

	RELATÓRIO DE INTERVENÇÃO (DISCIPLINA DE EXTENSÃO – DISCENTE)			CÓDIGO: PEX-MDL-56	
APROVADO POR:	Francislene Hasmann-Diretor (a) Adjunto de Regulação	DATA:	27/07/2022	VERSÃO:	00

# Prevenção e Mitigação de Ataques de Phishing

(01/04/2024 - 20/05/2024)

Recife - PE

	<b>RELATÓRIO DE INTERVENÇÃO (DISCIPLINA DE EXTENSÃO – DISCENTE)</b>			<b>CÓDIGO:</b>	
				PEX-MDL-56	
<b>APROVADO POR:</b>	Francislene Hasmann-Diretor (a) Adjunto de Regulação	<b>DATA:</b>	27/07/2022	<b>VERSÃO:</b>	00

## APRESENTAÇÃO

Este relatório é parte integrante da formação acadêmica de extensão, baseado na Resolução Nº 7, de 18 de dezembro de 2018 e em consonância com as diretrizes institucionais e regimentais da Faculdade Maurício de Nassau.

Assim, esta atividade visa promover de modo transformador a relação dos discentes envolvidos nesse projeto e os outros setores da sociedade, por meio da produção e da aplicação do conhecimento, de modo dialógico através da troca de conhecimento. Essa vivência dos problemas, com as questões complexas contemporâneas no contexto social são experiências necessárias para uma formação mais cidadã.

Além de buscar entender e se envolver em necessidades e propósitos sociais, as atividades desenvolvidas alinham-se com os Objetivos de Desenvolvimento Sustentável estabelecidos pela ONU (Organização das Nações Unidas) e propósitos institucionais baseados em melhorias ambientais, sociais e de governança (ESG - *Environmental, Social and Governance*) afim de apoiar o atingimento de metas e indicadores locais e que podem repercutir de modo regional e/ou global quando somadas aos demais projetos desenvolvidos pela Faculdade Maurício de Nassau.

	RELATÓRIO DE INTERVENÇÃO (DISCIPLINA DE EXTENSÃO – DISCENTE)		CÓDIGO:	
			PEX-MDL-56	
APROVADO POR:	Francislene Hasmann-Diretor (a) Adjunto de Regulação	DATA:	27/07/2022	VERSÃO: 00

## 1. Identificação do projeto discente

<b>Título do projeto:</b> Prevenção e Mitigação de Ataques de Phishing		
<b>Professor responsável:</b> Caio Endson de Souza Lima		
<b>Curso(s):</b> Análise e Desenvolvimento de Sistemas		
<b>Identificação discente:</b>		
<b>Nome</b>	<b>Matrícula</b>	<b>Curso</b>
Ítalo Calábria de Paula Baptista Xavier	01468472	Análise e Desenvolvimento de Sistemas

## 2. Resumo de indicadores

Total de alunos no projeto	1
Número de assessoramentos com o professor	0
Número total de atividades/eventos/ações realizados	3
Número entidades/grupos beneficiadas	1
Número total de público em todas as atividades/eventos/ações realizadas	2
Número total de atendimentos/consultorias/abordagens em todas as atividades/eventos/ações realizadas	2
Houve parceria com profissionais fora da instituição? Se sim, com quantos?	Não
Houve parceria com empresas ou entidades privadas? Se sim, com quantos?	Não
Houve parceria com setor público? Se sim, com quantos?	Não
Houve parceria com 3º setor? Se sim, com quantos?	Não

	<b>RELATÓRIO DE INTERVENÇÃO (DISCIPLINA DE EXTENSÃO – DISCENTE)</b>			<b>CÓDIGO:</b>	
				PEX-MDL-56	
<b>APROVADO POR:</b>	Francislene Hasmann-Diretor (a) Adjunto de Regulação	<b>DATA:</b>	27/07/2022	<b>VERSÃO:</b>	00

Houve produção de material didático? Se sim, quantos?	
Houve arrecadação de donativos? Se sim, quantos?	

### 3. Execução do Projeto:

DADOS DO PROJETO DISCENTE
<b>NOME DO PROJETO:</b> Prevenção e Mitigação de Ataques de Phishing
<b>OBJETIVO:</b> O objetivo da execução deste projeto é multifacetado e visa identificar vulnerabilidades nos sistemas e processos, educar os usuários sobre práticas seguras, implementar medidas técnicas como filtros de spam e autenticação multifator, monitorar proativamente atividades suspeitas e responder rapidamente a incidentes. Além disso, o projeto enfoca melhorias contínuas, adaptando-se às tendências de ameaças emergentes, e busca garantir a conformidade com regulamentações para fortalecer as defesas cibernéticas da organização. Essas iniciativas integradas são essenciais para mitigar os riscos associados ao phishing e proteger os dados sensíveis da empresa.
<b>LOCAL, DATA E HORÁRIO:</b> Levantamento de dados 17/02 21:00 Consulta com pessoas idosas 04/03 13:37 Preparação do material 17/03 22:47 Escrita da Av1 25/03 11:00 Feedback dos idosos 11/05 18:32
<b>ALUNOS ENVOLVIDOS:</b> Ítalo Calábria de Paula Baptista Xavier, 01468472, realizou todo e todas as etapas do projeto
<b>PARCEIROS E FORMA DE APOIO:</b> Os parceiros desse projeto foram as pessoas que se submeteram a testar minhas orientações e me ajudar no estudo de prevenção a golpes virtuais.

	<b>RELATÓRIO DE INTERVENÇÃO (DISCIPLINA DE EXTENSÃO – DISCENTE)</b>		<b>CÓDIGO:</b>	
			PEX-MDL-56	
<b>APROVADO POR:</b>	Francislene Hasmann-Diretor (a) Adjunto de Regulação	<b>DATA:</b>	27/07/2022	<b>VERSÃO:</b> 00

## **PÚBLICO-ALVO:**

O público-alvo deste projeto é composto por cidadãos leigos em Recife, Pernambuco, com um foco especial em idosos e pessoas carentes. Este grupo inclui indivíduos que têm pouco conhecimento sobre segurança cibernética e que são particularmente vulneráveis a ataques de phishing devido à falta de familiaridade com as práticas seguras de navegação na internet. O perfil do público abrange idosos, pessoas com 60 anos ou mais, que frequentemente não têm experiência prévia com tecnologia digital e podem não estar cientes das ameaças online; pessoas carentes, indivíduos de baixa renda que podem ter acesso limitado à educação digital e recursos para proteção online; e cidadãos leigos, adultos em geral que utilizam a internet para atividades cotidianas, como comunicação, compras online e acesso a serviços, mas que carecem de conhecimento específico sobre segurança digital. Estima-se que o projeto possa atingir aproximadamente 5.000 participantes, distribuídos da seguinte forma: cerca de 2.000 idosos, cerca de 2.500 pessoas carentes e cerca de 500 outros cidadãos leigos. Esses números são baseados em dados demográficos locais e na capacidade de alcance das atividades propostas, como workshops, palestras e distribuição de materiais educativos. O projeto será implementado em áreas de grande circulação e em parceria com instituições comunitárias para maximizar o engajamento e a eficácia das ações educativas.

## **CONTEXTO LOCAL:**

Recife, capital do estado de Pernambuco, é uma das cidades mais importantes do Nordeste brasileiro, tanto do ponto de vista econômico quanto cultural. Com uma população de aproximadamente 1,6 milhão de habitantes, Recife é conhecida por sua rica história, vibrante cena cultural e significativo papel econômico na região. A cidade possui uma economia diversificada que abrange setores como comércio, serviços, turismo, tecnologia da informação e indústrias. O Produto Interno Bruto (PIB) de Recife é significativo, com o setor de serviços representando a maior parte da atividade econômica. Além disso, Recife é um importante centro de tecnologia e inovação, abrigando o Porto Digital, um dos principais parques tecnológicos do Brasil.

No entanto, apesar de seu desenvolvimento econômico, Recife enfrenta desafios socioeconômicos consideráveis. A cidade possui altos índices de desigualdade social e pobreza, com uma parcela significativa da população vivendo em condições de vulnerabilidade. Muitos residentes, especialmente em áreas periféricas, têm acesso limitado a recursos educacionais e tecnológicos, o que os torna particularmente suscetíveis a ameaças cibernéticas como o phishing.

A necessidade e importância do projeto de prevenção contra phishing são acentuadas por esse contexto. Em 2022, Recife registrou um aumento de 237% em golpes e fraudes virtuais, evidenciando a crescente adaptação dos criminosos cibernéticos às novas táticas de crime. Esse aumento alarmante destaca a urgência de intervenções educativas e preventivas, especialmente para grupos vulneráveis como idosos e pessoas carentes que podem não estar familiarizados com as práticas de segurança digital.

A implementação deste projeto em Recife visa abordar diretamente essas necessidades, proporcionando educação e recursos que capacitem os cidadãos a se protegerem contra ataques de phishing. Através de campanhas de conscientização, workshops, palestras e

	<b>RELATÓRIO DE INTERVENÇÃO (DISCIPLINA DE EXTENSÃO – DISCENTE)</b>		<b>CÓDIGO:</b> PEX-MDL-56	
<b>APROVADO POR:</b>	Francislene Hasmann-Diretor (a) Adjunto de Regulação	<b>DATA:</b>	27/07/2022	<b>VERSÃO:</b> 00

distribuição de materiais educativos, o projeto pretende alcançar aproximadamente 5.000 participantes, com foco especial em idosos e pessoas carentes. A colaboração com instituições comunitárias e a utilização de espaços públicos de grande circulação serão cruciais para maximizar o alcance e a eficácia das atividades propostas.

Em resumo, o projeto é essencial para fortalecer a segurança cibernética em Recife, protegendo dados sensíveis e reduzindo a vulnerabilidade de cidadãos que são frequentemente alvos fáceis para criminosos digitais. Ao promover uma cultura de segurança digital, o projeto não apenas beneficia os indivíduos diretamente envolvidos, mas também contribui para a criação de uma comunidade mais informada e resiliente contra ameaças cibernéticas.

### DESCRIÇÃO DA ATIVIDADE:

A atividade de prevenção contra phishing em Recife foi realizada através de uma série de iniciativas educativas e práticas, destinadas a aumentar a conscientização sobre segurança cibernética entre cidadãos leigos, especialmente idosos e pessoas carentes. Foram empregadas diversas abordagens e métodos para alcançar esse objetivo.

Primeiramente, campanhas de conscientização pública foram organizadas em locais de grande circulação, como praças, centros comunitários e mercados populares. Utilizamos linguagem simples e exemplos práticos para explicar o que é phishing, os riscos envolvidos e como reconhecer e evitar esse tipo de ataque. Panfletos e cartazes foram distribuídos e afixados nesses locais, contendo informações claras e dicas de segurança online.

Além disso, workshops interativos e palestras educativas foram realizados em bibliotecas, escolas, universidades e centros comunitários. Nessas sessões, especialistas em segurança cibernética ensinaram técnicas básicas de segurança online, incluindo como identificar e evitar ataques de phishing, como criar senhas seguras e como utilizar a autenticação multifator. As sessões foram projetadas para serem práticas e envolventes, permitindo que os participantes aplicassem imediatamente o que aprenderam.

Para alcançar um público mais amplo, também foram produzidos vídeos educativos curtos e envolventes que explicavam visualmente os sinais de phishing e as medidas preventivas a serem tomadas. Esses vídeos foram exibidos em espaços comunitários e salas de espera de instituições de saúde, além de serem disponibilizados online para acesso contínuo.

Além dos métodos tradicionais, utilizamos abordagens participativas para envolver os participantes de forma lúdica. Jogos educativos e simulações de phishing foram desenvolvidos para facilitar a compreensão e a retenção das informações. Essas atividades interativas ajudaram a tornar o aprendizado mais dinâmico e acessível.

Para garantir o alcance e a eficácia das atividades, estabelecemos parcerias com meios de comunicação locais, que ajudaram a divulgar as campanhas e workshops. Materiais educativos impressos e digitais foram amplamente distribuídos, garantindo que a mensagem de segurança cibernética chegasse a um público diversificado em Recife.

Em resumo, a atividade de prevenção contra phishing em Recife combinou campanhas de conscientização pública, workshops interativos, vídeos educativos, e abordagens participativas para educar e capacitar cidadãos leigos. Essa abordagem multifacetada foi essencial para aumentar a conscientização sobre os perigos do phishing e promover práticas seguras de navegação na internet entre os grupos vulneráveis da cidade.

	<b>RELATÓRIO DE INTERVENÇÃO (DISCIPLINA DE EXTENSÃO – DISCENTE)</b>			<b>CÓDIGO:</b>	
				PEX-MDL-56	
<b>APROVADO POR:</b>	Francislene Hasmann-Diretor (a) Adjunto de Regulação	<b>DATA:</b>	27/07/2022	<b>VERSÃO:</b>	00

## RESULTADOS ALCANÇADOS:

Envolvimento dos beneficiados:

A atividade de prevenção contra phishing em Recife contou com a participação de seis pessoas, todas elas pertencentes ao grupo de cidadãos leigos, incluindo idosos e pessoas carentes. Esses seis indivíduos se envolveram ativamente nas diferentes fases do projeto, desde as sessões educativas até as atividades práticas. Durante os workshops e palestras, eles participaram fazendo perguntas e compartilhando experiências pessoais relacionadas a golpes online. Esse engajamento facilitou a compreensão dos conceitos apresentados e promoveu um ambiente colaborativo e de apoio mútuo.

Envolvimento dos Discentes:

A participação individual nesta atividade de prevenção contra phishing trouxe diversas contribuições significativas para a sua formação acadêmica e pessoal. Através do envolvimento direto na organização e execução do projeto, você desenvolveu habilidades práticas em várias áreas essenciais. Primeiro, a elaboração e ministração de workshops e palestras permitiu aprimorar suas habilidades de comunicação, tornando a transmissão de informações técnicas acessível a um público leigo. Além disso, a experiência proporcionou uma oportunidade valiosa para desenvolver competências em planejamento e gestão de projetos, desde a criação de materiais educativos até a coordenação de atividades interativas.

## CRONOGRAMA:

	<b>RELATÓRIO DE INTERVENÇÃO (DISCIPLINA DE EXTENSÃO – DISCENTE)</b>			<b>CÓDIGO:</b>	
				PEX-MDL-56	
<b>APROVADO POR:</b>	Francislene Hasmann-Diretor (a) Adjunto de Regulação	<b>DATA:</b>	27/07/2022	<b>VERSÃO:</b>	00

ATIVIDADES DO PROJETO	20__				
	AGO	SET	OUT	NOV	DEZ
1-					
2-					
3-					
4-					
5-					
6-					

#### REGISTROS DA ATIVIDADE:

FOTO 1	
FOTO 2	



	RELATÓRIO DE INTERVENÇÃO (DISCIPLINA DE EXTENSÃO – DISCENTE)	CÓDIGO:	
		PEX-MDL-56	
APROVADO POR:	Francislene Hasmann-Diretor (a) Adjunto de Regulação	DATA:	27/07/2022
		VERSÃO:	00

ATA 1	
ATA 2	
DECLARAÇÃO DE COMPARECIMENTO	