visto que é muito mais fácil conseguir informações explorando o homem, do que por falhas no sistema. Com isso precisa-se que os usuários sejam treinados e conscientizados dos perigos que a internet

e a grande exposição de informações podem trazer, sabendo assim como a informação precisa ser protegida e como protegê-la. [MITNICK, 2002]

Diante de todos esses fatores citados houve a necessidade de estudar e questionar as formas de utilização dos dispositivos computacionais por parte dos usuários, através de apostilas e minicursos desenvolvidos dentro do IFRN campus Zona Norte.

2. METODOLOGIA DO PROJETO

O projeto é composto em três etapas: Pesquisa do conteúdo, desenvolvimento do material didático (apostila e slides) e a posterior aplicação do minicurso com os assuntos abordados no mesmo. A primeira etapa foi feita através de pesquisas de livros (levantamento bibliográfico) e fichamento de fontes diretas de autores que tenham obras acerca da temática abordada, matérias de sites, blogs, como também uma discussão periódica com o orientador do projeto a fim de esclarecer alguns temas que seriam abordados na apostila; A segunda etapa foi o desenvolvimento da apostila e dos slides para o minicurso. Por conseguinte, foi aplicado o minicurso em forma de apresentação de slides, esse que foi correlacionado com o material desenvolvido e algumas práticas para que as pessoas que estejam interessadas possam aplicar os conhecimentos adquiridos durante o minicurso.

2.1 MÓDULO I: Introdução às práticas de Segurança da Informação

O primeiro módulo que iniciou o projeto consiste em esclarecer de forma introdutória a segurança da informação, desde seus princípios básicos até a identificação e remoção de malwares. Na apostila, vários assuntos foram abordados, mas em nenhum deles foi necessário conhecimento técnico aprofundado de TI por parte dos leitores. Associada a esta houve o minicurso em que algumas práticas foram desenvolvidas para complementar a teoria vista na apostila e sala de aula.

Alguns conceitos básicos relacionados à Segurança da Informação são de extrema importância e foram esclarecidos neste módulo. Grandes partes dos incidentes de segurança ocorrem por puro desconhecimento dos procedimentos básicos de por parte dos usuários. Saber como agir diante desses problemas, ajudará, e muito, nas investigações e resoluções de crimes virtuais, por isto este módulo trouxe explicação de alguns conceitos.

2.1.1 Dos assuntos abordados

Para iniciar o intuito do projeto explanaremos os assuntos que foram ministrados durante todo o projeto.

2.1.1.1 Princípios básicos

Figura 1: Pilares da Segurança da informação – Apostila desenvolvida pelos orientandos

Dentro destes direitos do usuário da rede, o mais importante é a segurança da informação, que dividido em cinco pilares permitindo que o usuário possa utilizar seus serviços em segurança. Os princípios básicos da segurança da informação são: integridade, confidencialidade, autenticidade, não repúdio e a disponibilidade. (PEIXOTO, 2006)

- Integridade: é a garantia que a informação não foi alterada sem a autorização do remetente durante o envio ou armazenamento.
- Confidencialidade: consiste em proteger a informação para que só pessoas autorizadas tenham acesso a ela. Esse mecanismo permite a privacidade dos dados.
- Autenticidade: é a comprovação de que a mensagem é realmente de quem diz ser, geralmente usamos senhas para comprovar nossa autenticidade.
- O não repúdio: são métodos que comprovam que o remetente enviou a mensagem, deixando-o impossibilitado de negar sua autenticidade.
- Disponibilidade: que garante que a informação esteja acessível quando o usuário necessitar dela.

2.1.1.2 Criptografia

A criptografia é a primeira técnica utilizada para proteção de informações. Ela consiste em transformar um dado legível em ilegível, que sem o auxílio de uma chave - senha, não pode ser interpretada, garantindo que apenas o receptor e o emissor possam acessá-las. Para isso vários tipos de criptografias podem ser usados, e ao passar do tempo modificada, aperfeiçoada e com o surgimento de novas outras de maneira, as tornar ainda mais seguras. [ALECRIM, 2005]

2.1.1.3 Esteganografia

A segunda técnica utilizada para proteção de dados é a esteganografia. Esta técnica é usada para mascarar mensagens, as inserindo dentro de outra informação, no qual apenas o receptor saberá a existência dessa mensagem ocultada dentro de outra mensagem. Ao longo da história, muitas técnicas de esteganografia foram desenvolvidas, um exemplo disso são as tintas invisíveis, elas visualmente eram apenas papeis, mas ao aquecidas mostravam a mensagem escrita. [ARTZ 2001].

2.1.1.4 Engenharia social

Primeiramente Engenharia Social é uma das técnicas utilizadas por Crackers que tem como objetivo obter acesso não autorizado a sistemas, redes ou informações com grande valor estratégico para as organizações. Os Crackers que utilizam desta técnica são conhecidos como Engenheiros Sociais. Esse termo ficou mais conhecido apenas em 1990, através de um famoso hacker conhecido como Kevin Mitnick.

Existem vários conceitos e interpretações dadas a Engenharia Social, mas uma das melhores é a seguinte:

> Engenharia social é uma ciência que estuda como o comportamento humano pode vim a ser utilizado de forma a induzir uma pessoa a fazer determinada coisa segundo seu desejo. Não se trata de controle de mente ou hipnose, porém as técnicas são amplamente utilizadas para obter informações, e para lograr todo tipo de fraude e inclusive invasão de sistemas eletrônicos. (KONSULTEX, 2004 apud PEIXOTO, 2006, p.4).

O principal motivo que leva a essa prática é que o ser humano é o elo mais fraco na segurança da informação, além disso, o desenvolvimento de tecnologias avançadas na segurança torna as invasões tecnológicas mais difíceis. Encontrar vulnerabilidades nesses sistemas demanda

um maior tempo e risco, sendo assim, explorar o fator humano é muito mais simples e menos arriscado.

"A engenharia social, propriamente dita, está inserida como um dos desafios (se não o maior deles) mais complexos no âmbito das vulnerabilidades encontradas na gestão da segurança da informação." (PEIXOTO, 2006, p. 36).

2.1.1.5 O comportamento humano

Abaixo são citados alguns dos comportamentos humanos que, quando adotados, facilitam os ataques dos engenheiros sociais deixando-os vulneráveis e suscetíveis a ataques da engenharia social: (JUNIOR, 2006).

- **Vaidade pessoal ou profissional**: O ser humano costuma ser mais receptivo as avaliações positivas e favoráveis aos seus objetivos;
- **Autoconfiança**: O ser humano busca transmitir em diálogos individuais ou coletivos o ato de fazer algo bem, buscando transmitir segurança, conhecimento, saber e eficiência;
- **Formação profissional**: O ser humano busca valorizar sua formação e suas habilidades, buscando o controle em uma comunicação, execução ou apresentação, seja ela profissional ou pessoal;
- **Vontade de se tornar útil**: O ser humano procura ser cortês ou ajudar os outros quando necessário.
- **Buscar amizades**: Os humanos costumam se sentir bem ao serem elogiados, de maneira que muitas vezes ficam abertos para fornecer informações.
- **Propagação de responsabilidade**: Trata-se da situação na qual o ser humano considera que ele não é o único responsável por um conjunto de atividades;

2.1.1.6 Como agem os engenheiros sociais

Antes de se proteger é necessário saber como os engenheiros sociais agem. Na apostila abordamos alguns tipos de ameaça que todos precisam saber para perceber quando esses engenheiros sutilmente tentam lhe persuadir para conseguir alguma informação. "Geralmente o engenheiro social é um tipo de pessoa agradável. Ou seja, uma pessoa educada, simpática, carismática. Mas, sobretudo criativa, flexível e dinâmica. Possuindo uma conversa bastante envolvente. " (ARAUJO, 2005, P.27).

A tabela abaixo mostra alguns tipos de invasores e seus respectivos objetivos ao utilizar a engenharia social. (POPPER; BRIGNOLI, 2003).

Tabela 1- tipos de invasores e seus objetivos

Tipos	Objetivo
Estudantes	Olhar mensagens de redes sociais, e-mails apenas por diversão ou curiosidade.
Crakers	Burlar sistemas de segurança e roubar informações confidenciais.
Representantes Comerciais	Encontrar planilhas referentes a preços ou cadastro de clientes.
Executivos	Descobrir esquemas militares
Terroristas Contadores	Causar pânico pela rede e roubar informações estratégicas. Desfalques financeiros.
Corretores de	Adulterar

valores	informações e obter lucro com valor das ações
Vigaristas	Roubar informações, como senhas e números de cartões de crédito.

Fonte: (POPPER/ BRIGNOLI,2003).

Os engenheiros sociais agem em uma espécie de ciclo, eles variam apenas as técnicas que utilizam em cada etapa. Esse ciclo é composto de quatro passos básicos, que não obedecem necessariamente a uma ordem fixa. (ALLEN, 2006, P.5)

Na primeira etapa, o engenheiro social faz uma pesquisa, recolhendo informações fáceis, geralmente de domínio público, para assim ficar a par do alvo a ser explorado. As redes sociais podem ser um exemplo de local de encontro dessas primeiras informações. Em seguida, o engenheiro começa a desenvolver um relacionamento com o alvo, conquistando a confiança da vítima. Uma das técnicas usadas nessa etapa é se passar por outra pessoa que seja leiga e busca ajuda, ou então fingir autoridade.

Após isso, quando ele já conhece e possui a confiança do seu alvo, ele parte para terceira etapa, iniciando assim a exploração das vulnerabilidades da vítima e através da manipulação recolhe as informações que realmente o interessam. Por último, ele faz o uso das informações adquiridas, caso essas informações sejam apenas uma etapa, ele retorna ao início do processo, até que o objetivo seja alcançado.

2.1.1.7 Termos da Segurança da Informação

Muitas pessoas usam esses termos de maneira equivocada, neste módulo é importante informar e esclarecer nomes como hackers e crackers, que muitas vezes são confundidos. Abaixo serão citados alguns desses termos e o que cada um deles significam:

- Hackers: aquele que possui conhecimento em linguagens de programação, sistemas operacionais e protocolos de rede, não relacionando esses conhecimentos a uma atividade maliciosa.

- Crackers: aqueles que também possuem o mesmo conhecimento de um Hacker, porém usam esse conhecimento para quebrar a segurança de sistemas, roubar informações, etc. Sempre em proveito próprio
- Phreakers: não muito encontrados nos tempos atuais, invadem e lesam os sistemas de telefonia, realizando chamadas gratuitas e clonagens de celulares.
- Script Kidies: utilizam algoritmos (programas) prontos, invadem e causam prejuízos sem ao menos saber o que estão fazendo.
- Lammers: são novos na área e usam um conhecimento que acreditam ter, porém não detém quase nenhuma bagagem técnica..
- Noobs: são novatos que apesar de não possuírem muito conhecimento na área, procuram se aprofundar no estudo das tecnologias. São bastante conhecidos por realizarem perguntas bobas em fóruns.

2.1.1.8 Páginas fakes

As páginas *fake* são um grande exemplo de métodos utilizados na Internet pelos engenheiros sociais para adquirir informações alheias. Elas são páginas falsas, que geralmente tentam simular o conteúdo de outras páginas. Geralmente imitam layout e o conteúdo de páginas de sites de empresas importantes, como de bancos ou de redes sociais.

2.1.1.9 Downloads de arquivos maliciosos

É muito comum ao fazer o download de alguma coisa, seja foto, musica, arquivos, vem de brinde arquivos executáveis e não só aquilo que foi solicitado. Com iss0 ao fazer download de programas ou de qualquer outro tipo de arquivo deve-se levar em consideração os perigos que o arquivo baixado pode trazer e se o site em que se está fazendo o download é de confiança. Basicamente, o perigo está nos chamados arquivos executáveis. Esses arquivos são facilmente identificados pela sua extensão, as letras que acompanham o nome do arquivo juntamente a um ponto (ex: arquivo.exe).

2.1.1.10 Boato

Boato ou hoax refere-se ao ato de espalhar informações com conteúdo duvidoso ou falso, sendo um ato muito comum em sites de redes sociais e principalmente de notícias. Geralmente para parecer mais verídico, tem como remetente, ou aponta como autora, alguma instituição, empresa importante ou organização governamental O boato se dissemina facilmente pela Internet em questão de minutos, assim como um vírus ao infectar sistemas. Essa é uma das práticas mais

comuns da engenharia social. Ela explora uma característica marcante em praticamente todos os seres-humanos, a curiosidade.

Segundo o comitê gestor de internet do Brasil, o boato pode provocar diversos problemas, tanto para aqueles que os recebem e os distribuem, como para aqueles que são citados em seu conteúdo. Entre estes diversos problemas, um boato pode:

- conter códigos maliciosos;
- espalhar desinformação pela Internet;
- comprometer a credibilidade e a reputação de pessoas ou entidades referenciadas na mensagem;
- comprometer a credibilidade e a reputação da pessoa que o repassa, pois, ao fazer isto, esta pessoa estará supostamente endossando ou concordando com o conteúdo da mensagem;
- aumentar excessivamente a carga de servidores de e-mail e o consumo de banda de rede, necessários para a transmissão e o processamento das mensagens;
- indicar, no conteúdo da mensagem, ações a serem realizadas e que, se forem efetivadas, podem resultar em sérios danos, como apagar um arquivo que supostamente contém um código malicioso, mas que na verdade e parte importante do sistema operacional instalado no computador.

2.1.1.11 Pop-ups

As pop-ups são janelas que abrem no navegador, sobressaindo a janela principal sem que o usuário tenha solicitado. A maioria dos navegadores atuais vem com uma Normalmente essas janelas aparecem quando você navega em sites de conteúdo duvidoso, sendo essas janelas comumente disseminadoras de conteúdo malicioso.

2.1.1.12 Deep web: uma lenda cibernética

A Deep Web corresponde a área da rede que exige métodos específicos para ser acessada, sendo capaz de proporcionar o anonimato, através da criptografia dos dados e pelo mascaramento do IP, evitando que ele seja rastreado. Com a não identificação dos usuários, as práticas ilegais surgem numa espécie de mercado negro de redes criminosas de todos os tipos, que vão desde o incentivo à violência por discriminação, à terroristas, nazistas, pedófilos e assassinos em série. Para acessar essa parte da internet que não estão indexadas ao DNS, é preciso instalar o Thor que mascara seu IP para que você não seja identificado.

2.1.1.13 Backup

O backup consiste na cópia de dados específicos, que podem ser restaurados caso ocorra uma perda dos originais, devido a problemas nos dispositivos, malwares, exclusão involuntária ou por outros motivos. É uma forma de manter os dados seguros. Quanto mais cópia se faz de um arquivo, menor é a chance de perdê-lo. O backup deve ser feito em locais ou dispositivos diferentes do original e até mesmo na nuvem.

2.1.1.14 Armazenamento em nuvem

A nuvem nada mais é do que um termo para se referir à Internet. Os arquivos podem estar visíveis para o usuário sempre, basta ele ter uma conexão com a Internet e poderá visualizá-los. O arquivo que nela se encontra pode ainda ser acessado por vários usuários em diferentes lugares. Desse modo, ao armazenar arquivos na Internet, mesmo que o usuário se desloque, poderá acessá-lo de diferentes dispositivos - computador, celular, tablet e diversos outros.

> O modelo de cloud computing, ou computação em nuvem, veio revolucionar o mercado de Tecnologia da Informação (TI). Essa forma de armazenamento se baseia em acessar e utilizar programas à distância, via internet, sem que seja necessário que essas ferramentas estejam instaladas localmente (no computador do usuário). Dessa forma, os softwares passam a ficar disponíveis em servidores, podendo ser utilizados a qualquer momento. (ANDRADE, 2010, p.1)

2.1.1.15 Malwares

A palavra "malware" abreviada do inglês "malicious software", trata-se de um termo geral dado à qualquer software malicioso destinado a causar danos em computadores ou servidores de forma ilegal, ou seja, qualquer tipo de software indesejado. Seu objetivo, depois de sua infiltração, é causar danos como apagar dados, roubar informações, alterar ou impedir o funcionamento do sistema operacional, dentre outros.

- pela exploração de vulnerabilidades existentes nos programas instalados;
- pelo auto execução de mídias removíveis t, incluem arquivos contendo códigos maliciosos;

- pela execução de arquivos previamente infectados, obtidos em anexos de mensagens eletrônicas, via mídias removíveis, em páginas Web ou diretamente de outros computadores (através do compartilhamento de recursos).

2.1.1.16 Tipos de Malwares

- Vírus: Necessitam de um hospedeiro, semelhante ao vírus biológico; se infiltram em um arquivo ou programa alterando-o de maneira nociva; multiplicam-se rapidamente fazendo várias cópias de si mesmo; se escondem para não serem excluídos.

- Worms: Não necessitam de um hospedeiro; se replicam sós, podendo excluir arquivos, enviar documentos, e deixar o sistema vulnerável a outros ataques; podem ser espalhados pela rede, drives USB e e-mails infectados.

- Keyloggers: Capturam as teclas digitadas e enviam para o e-mail do invasor ou em tempo real; uma variação desses malwares são os Screenloggers, que capturam imagens das telas. Lentidão acompanhada de uma piscada instantânea no cursor, ou tela, podem ser sintomas que seu dispositivo está infectado.

- Ransomwares: Restringem o acesso ao sistema ou a arquivos específicos e cobram um valor resgate para o acesso ser restabelecido; podem ser instalados através de links falsos, e-mails ou em sites maliciosos.

- Spywares: Sua principal função é capturar informações; pop-ups são um dos sintomas; alteram a página de navegação e configurações de pesquisa; se instalam através de programas sobrepostos ou downloads guiados.

- Adwares: Exibem propagandas e anúncios sem autorização através de pop-ups; enviam spam, fazem redirecionamento automático nas páginas.

- Cavalo de Tróia ou trojan: Chegam como presentes disfarçados de outros arquivos; quando aceitos abrem portas para outras pragas; roubam senhas, alteram e destroem arquivos.

2.1.1.17 Antivírus

É um tipo de ferramenta desenvolvida para detectar, remover e bloquear ações mal-intencionadas provocadas por vírus e outros malwares que prejudicam o bom funcionamento de diversos dispositivos. Um Antivírus pode vir com outros softwares incorporados a ele, como: antispywares e firewalls pessoais, tornando-o mais seguro.

2.1.1.18 Biblioteca e vacinas

A biblioteca do antivírus consiste em uma espécie de lista de vacinas que atuam contra o malware detectado, isto é, são códigos desenvolvidos a partir dos malwares detectados após a atualização do Antivírus. Quando o antivírus detecta linhas de códigos idênticas ou semelhantes a vacina, ele bloqueia, remove ou os deixa em quarentena, sendo assim, o desenvolvedor responsável pelo antivírus, busca na rede novas ameaças para a atualização da biblioteca, aumentando a quantidade de vacinas.

2.1.1.19 Virustotal

O VirusTotal é um serviço gratuito online que analisa arquivos e URLs suspeitas e facilita a rápida detecção de vírus e de todos os tipos de arquivos maliciosos até mesmo de falsos positivos. Ele é composto por 52 antivírus que escaneam separadamente os arquivos ou URLs, não causando conflito entre os antivírus, tornando-o seguro.

2.1.1.20 Antispyware

Antispyware é um software de segurança utilizado para detectar, bloquear ou remover malwares do tipo spyware ou adware, bloqueando pop-ups, barra de ferramentas indesejadas, baixo desempenho e ameaça de segurança provocados por esses softwares maliciosos. A principal diferença de um antispyware para um antivírus é a classe de programas que eles removem.

Alguns exemplos de softwares de remoção dos spywares são: Windows Defender; Spybot; Spyware Terminator; Ad-Aware e Spy Sweeper.

2.1.2 Das Práticas

As práticas desse módulo foram voltadas para os malwares, para que as pessoas vissem na prática como eles funcionam. Inicialmente infectamos as máquinas, estas que eram virtuais, com vários malwares. Os participantes puderam ver um keylloger coletando os dados digitados no teclado e vários pop-ups, gerando lentidão e baixo desempenho do processador. Em seguida instalamos um bom antivírus, de acordo com o ranking que fizemos e que foi mostrado durante o minicurso, acompanhado de um bom antispyware, para limpar a máquina totalmente infectada.

Alguns vídeos foram selecionados para esclarecer algumas dúvidas e servir de reforço à apresentação. Após a explicação da criptografia mostramos um vídeo para ilustrar de forma mais simples este assunto, visto que era um bate-papo bem informal para descobrir qual mensagem foi criptografada.

Na parte da explicação dos malwares foi mostrado o vídeo que diferencia o vírus de um worm, para reforçar o que foi dito e um vídeo sobre toda a evolução dos vírus de computador, para dar uma ideia mais ampla de todo contexto que surgiu, se aperfeiçoando até os dias de hoje. E por fim foi mostrado um vídeo sobre o spam, o que é e como pode ser identificado, sendo uma das coisas mais chatas e indesejadas desse mundo virtual.

2.2 MÓDULO II: Segurança em Redes Sociais e Dispositivos Móveis

O módulo 2 foi desenvolvido para que o foco fosse os meios em que os usuários mais sentem dificuldade e expõe mais suas informações pessoais, os dispositivos móveis e as redes sociais. Desenvolvemos em cima da problemática da engenharia social aplicada em redes sociais, de como as pessoas mal-intencionadas exploram todo o conteúdo que é colocado nessas ferramentas e de todas as ameaças que estamos propensos a enfrentar por meio delas. Além de todo o histórico das redes sociais digitais, para que todos soubessem como se deu a evolução delas até chegar nessas plataformas sociais integradas como as de atualmente.

2.2.1 Dos assuntos abordados

A seguir serão listados os assuntos abordados no segundo módulo. Esta diferenciação foi feita para separarmos a parte conceitual das práticas desenvolvidas no projeto.

2.2.1.1 Redes sociais

Sabemos que desde os primórdios da humanidade o homem sempre sentiu a necessidade de interações sociais através de semelhanças e compatibilidade. Entendemos como redes sociais qualquer grupo que partilhe um interesse em comum, um ideal ou preferência, como clube de futebol, igreja, ou mesmo, sala de aula.

Quando essa interação parte para o ambiente online, temos as chamadas redes sociais digitais, que vêm passando constantemente por uma série de evoluções. Essas Redes sociais digitais nos permitem uma infinidade de coisas, desde encontrar emprego e fazer amizades, através das relações entre as pessoas conhecidas. Porém deve-se ter cuidados na hora de postar, compartilhar informações nesta rede.

2.2.1.2 Ameaças nas redes sociais

As ameaças que podem surgir com o advento das redes sociais são as páginas fake e o phishing. As páginas falsas (fake) são bastante comuns quando o engenheiro social deseja coletar informações manipulando seu alvo. Normalmente, essas páginas simulam o layout, URL (endereço web) e conteúdo das páginas originais, com a intenção de convencer a vítima que aquela conexão é segura e autêntica.

O *phishing* também é um recurso da página falsa, mas seu objetivo principal é coletar dados pessoais, como senhas ou dados financeiros, através de uma comunicação eletrônica digital. Geralmente isso é feito através de formulários HTML que o usuário preenche inocentemente e depois envia, acreditando estar em uma conexão autêntica devido à semelhança a uma página original.

2.2.1.3 Email

Além das redes sociais, o e-mail é uma importante ferramenta de comunicação em que se deve ter cuidado também nos e-mails que te solicitam dados pessoais, podendo ao clicar, lhe redirecionar para uma página falsa e pegar seus dados com o phishing. Além disso, possui o Spam, um termo usado para referir-se aos e-mails não desejados e nem solicitados, que geralmente são enviados para um grande número de pessoas sem a devida autorização. Quando o conteúdo é exclusivamente comercial, esse tipo de mensagem é chamado de UCE (do inglês e-mail comercial não solicitado).

2.2.1.4 Autenticação

Nesse módulo também temos os assuntos que abordam um dos princípios da segurança da informação, a autenticidade. Esta que possui três tipos: Por característica, por propriedade e por conhecimento. [ANTUNES, 2014]

- A autenticação baseada no conhecimento: refere-se à autenticação cujos dados de acesso ou o mecanismo, baseia-se em algo que o usuário sabe. É o método mais comum, geralmente utiliza um dado único (e-mail, nome de usuário, id) e uma senha que deve ser de conhecimento apenas do usuário ao qual pertence.
- A autenticação baseada na propriedade: diz respeito à autenticação baseada naquilo que o usuário possui que pode ser um cartão ou qualquer outro dispositivo eletrônico capaz de fazer comunicação com um sistema. Existe a desvantagem que esse objeto pode ser perdido.

- A autenticação baseada na característica: é aquela à qual se baseia em algo que o usuário é. O exemplo mais clássico é a biometria baseada na entrada da digital do usuário. Outros métodos já são conhecidos, como a leitura da íris, batimentos cardíacos, reconhecimento facial, da mão, dentre outros.

2.2.1.5 Autenticação em dois passos

Existe ainda autenticação de dois passos um processo que se dá através da autenticação da senha e código relacionado a algo físico do usuário. Por exemplo, quando cadastramos o nosso e-mail e o vinculamos a algum celular e fazemos esta atualização, a conta trabalhará com este tipo de autenticação, na qual, qualquer mudança que requerida pelo usuário - que já autenticou sua senha - também necessitará a autenticação do código que seria enviado ao celular do usuário para comprovar virtual e fisicamente sua autenticidade. Quase todas as redes sociais e serviços web já fornecem a possibilidade de autenticação em dois passos.

2.2.1.6 Senhas

Recomenda-se, criar uma senha misturando letras maiúsculas, minúsculas, números e sinais de pontuação. Vale ressaltar que é preferível anotar a senha e guardá-la em local seguro, do que optar pelo uso de senhas fracas apenas para memorização mais conveniente. (CERT.br, 2006, p.3, grifo do autor).

Algumas dicas de elaboração de senhas, são dadas pelo Centro de Atendimento a Incidentes de Segurança (CAIS/RNP)

> Use pelo menos 8 caracteres na sua senha. Utilize números, letras maiúsculas e minúsculas, alguns caracteres especiais (“_” e “-” são os mais indicados). Os sites normalmente indicam se a senha que você escolheu é “Forte” ou não. Escolha senhas que indiquem “Strong” (Forte) ou “Very Strong” (Muito forte). Não use a mesma senha de outros serviços! Use um software para gerenciar suas senhas. (...) troque sua senha com frequência, especialmente quando utilizar o serviço de redes sociais em locais públicos como redes Wi-Fi de aeroportos, eventos, lan houses ou no computador de outra pessoa. (CAIS/RNP, 2011, p.2)

2.2.1.7 Segurança em dispositivos móveis

Por fim, sendo o último assunto da apostila, a segurança em dispositivos móveis. É muito importante ser abordado pois nos dias atuais, os smartphones estão presentes em nossas vidas muito mais que os nossos computadores por vários motivos, seja oferecendo a mobilidade ou a

praticidade que ele propõe, sendo capazes de executar grande parte das ações realizadas por computadores pessoais.

Devido a quantidade de troca de dados entre a rede e o celular ser enorme e vêm crescendo a cada dia, é extremamente necessário que tomemos precauções para garantir que os dados que depositamos nele continue intactos. Para isto, é necessário definir uma senha para acessar o dispositivo, fazer backup dele e/ou usar o serviço de localização para casos de perda.

Com isso é relevante trazer a questão de segurança e como aplicá-las de maneira mais correta, uma vez que estes dispositivos são mecanismos que podem ser vulneráveis a diferentes tipos de ataques.

A Segurança relacionada ao Android é uma questão sensível, sendo um sistema altamente criticado devido as suas falhas de segurança que podem ser exploradas facilmente por pessoas mal-intencionadas.

Diferente do Android, o Windows Phone tem uma plataforma desenvolvida de modo que ele seja seguro por design. Muitos recursos de segurança estão ligados por padrão, como por exemplo, aplicativos baixados da Loja do Windows Phone são testados pela Microsoft e criptografados para garantir que você não instale acidentalmente software malicioso no seu telefone, pois eles analisam todos os aplicativos que os desenvolvedores enviam procurando por malwares ou problema técnicos. Segundo uma pesquisa feita pela empresa de segurança digital Sourcefire, o Windows Phone é realmente um sistema operacional mais seguro do que o iOS da Apple e do que o Android da Google.

O sistema operacional IOS Apesar de uma distribuição Unix exclusiva da Apple, diferente do que todos pensam, ele também possui vírus. A questão é a quantidade, dizem que por ser pouco não se deve tomar precauções. Bem, uma coisa é verdade: a quantidade de vírus para iOS comparado a Android é mínima, mas é importante tomar precauções uma vez que o iOS não possui nenhum aplicativo antivírus nativo ou embutido, isso não quer dizer que ele está livre de ataques.

2.2.2 Das práticas

As práticas destinadas a esse módulo focaram mais na parte da segurança pessoal dos participantes. Nós ensinamos como retirar uma informação sua do Google que não seja desejada através de sua política de remoção. Em seguida, exploramos um pouco as configurações de privacidade das redes sociais, deixando algumas informações do perfil privadas, evitando um ataque futuro de engenharia social.

A outra prática foi sobre e-mail, um assunto que foi abordado no minicurso. O objetivo dessa prática foi colocar filtros AntiSpam e limpar a caixa entrada do e-mail deixando apenas os que são desejados. Com isso foi adicionado regras do que é ou spam para cada usuário.

Passamos também vídeos de alertas sobre o de redes sociais e a engenharia social, para que pensassem antes de postar qualquer coisa em seu perfil, pois como a informação está sendo muito difundida não é importante ficar atento e pensar duas vezes antes de postar ou compartilhar qualquer coisa na rede, pois não tem volta.

2.3 MÓDULO III: Instalação e configuração de roteadores wireless em redes domésticas

Devido alguns problemas de final de ano letivo, não conseguimos desenvolver a apostila e nem a aplicação do minicurso. A ideia seria que apenas pessoas com um conhecimento um pouco mais técnico viesse a participar, visto que seriam dados alguns conceitos e o ideal seria que existisse uma continuidade dos módulos anteriores.

2.3.1 Dos assuntos

Os assuntos que seriam tratados neste módulo são aqueles que são necessários para a instalação e configuração de roteadores wireless em redes domésticas, tais como princípios básicos de redes LAN e W-LAN, endereçamento IP, serviços de rede, redes sem fio, entender as diferenças entre os equipamentos de rede: Hub, Switch, Roteador, Access Point e conhecer os protocolos de segurança WEP, WPA, WPA2, WPS.

3. RESULTADOS

Após cada módulo fizemos um formulário para que os alunos pudessem avaliar o nosso projeto. As perguntas serviram de feedback para que pudéssemos melhorar nos próximos módulos. De acordo com os dados coletados a maioria respondeu que os ministradores do projeto souberam explicar bem o conteúdo, com paciência, relacionando os assuntos as práticas. Houve também sugestão de que nos próximos tivesse mais prática e um pouco mais de duração em cada dia de minicurso.

Ao final, temos como resultado a apresentação de dois módulos cada um com sua respectiva apostila e determinado foco. O módulo 1 que é a introdução a segurança da informação possui uma apostila bem didática contendo 45 páginas e a apresentação de slides para auxiliar à apresentação. O módulo 2, focado à segurança dos dispositivos móveis e as redes sociais, possui uma apostila com 74 páginas, podendo ser disponibilizada para as pessoas que desejam e que participaram do minicurso.

4. CONSIDERAÇÕES FINAIS

Nesse relatório procurou-se mostrar como se deu o desenvolvimento desse projeto de extensão, desde desenvolvimento do material didático através do levantamento bibliográfico até a preparação e aplicação do minicurso no campus no IFRN.

Todos os assuntos abordados foram devidamente selecionados de forma que fosse relevante a explicação de acordo com o contexto de cada módulo, correlacionando todos com o nosso objetivo principal que foi proporcionar um ambiente em que pessoas de dentro e fora do nossa instituição tivessem a oportunidade de se informar sobre a segurança da informação de modo a evitar incidentes de segurança devido o desconhecimento de práticas.

Acredita-se, que embora o módulo 3 não tenha sido aplicado, o projeto foi concluído de forma satisfatória e com uma boa quantidade de participantes sabendo como se proteger melhor nesse mundo virtual, principalmente as redes sociais e os ataques de engenharia social. Além disso, alguns conceitos básicos e essenciais á segurança da informação, como criptografia, esteganografia, autenticação, senhas, foram relacionados as práticas para que fossem melhor entendidos.

REFERÊNCIAS

ALECRIM, Emerson. **Criptografia.** Disponível em:<http://www.infowester.com/criptografia.php> Acesso em: 05 de março de 2016.

ALLEN, Malcolm. **Social Enginnering: A Means to Violate a Computer System. SANS Institute InfoSec Reading Room**. Disponível em: <http://www.sans.org/reading_room/whitepapers/engineering/social-engineering means-violate-computer-system_529> Acesso em: 06 de março de 2016.

Andrade, D.J.de. **Computação no mundo das nuvens. Instituto de Educação Superior. Brasília, 2010**. Disponível em:< http://www.iesb.br/moduloonline/napratica/?fuseaction=fbx.Materia&CodMateria=5024>. Acesso em: 07 de março de 2016.

ANTUNES, BRUNO. **Conheça os 3 tipos de métodos de autenticação.** Disponível em:<http://segurancaemsimplesatos.com.br/blog/conheca-os-3-tipos-de-metodos-de-autenticacao/> Acesso em: 05 de março de 2016.

ARTZ, D. **Digital Steganography: Hiding Data within Data. IEEE Internet Computing**, p. 75-80, maio/junho 2001.

CARDOSO, Ruth. O Sistema Operacional Móvel da Apple. Disponível em:<http://pt.slideshare.net/lyzaseiko/ios-sistema-operacional> Acesso em: 05 de março de 2016.

Cartilha de segurança para internet. Mecanismos de segurança. Disponível em:<http://cartilha.cert.br/mecanismos/>. Acesso em: 07 de março de 2016.

JUNIOR, Guilherme. **Entendendo o que é Engenharia Social.2006.**

Disponivel em: http://www.vivaolinux.com.br/artigo/Entendendo-o-que-e-Engenharia-Social. Acesso em: 28 fevereiro de 2016.

UFRGS. **Autenticação de Usuários**. Disponível em:<http://penta.ufrgs.br/pesquisa/fiorese/autenticacaoeadcap2.htm/> Acesso em: 05 de março de 2016

UFRJ. **Esteganografia**. Disponivel em:<http://www.gta.ufrj.br/grad/09_1/versao-final/stegano/introducao.html/> Acesso em: 28 fevereiro de 2016.

PEIXOTO, Mário C.P. **Engenharia Social e Segurança da Informação na Gestão Corporativa.** Rio de Janeiro: Brasport, 2006. Disponível em: <http://www.cippguide.org/2010/08/03/cia-triad/>. Acesso em: 25 de fevereiro de 2016

PILARES da segurança da informação. Disponível em: http://www.f4.inf.br/wp-content/uploads/2015/06/pilares_da_seguranca.png. Acesso em: 28 de fevereiro de 2016

POPPER, Marcos Antonio; BRIGNOLI, Juliano Tonizetti. **ENGENHARIA SOCIAL: Um Perigo Eminente. [2003]. Monografia (Especialização)- Gestão Empresarial e Estratégias de Informática, Instituto Catarinense de Pós –Graduação- ICPG, 2003.** Disponível em: <http://fabricio.unis.edu.br/SI/Eng_Social.pdf> . Acesso em: 28 de fevereiro de 2016.

SCRIPT BRASIL. Windows Phone - Origem e Curiosidades. Disponível em:<http://www.scriptbrasil.com.br/celulares-e-tablets/windows-phone/windows-phone-origem-e-curiosidades.html> Acesso em: 05 de março de 2016.

SILVA, Maicon H. L. F. DA; COSTA, V.A DE S . F. **O fator humano como pilar da Segurança da Informaçao:** uma proposta alternativa. Serra Talhada (PE), 2009.

TERRA. Dicas de segurança iOS. Disponível em:<http://tecnologia.terra.com.br/dicas-seguranca-ios/> Acesso em: 24 de nov 2015.