SISTEMAS OPERACIONAIS 1º PERÍODO
PROFESSOR: CARLOS MAGNO

PHISHING

EXPLORANDO O MUNDO DO PHISHING: COMO PROTEGER-SE CONTRA ATAQUES CIBERNÉTICOS

INTRODUÇÃO

É um prazer estar aqui hoje para discutirmos um assunto extremamente relevante no mundo digital: a segurança cibernética. Nos últimos anos, presenciamos um aumento significativo nos ataques cibernéticos, e um dos métodos mais comuns e perigosos utilizados pelos cibercriminosos é o phishing.

Phishing é uma técnica que visa enganar as pessoas, fazendo-as acreditar que estão interagindo com instituições confiáveis ou conhecidas, quando, na verdade, estão sendo direcionadas para sites falsos ou sendo manipuladas a fornecer informações pessoais e confidenciais. Hoje, vamos explorar esse mundo do phishing, entender como ele funciona e, o mais importante, aprender como nos protegermos contra esses ataques.

Nosso objetivo é garantir que todos vocês saiam desta apresentação com conhecimentos práticos que poderão ser aplicados imediatamente em sua vida digital. Então, vamos mergulhar nesse assunto fascinante e fundamental para a nossa segurança online.

Mas antes de irmos adiante, quero fazer uma pergunta: quantos de vocês já ouviram falar sobre phishing? Se você está familiarizado com o termo, ótimo! Você está um passo à frente. Se não, não se preocupe, estamos aqui para lhe fornecer todas as informações necessárias.

Durante esta apresentação, exploraremos os diferentes tipos de ataques de phishing, os sinais de alerta para identificar um ataque em potencial e forneceremos dicas práticas para se proteger contra essas ameaças. Afinal, a melhor defesa é o conhecimento!

Então, sem mais delongas, vamos começar essa jornada de descoberta sobre o mundo do phishing e como nos protegermos contra ele. Estão todos prontos? Ótimo! Vamos lá!

Qual a origem desse termo ?

A palavra "phishing", derivada do inglês "fishing" (pesca), é uma analogia criada pelos golpistas para descrever sua tática de "pescar" informações de usuários usando "iscas" na forma de mensagens eletrônicas.

Quais são os métodos utilizados pelos golpistas ?

Os golpistas geralmente se passam por entidades confiáveis, como bancos, empresas, redes sociais, instituições governamentais e outros serviços populares na Internet.

Sites fraudulentos

A isca mais comum que os golpistas utilizam para pescar dados pessoais são os falsos sites. Um site de phishing é criado para se assemelhar a um site legítimo, como de uma instituição ou empresa conhecida, o objetivo é enganar o usuário se passando por uma fonte confiável quando na verdade estão acessando uma página golpista.

Mensagens de phishing

Uma das ferramentas mais utilizadas pelos golpistas são as mensagens de texto, os criminosos cibernéticos normalmente fingem ser empresas confiáveis, amigos ou pessoas conhecidas em uma mensagem falsa, que contém um link para um site fraudulento. Essas mensagens são encaminhadas através de e-mails, sms, redes sociais etc. Como você pode se proteger dessas falsas informações ?

1. **Se atente ao tom da mensagem:** muitos dos golpistas exploram os sentimentos das pessoas, como medo, obediência, caridade, carência afetiva e ganância, com o objetivo de persuadi-las a agir de acordo com seus desejos, de forma impulsiva e rápida.
2. **Busque informações:** se após analisar o tom da mensagem que você recebeu sobraram dúvidas sobre o ocorrido, não se esqueça de buscar informações, pesquise relatos sobre golpes semelhantes, entre em contato com amigos e familiares e fale sobre o assunto.

3. **O conteúdo faz sentido?** Muitos golpistas enviam as mesmas mensagens para pessoas diferentes, questionar se o conteúdo faz sentido para você ajuda a não cair em golpes. Pergunte-se, por exemplo:
    - tenho conta neste banco?
    - Tenho algum relacionamento ou contato com a empresa/instituição que está solicitando informações?
    - O texto contém erros de ortografia, gramática ou frases estranhas que seriam suspeitas vindo de uma instituição confiável?
4. **Suspeite de mensagens com temas cotidianos:** para atrair os usuários, os golpistas costumam usar assuntos do dia a dia para coletar dados e informações relevantes. Suspeite das seguintes solicitações: recadastramento de token, cancelamento de CPF, débitos pendentes, oferta de emprego, pontos ou bônus a vencer etc. Na dúvida entre em contato com a instituição usando um canal oficial.
5. **Se atente aos golpes do momento:** para atrair vítimas os golpistas usam o que está sendo mais comentado no momento, como eventos, promoções, ocasiões que geram comoção (ex: desastres naturais), prazo para declarar imposto de renda etc. Sendo assim, suspeite de mensagens que possuem ofertas que estão muito abaixo do valor de mercado e se atente ao fazer doações e pagamentos.

Operações bancárias e compras online

Fraudadores utilizam de vários métodos para desviar transações financeiras. Se atente às orientações a seguir.

1. **Confirme a identidade:** muitas vezes os golpistas se passam por amigos ou familiares pedindo ajuda financeira geralmente com urgência. Desconfie desse tipo de mensagem, entre em contato com a pessoa por outro meio de comunicação e informe o ocorrido ao real dono da conta.
2. **O site/loja é confiável ?** Ao efetuar uma compra online pesquise se aquele site é confiável, procure saber a reputação da empresa e as opiniões de quem já comprou, faça uma pesquisa de mercado e verifique se o preço está muito abaixo.
3. **Faça pagamentos apenas na plataforma original da compra:** golpistas alegam falhas no sistema e pedem à vítima para fazer transações fora da plataforma de compra. No pagamento externo o fraudador altera o valor de compra e o oculta para cobrar mais do usuário, muitas vezes o cartão também é clonado.

Proteção tecnológica

É importante usar medidas de proteção tecnológica para ajudar a prevenir ataques de phishing. Isso inclui o uso de software antivírus e antimalware atualizados, filtros de spam e firewalls, que podem ajudar a identificar e bloquear mensagens de phishing.

Impactos causados pelo 333

Quando alguém cai em um ataque de phishing, pode haver diversos impactos negativos, como por exemplo:

1. **Perda financeira:**

   Se um usuário fornecer informações financeiras, como detalhes de cartão de crédito, a um atacante em um ataque de phishing, os invasores podem usar essas informações para realizar transações fraudulentas e/ou roubar dinheiro diretamente das contas bancárias das vítimas, causando perda financeira significativa.]

2. **Roubo de identidade:**

   Ao obter informações sensíveis, como CPF/ RG, data de nascimento e endereço, os invasores podem roubar a identidade da vítima. Isso pode levar a problemas sérios, como abertura de contas em nome da vítima, solicitação de empréstimos e até mesmo envolvimento em atividades criminosas.

3. **Perda do acesso a fotos, vídeos, arquivos, e-mail e outros documentos importantes:**

   Quando alguém cai em um ataque de phishing, isso pode comprometer a segurança não apenas da própria vítima, mas também de outras pessoas ou organizações. Se as contas de e-mail ou redes sociais de uma vítima forem comprometidas por meio de phishing, os invasores podem enviar mensagens ou postagens fraudulentas em nome da vítima. Isso pode levar a danos à reputação pessoal ou profissional da vítima, bem como a problemas de confiança com amigos, familiares e colegas.

O que fazer se você for vítima

Depois de enviar suas informações a um invasor, elas provavelmente serão divulgadas a outros golpistas. Você provavelmente receberá mensagens de vishing e smishing, novos e-mails de phishing e chamadas de voz. Fique sempre alerta para mensagens suspeitas solicitando suas

informações ou detalhes financeiros, neste caso é importante agir rapidamente para minimizar os danos, como por exemplo:

-Notificar a empresa ou organização afetada;

-Alterar suas senhas;

-Verifique suas contas bancárias, e-mails e redes sociais;

-Execute uma varredura antivírus;