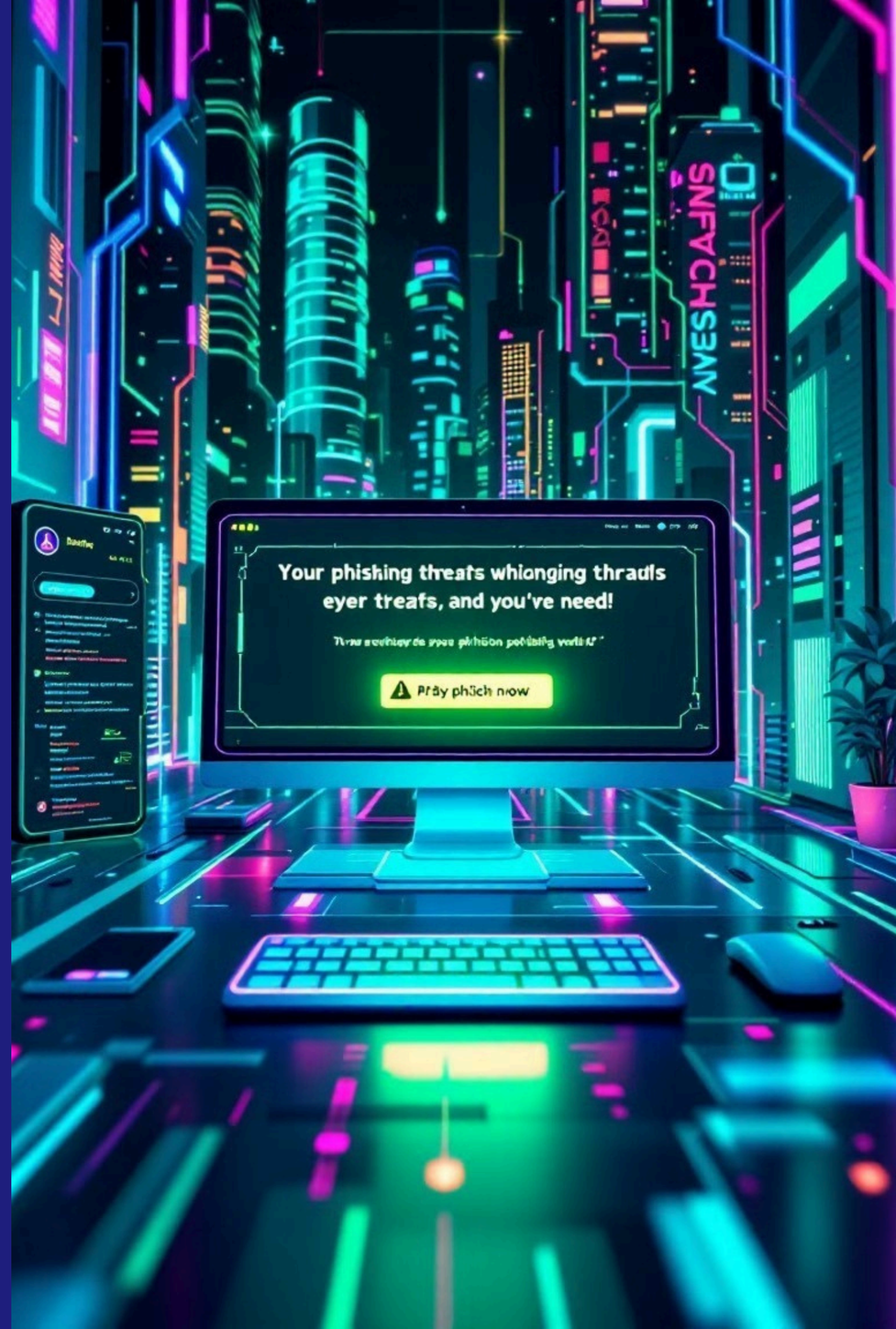
COTIC

A Coordenação de Tecnologia da Informação e Conectividade (COTIC) da FUNARTE apresenta uma nova fase da campanha de conscientização sobre segurança digital e privacidade, direcionada a todos(as) os(as) servidores(as) e colaboradores(as). Um dos primeiros temas abordados será o Phishing, uma ameaça cibernética comum que exige atenção e cuidado.

Phishing: Ameaça Digital em Evolução

Nos últimos anos, o phishing se tornou uma das maiores ameaças cibernéticas, evoluindo constantemente para enganar usuários e roubar dados valiosos. No Brasil, o cenário ainda é preocupante com o crescimento exponencial de ataques. Essa apresentação analisa o phishing, suas características, métodos e tendências, além de oferecer dicas para prevenção e segurança.



O que é Phishing?

Definição

O phishing é uma técnica fraudulenta usada por criminosos para roubar dados sensíveis, como senhas, números de cartão de crédito e informações pessoais. Eles se disfarçam como entidades confiáveis, como bancos, empresas ou órgãos governamentais, para enganar as vítimas.

Características

Inteligência Artificial

A IA permite que os criminosos personalizem os ataques de phishing, adaptando as mensagens e o conteúdo para cada vítima, aumentando a eficácia da fraude.

Deepfakes

O vishing (phishing por telefone) utiliza deepfakes para criar chamadas de vídeo realistas com a imagem de pessoas conhecidas, enganando as vítimas e roubando suas credenciais.

QR Codes Maliciosos

O quishing envolve a utilização de QR Codes falsos que direcionam as vítimas para sites maliciosos, onde seus dados são roubados.

SMS Fraudulentos

O smishing utiliza mensagens SMS falsas para enganar as vítimas e obter informações confidenciais, como senhas de bancos ou números de cartão de crédito.

Métodos de Ataque Mais Comuns

E-mails Fraudulentos

E-mails com links falsos para **sites clonados**, **mensagens de alerta falsas ou promoções irresistíveis**, com o objetivo de roubar credenciais ou dados bancários.

Links Maliciosos

Links enviados via **WhatsApp** que levam para páginas falsas ou download de arquivos infectados, como vírus ou ransomware, que podem roubar dados ou sequestrar dispositivos.

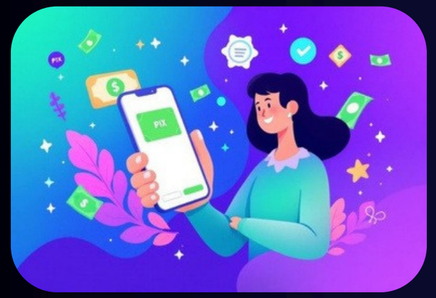
Sites Falsos

Sites de **e-commerce** falsos, que imitam a aparência de **lojas online** conhecidas, para coletar dados de pagamento e roubar dinheiro das vítimas.

Aplicativos Clonados

Aplicativos **bancários** falsos, que se parecem com os originais, para roubar dados de acesso e realizar transações fraudulentas.

Casos comuns no Brasil



Golpe Pix

Criminosos exploram a popularidade do Pix para enganar pessoas com mensagens falsas, solicitando transferências de dinheiro para contas falsas, resultando em milhões de reais em prejuízo para os usuários.

Vazamento de Dados

A segurança da informação depende de boas práticas por parte das empresas, órgãos governamentais, servidores e colaboradores. O uso inadequado ou negligente de dados pode contribuir para exposições indevidas, incluindo informações sensíveis como CPF, RG, endereços e dados bancários. Essas situações podem facilitar fraudes e outros riscos, tornando essencial a adoção de medidas rigorosas para a proteção das informações.

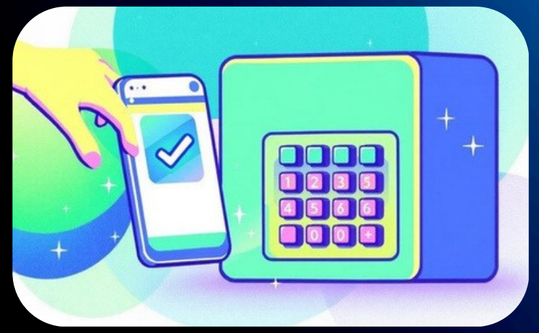
Black Friday

Ataques de phishing se intensificam durante a Black Friday, aproveitando o aumento das compras online para enganar consumidores e roubar dados de pagamento.

Clonagem de WhatsApp

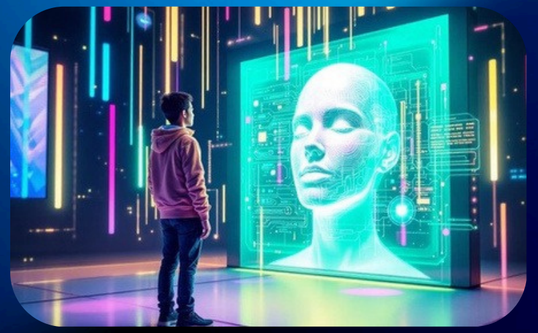
Criminosos utilizam técnicas de phishing para clonar contas de WhatsApp, obtendo acesso às conversas e contatos das vítimas, e usando essa informação para cometer fraudes e extorsões.

Tecnologias Anti-Phishing



Autenticação de Dois Fatores (2FA)

Adiciona uma camada extra de segurança, exigindo um código de verificação enviado por SMS ou aplicativo, além da senha tradicional, para acessar contas online.



Verificação Biométrica

Utiliza reconhecimento facial, digital ou de íris para autenticar a identidade do usuário, dificultando a invasão de contas por criminosos.

Blockchain

Tecnologia de registro descentralizado que garante a segurança e a integridade de transações online, dificultando fraudes e roubos de dados.

Machine Learning

Algoritmos de aprendizado de máquina são utilizados para identificar padrões suspeitos em transações online, detectando fraudes e bloqueando ataques de phishing.

Prevenção e Boas Práticas

1

Verificar URLs e Certificados

Verifique cuidadosamente URLs e certificados digitais antes de inserir dados sensíveis em sites ou aplicativos.

2

Evitar Links Suspeitos

Nunca clique em links suspeitos em emails, mensagens SMS ou redes sociais, principalmente se forem de remetentes desconhecidos ou que solicitarem informações pessoais.

3

Manter Softwares Atualizados

Mantenha seus softwares e aplicativos atualizados, pois as atualizações incluem correções de segurança que podem proteger contra ataques de phishing.

4

Usar Gerenciadores de Senhas

Utilize gerenciadores de senhas para armazenar suas senhas de forma segura e evitar o uso da mesma senha em diferentes plataformas.

5

Monitorar Contas Online

Monitore suas contas online regularmente, verificando se houve alguma atividade suspeita ou tentativa de acesso não autorizado.

Tendências e Perspectivas para o ano de 2025

200%
Metaverso

Os ataques de phishing migrarão para o metaverso, explorando novas formas de enganar usuários em ambientes virtuais.

150%
Ataques Mobile

Os ataques de phishing em dispositivos móveis aumentarão, aproveitando a crescente popularidade de smartphones e tablets.

US$12B
Prejuízo Global

As perdas globais com phishing são projetadas para alcançar US$ 12 bilhões em 2025, demonstrando a crescente ameaça cibernética.

Alerta Contínuo: Proteja-se Contra o Phishing

Em conclusão, o phishing permanece uma ameaça cibernética persistente e sofisticada. Ao longo desta apresentação, exploramos suas características, métodos de ataque, casos notáveis e tecnologias anti-phishing.

É crucial que todos, desde usuários individuais até administradores de servidores, permaneçam vigilantes e proativos. Adote as boas práticas de prevenção, verifique URLs, evite links suspeitos, mantenha softwares atualizados e monitore contas online regularmente.

A segurança cibernética é uma responsabilidade compartilhada. Ao nos mantermos informados e implementarmos medidas de proteção robustas, podemos mitigar os riscos e proteger nossos dados e sistemas contra ataques de phishing.