**CENTRO PAULA SOUZA**

**ETEC PROFESSOR CAMARGO ARANHA**

**DESENVOLVIMENTO DE SISTEMAS**

**ISAAC YAN DE MELO MARTINS ARAUJO**

**SÃO PAULO**

**2025**

* **GOLPES NA INTERNET**

Golpes na internet estão cada vez mais sofisticados, colocando em risco a segurança dos usuários. Apresento três golpes online e um caso real relacionado a um.

**1. Phishing.**

O phishing é uma técnica em que criminosos se passam por entidades confiáveis para induzir as vítimas a fornecer informações pessoais e financeiras. Isso é feito por e-mails, mensagens ou sites falsos que imitam páginas legítimas. Por exemplo, um e-mail do seu banco solicitando atualização de dados ou confirmação de transações.

**2. Golpe da falta de suporte técnico.**

Os criminosos se apresentam como representantes de empresas de tecnologia ou provedores de serviços de internet, alegando que o computador da vítima está infectado ou com problemas. Eles pedem acesso remoto para "corrigir" o problema, mas roubam informações pessoais ou instalam malware.

**3. Golpe do Dinheiro Esquecido**

Recentemente, houve um aumento de anúncios fraudulentos nas redes sociais que utilizam vídeos manipulados de figuras públicas, como políticos, para promover links falsos prometendo resgate de valores esquecidos em contas bancárias. Esses anúncios instruem os usuários a acessar sites falsos e seguir orientações de atendentes virtuais, afirmando erroneamente que "hoje" seria o último dia para o resgate. Esses vídeos não têm qualquer relação original com dinheiro esquecido, e a restituição legítima ocorre apenas pelo Sistema Valores a Receber do Banco Central, que não cobra pelas transações.

**Caso Real: Golpe do Dinheiro Esquecido com Vídeos Manipulados**

Em outubro de 2024, foram identificados anúncios fraudulentos no Facebook que utilizavam vídeos manipulados com inteligência artificial de figuras públicas, como Jair Bolsonaro, Fernando Haddad e Nikolas Ferreira, para promover links falsos prometendo resgate de valores esquecidos em contas bancárias. Esses vídeos instruíam os usuários a acessar sites e seguir orientações de uma atendente virtual, afirmando erroneamente que "hoje" seria o último dia para o resgate. Esses vídeos não tinham qualquer relação original com dinheiro esquecido, e a restituição legítima ocorre apenas pelo Sistema Valores a Receber do Banco Central, que não cobra pelas transações.

* **ATAQUES CIBERNÉTICOS**

Ataques cibernéticos são ações maliciosas que comprometem sistemas, redes ou dados para roubar informações, extorsão ou interrupção de serviços. Apresentarei dois tipos comuns de ataques cibernéticos, com exemplos reais, datas, empresas envolvidas, valores de prejuízo e ferramentas utilizadas.

**1. Ransomware (Vírus de Sequestro de Arquivos)**

O ransomware é um tipo de vírus que, quando entra no seu computador ou na empresa, "tranca" seus arquivos e só vai liberar de novo se você pagar um valor (resgate). É tipo um sequestrador, mas em vez de gente, ele sequestra seus dados.

*Exemplo Real: Ataque à CNA Financial (Março de 2021)*

Em 2021, a empresa CNA Financial, que trabalha com seguros, foi atacada por hackers. Eles usaram esse tipo de vírus, o ransomware, para trancar os arquivos da empresa. Eles pediram dinheiro para liberar tudo. O valor que eles pediram não foi divulgado, mas o prejuízo da empresa foi enorme porque teve que gastar muito para recuperar tudo.

**2. Engenharia Social (Golpes Psicológicos para Roubo de Dados)**

A engenharia social é quando os hackers tentam enganar as pessoas para roubar informações. Em vez de invadir o computador diretamente, eles manipulam a vítima para que ela acabe entregando senhas ou dados importantes.

*Exemplo Real: Ataque à Sony Pictures (Novembro de 2014)*

Em 2014, a Sony Pictures foi hackeada e teve seus dados vazados. Os hackers conseguiram pegar informações como filmes antes de serem lançados e e-mails privados. O que aconteceu foi que eles enganaram os funcionários, fazendo com que eles entregassem informações. O prejuízo foi gigantesco, estimado em 15 milhões de dólares, sem contar o impacto na imagem da empresa.

No fim das contas, esses ataques cibernéticos são um grande alerta para todos nós. Com o avanço da tecnologia, os hackers estão ficando cada vez mais criativos e conseguem enganar até as pessoas mais atentas. Por isso, é essencial ficar de olho nas mensagens que recebemos, não clicar em links suspeitos e sempre usar ferramentas de segurança, como antivírus. Além disso, nunca compartilhe informações pessoais sem ter certeza de quem está pedindo. A internet pode ser muito útil, mas também é um lugar onde precisamos estar atentos para não cair em golpes e proteger nossos dados.

**BIBLIOGRAFIA**

<https://www.kaspersky.com.br/resource-center/threats/top-scams-how-to-avoid-becoming-a-victim>

[**https://www.oi.com.br/blog/internet/principais-golpes-digitais-e-como-se-proteger-na-internet**](https://www.oi.com.br/blog/internet/principais-golpes-digitais-e-como-se-proteger-na-internet)

<https://www.reuters.com/fact-check/portugues/FOGJ4OL2UZM6NCROGUM6JYUW6Q-2024-10-23>

<https://algardata.com/blog/ciberseguranca/7-maiores-ciberataques-de-2021-ate-ao-momento>

<https://canaltech.com.br/seguranca/os-6-maiores-ataques-ciberneticos-da-historia-213069>