ISSN 2763-616X
DOI 10.20396/ijoce.v3i00.16021

PRÁTICAS EM EXTENSÃO UNIVERSITÁRIA

EXTENSÃO UNIVERSITÁRIA
Uma abordagem teórica e prática diante de atividades maliciosas em home office, boas práticas e prevenção

Andressa Fouchy Schons
Universidade Tecnológica Federal do Paraná, Ponta Grossa, PR, Brasil, andressa.schons@acad.ufsm.br
Marcia Henke
Universidade Federal de Santa Maria, Santa Maria, RS, Brasil, marcia.henke@ufsm.br
Simone Regina Ceolin
Universidade Federal de Santa Maria, Santa Maria, RS, Brasil, sceolin@redes.ufsm.br

RESUMO
O projeto de extensão, Segurança física e lógica no ambiente organizacional, uma abordagem teórico e prática, criado em 2016, tem como linha de extensão a Tecnologia da Informação, atende a política de extensão da UFSM e o Plano de Desenvolvimento Institucional (PDI - CTISM/UFSM). Tendo como principal meta o fortalecimento do vínculo da Instituição de Ensino com o ambiente corporativo, levando à comunidade alertas e boas práticas para mitigar atividades maliciosas no uso da Internet. Durante os anos de aplicação, foi visto que a extensão universitária desempenha um papel muito maior do que o de democratizar o conhecimento, como também de aproximar a comunidade em geral da instituição de ensino, adequando a pesquisa ao contexto da população em geral. Tornando-se um meio de interligação do ensino com a pesquisa e a prática em meio a comunidade. O presente artigo aborda os principais resultados do projeto mencionando as diretrizes de extensão universitária através do seu objetivo principal

PALAVRAS-CHAVE
Extensão universitária; Sistema computacional; Crimes virtuais

UNIVERSITY EXTENSION
A theoretical and practical approach to malicious activities in the home office, good practices and prevention

ABSTRACT
The extension project, Physical and logical security in the organizational environment, a theoretical and practical approach, created in 2016, has Information Technology as its extension line, meets the UFSM extension policy and the Institutional Development Plan (PDI - CTISM /UFSM). Its main goal is to strengthen the link between the Educational Institution and the corporate environment, bringing alerts and good practices to the community to mitigate malicious activities in the use of the Internet. During the years of application, it was seen that university extension plays a much greater role than that of democratizing knowledge, as well as bringing the general community closer to the educational institution, adapting the research to the context of the general population. Becoming a means of interconnecting teaching with research and practice in the community. This article addresses the main results of the project mentioning the university extension guidelines through its main objective.

KEYWORDS
University extension; Computer system; Cybercrimes.

Submetido em: 22/12/2021 **– Aprovado em:** 17/12/2022 **– Publicado em:** 19/12/2022

1. INTRODUÇÃO

A internet já tomou uma proporção enorme na vida das pessoas, sabendo-se que junto com todas as facilidades que se tem através da rede mundial de computadores estão uma série de vulnerabilidades. A pandemia do Coronavírus somente intensificou o uso da internet para manter o fluxo de trabalho em casa, *home office*, e aulas online, dando uma leve sensação de normalidade à situação; porém a exposição às vulnerabilidades da internet aumentarem consideravelmente diante de um ambiente sem regras e sem controle, onde atacantes se aproveitam desse cenário para disseminar atividades maliciosas, aplicando golpes e ataques contra usuários desinformados. Muitas pesquisas mostram que o fator humano é um fator de alvo dos atacantes para a disseminação dessas atividades maliciosas, por exemplo:

- Alcoforado, Ribeiro e Cunha (2012) constatam que os principais problemas de segurança da informação em uma empresa são muito mais sociológicos do que tecnológicos, enfatizando os recursos humanos como elo mais fraco de um processo de segurança de informação. Relatam a importância de uma política de segurança adotada pelas empresas para proteção dos ativos informacionais e comprometimento da empresa com divulgação ampla da política e medidas educacionais, treinando a equipe para que sejam adotados os procedimentos da política de segurança. Também salienta-se que os três itens mais importantes na segurança da informação seriam: a elaboração de uma política de segurança, gerenciamento de suporte adequado e nível de conscientização dos funcionários.
- Silva, Araújo e de Azevedo (2013) constatam que as redes sociais tornaram públicas informações pessoais, visto que há a necessidade do usuário compartilhar seu círculo de amigos, locais que visita, cargo em determinada empresa e outros detalhes para a criação do seu perfil. Pois, os engenheiros sociais utilizam esse perfil para a criação de perfis falsos em redes sociais com a finalidade de efetuar um ataque, ou para o levantamento de outros dados mais importantes, como os de renda.
- Moreira (2019) abordou dados relacionados à influência de engenheiros sociais sobre usuários. Os ataques efetuados pelos engenheiros normalmente não são abordados dentro da Segurança de TI, já que não deixam rastros, tornando difícil se descobrir quem o efetuou. Comenta que os engenheiros sociais utilizam dois tipos de abordagem: a direta e a indireta, a primeira quando se utiliza de contato com a vítima, por mensagens ou até pessoalmente, e a segunda consiste na aplicação de mecanismos como spywares, softwares ou perfis falsos em redes sociais, ambas abordagens partem do princípio do fator humano. Moreira enfatiza que as empresas desenvolvem maneiras de proteger as vulnerabilidades do sistema, mas esquecem das fraquezas humanas. O autor ressalta a importância de um Termo de Política de Segurança, sendo esse um documento no qual constam os meios de conscientização dos trabalhadores para os riscos decorrentes de ataques efetuados por engenheiros sociais;
- Nagli (2020) apresenta que o isolamento social e a migração para o *home office* aumentaram a exposição dos funcionários aos crimes cometidos em meio virtual, ressaltando ainda que o usuário não teve preparo prévio sobre como se proteger deles. Demonstra, também, os impactos dessa mudança brusca, como o

Spear-Phishing, em que se usam das informações coletadas previamente para que o ataque tenha maior taxa de sucesso, ou da Engenharia Social e a necessidade da educação digital, visto que o *home office* exige a, chamada pelo autor, higiene digital, um conjunto de regras para proteção dos usuários. Também destaca que dentro do ambiente de trabalho existem meios de proteção e monitoramento ao contrário do que ocorre quando se está trabalhando de casa, deixando o usuário um alvo mais vulnerável a ataques. Enfim, o autor utiliza das medidas de proteção ao coronavírus como uma analogia às medidas que devem ser tomadas para se proteger dos crimes virtuais, demonstrando que as equipes devem estar preparadas para essa nova forma de trabalho.

A partir deste contexto se pode observar que o fator humano ou usuário apresenta grande vulnerabilidade no uso dos sistemas computacionais. Os ataques por meio virtual dão-se por uma fragilidade humana, que pode acabar causando um estrago descomunal para a organização. Conscientizar o usuário da sua responsabilidade sobre o uso da internet contribui significativamente na mitigação das atividades maliciosas juntamente com as técnicas e estratégias de configuração de servidores, softwares de proteção, antivírus entre outros. Logo, mantendo uma postura preventiva, pode-se mitigar tais atividades maliciosas. Para tanto, este artigo apresenta na Seção 2 a metodologia abordada antes e depois da pandemia para atingir o público. A Seção 3 exibe as ações do projeto, finalizando com a conclusão na Seção 4.

2 METODOLOGIA

Esta seção apresenta a metodologia inicial aplicada ao projeto e a necessidade de modificá-la durante a pandemia.

2.1 Antes Da Pandemia (Covid-19)

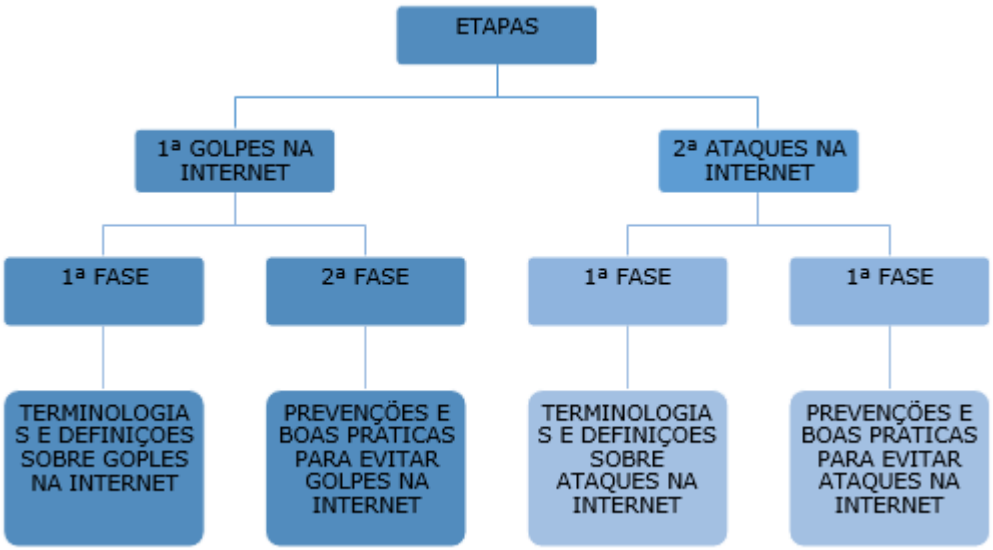
A metodologia deste trabalho consiste de uma análise descritiva qualitativa de cunho crítico-reflexivo acerca de um relato de experiência a partir das ações realizadas em um projeto de extensão desde 2016. Assim, nesta seção será apresentada a forma como foi conduzida a aplicação desse projeto, assim como serão caracterizados os estudantes e o público alvo. A aproximação entre estudantes e público externo oportunizou a troca de conhecimento a partir dos assuntos abordados e a interação dos participantes.

Os estudantes voluntários e bolsistas que compõem o projeto são oriundos do Curso Superior de Tecnologia em Redes de Computadores da Universidade Federal de Santa Maria (UFSM) e do Ensino Médio Técnico de Informática para Internet do Colégio Técnico Industrial de Santa Maria (CTISM). O público externo envolvido no projeto foi composto pelas Organizações Militares de Santa Maria e Base Aérea (ALA 4), com média de 20 participantes. Os encontros ocorreram quinzenalmente nos laboratórios de informática do CTISM/UFSM e os workshops foram ministrados pela coordenadora do projeto com auxílio dos alunos participantes.

O projeto é executado em duas etapas que são divididas em duas fases. Cada fase é composta por

dois encontros de 4 horas. A primeira etapa aborda os golpes na Internet a partir do estudo das suas terminologias e das boas práticas para se evitar esses golpes. A segunda etapa, trata dos ataques na internet e as terminologias usadas para esses ataques, assim como orientações para evitá-los. A Figura 1 apresenta um diagrama da metodologia aplicada para execução do projeto.

Figura 1 – Diagrama da Metodologia Aplicada para Execução do Projeto

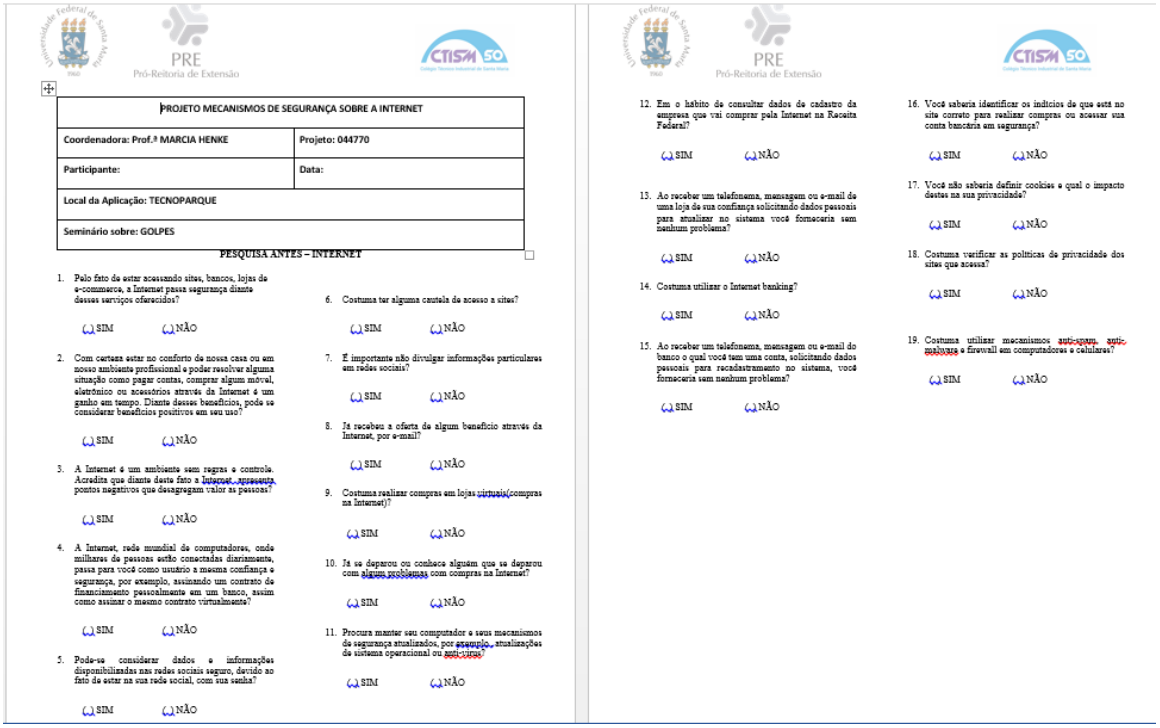


Fonte: Autoria própria

Desta forma os alunos possuem dois encontros de quatro horas cada um com cada turma do público externo durante a execução do projeto de extensão.

A formação das turmas, dos alunos com o público externo, aconteceu a partir de workshops e práticas em laboratório o que proporcionou aos estudantes contato com um público diversificado e com uma interação dialógica repleta de fatos diferenciados. Além da troca de informações e discussão de fatos que os participantes compartilharam ao longo da explanação sobre as boas práticas para uso seguro na Internet, foi aplicado um questionário, Figura 2, com o objetivo de identificar as necessidades do público quanto às abordagens de segurança para uma melhoria contínua nos workshops.

Figura 2 – Amostra de Questionário Aplicado ao Público Alvo no Workshop Golpes



PRE
Pró-Reitoria de Extensão

PROJETO MECANISMOS DE SEGURANÇA SOBRE A INTERNET	
Coordenadora: Prof.ª MARCIA HENKE	Projeto: 044770
Participante:	Data:
Local da Aplicação: TECNOPARQUE	
Seminário sobre: GOLPES	

PESQUISA ANTES – INTERNET

1. Pelo fato de estar acessando sites, bancos, lojas de e-commerce, a Internet passa segurança diante desses serviços oferecidos?
( ) SIM ( ) NÃO
2. Com certeza estar no conforto de nossa casa ou em nosso ambiente profissional e poder resolver alguma situação como pagar contas, comprar algum móvel, eletrônico ou acessórios através da Internet é um ganho em tempo. Diante desses benefícios, pode se considerar benefícios positivos em seu uso?
( ) SIM ( ) NÃO
3. A Internet é um ambiente sem regras e controle. Acredita que diante desta fato a Internet apresenta pontos negativos que desagregam valor as pessoas?
( ) SIM ( ) NÃO
4. A Internet, rede mundial de computadores, onde milhares de pessoas estão conectadas diariamente, passa para você como usuário a mesma confiança e segurança, por exemplo, assinando um contrato de financiamento pessoalmente em um banco, assim como assinar o mesmo contrato virtualmente?
( ) SIM ( ) NÃO
5. Pode-se considerar dados e informações disponibilizadas nas redes sociais seguro, devido ao fato de estar na sua rede social, com sua senha?
( ) SIM ( ) NÃO
6. Costuma ter alguma cautela de acesso a sites?
( ) SIM ( ) NÃO
7. É importante não divulgar informações particulares em redes sociais?
( ) SIM ( ) NÃO
8. Já recebeu a oferta de algum benefício através da Internet, por e-mail?
( ) SIM ( ) NÃO
9. Costuma realizar compras em lojas virtuais(compras na Internet)?
( ) SIM ( ) NÃO
10. Já se deparou ou conhece alguém que se deparou com algum problemas com compras na Internet?
( ) SIM ( ) NÃO
11. Procura manter seu computador e seus mecanismos de segurança atualizados, por exemplo, atualizações de sistema operacional ou anti-virus?
( ) SIM ( ) NÃO

PRE
Pró-Reitoria de Extensão

12. Em o hábito de consultar dados de cadastro da empresa que vai comprar pela Internet na Receita Federal?
( ) SIM ( ) NÃO
13. Ao receber um telefonema, mensagem ou e-mail de uma loja de sua confiança solicitando dados pessoais para atualizar no sistema você forneceria sem nenhum problema?
( ) SIM ( ) NÃO
14. Costuma utilizar o Internet banking?
( ) SIM ( ) NÃO
15. Ao receber um telefonema, mensagem ou e-mail do banco o qual você tem uma conta, solicitando dados pessoais para recadastramento no sistema, você forneceria sem nenhum problema?
( ) SIM ( ) NÃO
16. Você saberia identificar os indícios de que está no site correto para realizar compras ou acessar sua conta bancária em segurança?
( ) SIM ( ) NÃO
17. Você não saberia definir cookies e qual o impacto destes na sua privacidade?
( ) SIM ( ) NÃO
18. Costuma verificar as políticas de privacidade dos sites que acessa?
( ) SIM ( ) NÃO
19. Costuma utilizar mecanismos anti-spam, anti-malware e firewall em computadores e celulares?
( ) SIM ( ) NÃO

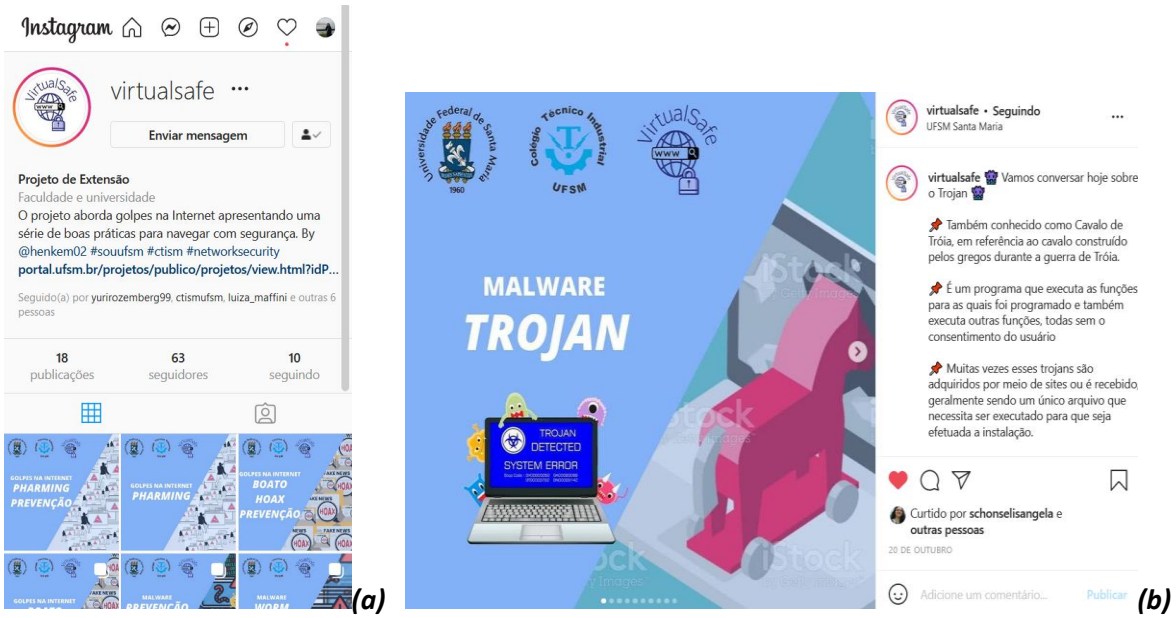
Fonte: As autoras.

Os estudantes construíram saberes a partir das discussões com a equipe do projeto que tinha como base a interação presencial e a interação a partir do questionário. As perguntas auxiliaram na direção do aperfeiçoamento do que era visto nos workshops e das necessidades apresentadas pelo público externo. A partir dessa direção os estudantes realizavam pesquisas, sendo elas necessárias para confeccionar novas práticas e alimentar a página do projeto no Moodle, mantendo a interação com os participantes a partir da disponibilização de material atual sobre as boas práticas.

2.2 Durante Pandemia

Com o início da pandemia da covid-19 e a grande necessidade do distanciamento social, as atividades práticas do projeto foram pausadas. Contudo, o novo cenário somente demonstrou a necessidade do projeto diante do uso intensificado da internet, desta forma o projeto direcionou sua abrangência através das redes sociais e uma página exibindo objetivos e ações do projeto. Adaptou-se o conteúdo do projeto para o meio virtual, a Figura 5 apresenta uma amostra da interação e disseminação dos principais golpes e ataques apresentados aos usuários e como se proteger.

Figura 5 – Post sobre as redes sociais, Instagram, do Projeto, figura (a) apresenta a "bio" do projeto e a figura (b) um post no *feed* do projeto.



Fonte: As autoras.

Pode-se ter acesso ao Instagram do projeto pelo apelido "Virtual Safe", @virtualsafe, onde, em parceria com outros departamentos da UFSM, as informações são disseminadas através das Hashtag (#), com o intuito de atingir aos usuários e levar as informações pertinentes sobre possíveis atividades maliciosas. A página do projeto está inserida no portal da UFSM, https://www.ufsm.br/unidades-universitarias/ctism/virtualsafe.

3 AÇÕES E CONSIDERAÇÕES

3.1 Correlação Do Projeto E As Diretrizes De Extensão

No decorrer do projeto, foram percebidas respostas às diretrizes de extensão universitárias propostas pela UFSM (UFSM, 2008). As diretrizes são utilizadas para levantamento da interferência que o projeto tem na comunidade, algumas delas dizem respeito ao impacto dentro da comunidade universitária e outras que visam o impacto na sociedade em geral. Apresentamos, na Tabela 1, o resultado obtido em cada uma das diretrizes de extensão.

Quadro 1 - Resultados a partir das Diretrizes para Ação de Extensão Universitária

Diretrizes	**Resultados**
Interação Dialógica	Surge naturalmente a partir dos assuntos abordados em questões sobre segurança na Internet. A participação do público é instigada com apresentação de fatos ocorridos sobre as ameaças e o modo comportamental dos usuários na rede mundial de computadores, levando o público participante a compartilhar suas experiências e vivências no dia-a-dia, gerando a participação e a democratização do conhecimento.
Interdisciplinaridade e Interprofissionalidade	As disciplinas envolvidas e que remetem ao estudante a aplicação prática no projeto são: Sistemas Operacionais, Administração de Sistemas de Redes, Segurança em Redes de Computadores. Além das disciplinas, os estudantes envolvidos no projeto são dos cursos de Redes de Computadores e Ensino Médio Informática na Internet.
Indissociabilidade Ensino-Pesquisa-Extensão	O projeto aborda o ensino a partir da prática empregada com base na teoria da sala de aula; a pesquisa leva os estudantes a buscar nos veículos de publicação as ações sobre segurança empregadas nos workshops e a extensão aborda neste momento unidades das OMs e da base aérea, ALA 4.
Impacto na Formação do Estudante	Impacto maior sobre a visão profissional do comportamento organizacional e a postura profissional, que permitiu aos estudantes vivenciarem durante os workshops.
Impacto e Transformação social	Impacto sobre a visão do estudante fora dos muros da universidade e em contrapartida a visão da comunidade sobre o que é trabalhando na universidade, visando a sociedade e adequando as necessidades, trazendo-as para a sala de aula.

Fonte: As autoras.

As diretrizes de extensão podem ser consideradas como um indicador de desempenho do projeto a partir do objetivo geral, aproximar a comunidade acadêmica da comunidade de Santa Maria, oportunizando o estudante a aplicar seus conhecimentos adquiridos em sala. A tabela 1 apresenta essa indicação de forma coerente entre as diretrizes com os resultados alcançados em cada uma.

3.2 Junto A Comunidade

Durante os workshops, os estudantes são responsáveis pela parte prática e confecção dos slides sob orientação da professora coordenadora do projeto, ou seja, após a explanação teórica das principais definições pela coordenadora do projeto, os estudantes aplicavam uma prática. A Figura 3 apresenta a primeira fase da etapa sobre Golpes na Internet abordando as terminologias e definições e a Figura 4 a interação dos estudantes na segunda fase do workshop. Nessa interação os estudantes orientam os participantes do workshop na criptografia de arquivos.

Este workshop foi direcionado ao pessoal técnico das principais organizações militares (OM) de Santa Maria. Foi planejada pelos alunos do 5° período, orientada pela coordenadora do projeto e auxiliada pelos demais estudantes, pois exigia configuração de roteadores e preparação de cada máquina usada pelos participantes do workshop. O ambiente da prática foi preparado previamente para a data de realização do workshop.

Figura 3 – Introdução a Terminologias e Conceitos sobre Golpes na Internet

Fonte: As autoras.

Figura 4 – Interação dos Estudantes com Práticas e Orientações do uso da Internet, dirigindo os Participantes a Execução de Criptografia de Arquivos.

Fonte: As autoras.

Para os estudantes, os encontros realizados oportunizaram a interação com o público externo e o acesso a fatos ocorridos em ambiente de trabalho, o que enriquece a construção de conhecimento e possibilita o emprego do que é abordado em sala de aula, inclusive levando a pesquisas e construção de

novos conhecimentos estimulados pelo compartilhamento de experiências por parte do público alvo, ao longo da execução do projeto.

4 CONCLUSÃO

O projeto trouxe, aos estudantes e aos participantes, uma experiência abundante em troca de vivências e o entendimento das necessidades da comunidade quanto às orientações de boas práticas no uso dos sistemas computacionais pelos usuários. Os estudantes colocaram em prática os conhecimentos adquiridos na teoria, entendendo que a aprendizagem ultrapassa as barreiras da sala de aula, e demonstrando o interesse da universidade pública em buscar a melhoria na qualidade do ensino baseado nas trocas de experiências com a sociedade.

As diretrizes de extensão são somente uma das diversas maneiras de medir a interferência do projeto na sociedade, no momento que a análise das diretrizes traz bons resultados, é notório que ele cumpre suas intenções, principalmente atingindo seu objetivo majoritário de aproximar a comunidade acadêmica da sociedade em geral. A adequação do projeto ao "novo normal" foi estratégica para alcançarmos o objetivo principal. Mantendo os estudantes envolvidos no aprofundamento do conteúdo do projeto e os desafiando a interagir através das redes sociais junto aos demais departamentos da UFSM, fortalecendo-se para se manter ativos diante do cenário que estamos vivenciando.

REFERÊNCIAS

Alcoforado, A., Ribeiro, E. & Cunha, J. (2012, janeiro). Condutas do fator humano: Alicerce da Segurança da Informação. Anais do 15° Encontro Regional De Estudantes De Biblioteconomia, Documentação, Ciência E Gestão Da Informação, Cariri, CE.

De Araújo, W., De Azevedo, P. M., Silva, N. B. X. (2013) Engenharia social nas redes sociais online: um estudo de caso sobre a exposição de informações pessoais e a necessidade de estratégias de segurança da informação. Revista Ibero-americana de Ciência da Informação. vol. 6 (n. 2), p 37-55.

Moreira, E. S. O uso de ataques diretos e pessoais da engenharia social para a obtenção de informações de uma corporação. Revista Inteligência Competitiva (2019)*, v. 9* (n. 1), p. 55-72.

Nagli, L. S. D. (2020, novembro). Pandemia na Pandemia: A Escalada de Ataques Cibernéticos Pós COVID-19. Anais Congresso Transformação Digital 2020, São Paulo, SP.

Universidade Federal de Santa Maria. 2008. Política de Extensão da UFSM. Santa Maria, RS. Recuperado de http://jararaca.ufsm.br/websites/prex/download/Politica/Politica.pdf