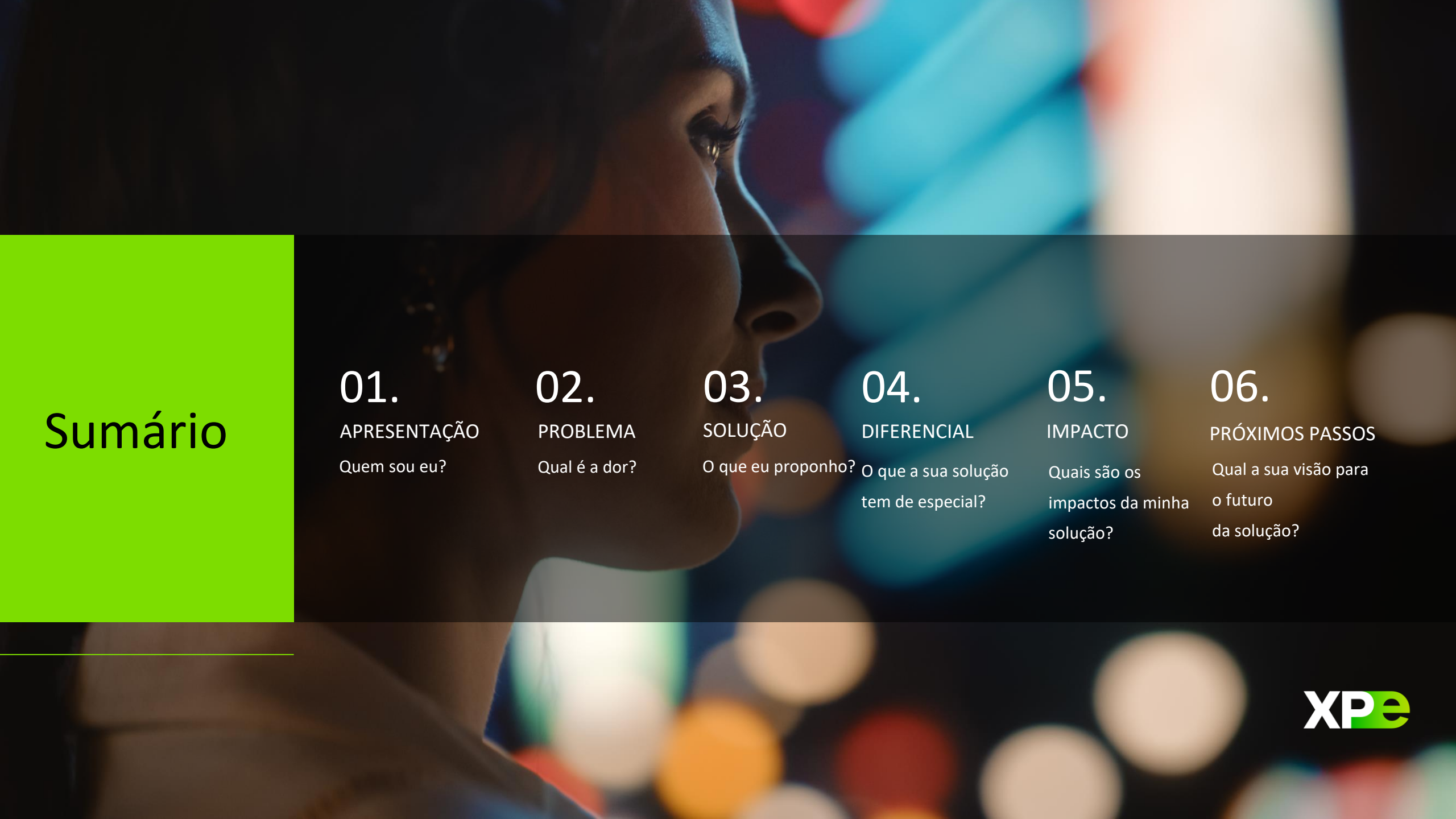
Pitch

PROJETO APLICADO | PÓS-GRADUAÇÃO

Defesa Cibernética contra IA Generativa em Ambientes Bancários



Sumário

01. APRESENTAÇÃO
Quem sou eu?

02. PROBLEMA
Qual é a dor?

03. SOLUÇÃO
O que eu proponho?

04. DIFERENCIAL
O que a sua solução tem de especial?

05. IMPACTO
Quais são os impactos da minha solução?

06. PRÓXIMOS PASSOS
Qual a sua visão para o futuro da solução?

02.
Problema

Qual é a dor?

Aumento dos Ataques de Engenharia Social: O setor bancário enfrenta um número crescente de ataques de engenharia social, como phishing, clonagem de voz e mensagens fraudulentas em aplicativos de mensagens. Criminosos cibernéticos estão utilizando IA generativa para criar ataques altamente personalizados, tornando-os mais difíceis de detectar.

Vazamentos de Dados: Criminosos obtêm dados pessoais de clientes de diversas fontes com diferentes níveis de segurança, como órgãos governamentais, pequenas empresas, lojas de varejo, farmácias e postos de gasolina. Essas entidades, muitas vezes, não possuem sistemas de segurança robustos, tornando-se alvos fáceis para vazamentos ou roubo de informações.

IA Generativa: A IA generativa permite a criação de mensagens fraudulentas extremamente convincentes, explorando a confiança e o desconhecimento dos clientes. Ataques personalizados, utilizando dados pessoais obtidos de forma ilícita, são mais eficazes e difíceis de identificar.

Baixa Conscientização: Clientes e funcionários, muitas vezes, não estão cientes das novas técnicas de fraude, tornando-se vulneráveis a ataques. Campanhas de conscientização tradicionais, com abordagens genéricas, não são mais eficazes para treinar os usuários a detectar ataques avançados.

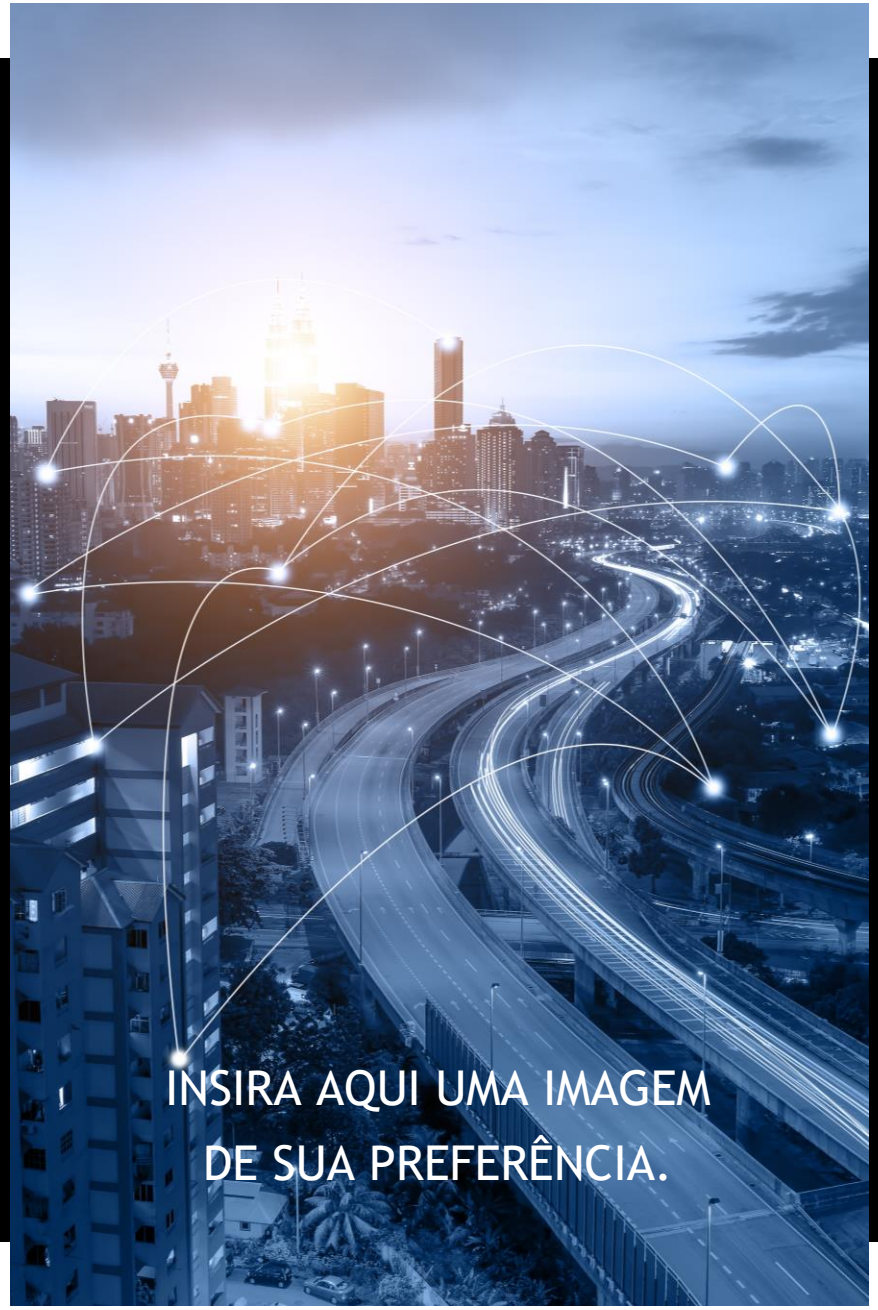
03.

Solução

O que eu proponho?

Um sistema de defesa cibernética que combina:

- **Conscientização e Treinamento:** Para clientes e funcionários, incluindo simulações práticas.
- **Uso de IA Generativa:** Para criar exemplos realistas de phishing e treinar reconhecimento de ataques.
- **Framework POEMS:** Análise do ambiente bancário considerando aspectos de pessoas, objetos, ambiente, mensagens e serviços.



04.

Diferencial

O que a sua solução tem de especial?

Abordagem proativa e centrada no usuário: O projeto se concentra em capacitar clientes e funcionários, tornando-os a primeira linha de defesa. A educação e conscientização são ferramentas proativas que permitem aos usuários se protegerem de forma independente.

Combinação de Tecnologia e Educação: A solução integra ferramentas de detecção automatizada com campanhas de conscientização. Essa abordagem multifacetada garante uma proteção mais abrangente contra fraudes.

Foco em Ameaças Emergentes: O projeto aborda as ameaças mais recentes, utilizando IA generativa. Através da simulação de ataques personalizados, os usuários são preparados para as táticas mais sofisticadas.

05.

Impacto

Como funciona o seu produto?

Conscientização 1

Campanhas educacionais abrangentes, utilizando diversos canais de comunicação, como e-mail, SMS, notificações em aplicativos, página web e redes sociais.

Treinamento 2

Simulações de ataques de phishing personalizados para demonstrar as técnicas dos criminosos e como identificá-las.

Detecção 3

Implementação de ferramentas automatizadas para identificar e bloquear atividades suspeitas em tempo real. O banco disponibiliza um canal dedicado para que os clientes possam verificar se uma comunicação é fraudulenta, além de detectar automaticamente possíveis fraudes.

06.

Próximos Passos

Qual a sua visão para o futuro da solução?

A solução proposta se expande além do uso imediato e visa uma abordagem de longo prazo para a conscientização e proteção contra fraudes cibernéticas. O objetivo é criar uma cultura de segurança dentro das instituições financeiras, onde clientes e funcionários estejam constantemente atualizados sobre as últimas ameaças digitais. A visão para o futuro inclui a continuidade e ampliação das campanhas de conscientização, adaptando-as a novos desafios tecnológicos e integrando feedback contínuo para refinar as estratégias. A expansão dessa iniciativa também busca estabelecer parcerias com outras instituições financeiras e órgãos reguladores, colaborando para construir um setor financeiro mais seguro e resiliente.

1

Continuidade das Campanhas

Ampliação do alcance das campanhas educacionais.

2

Feedback Contínuo

Coleta de feedback de clientes e colaboradores para aprimorar os materiais educativos.

3

Parcerias Estratégicas

Colaboração com órgãos reguladores e outros bancos para fortalecer a segurança do setor financeiro.


Obrigado!