**ETEC PROF. CAMARGO ARANHA**

**DESENVOLVIMENTO DE SISTEMAS**

**3 SEMESTRE**

**ATIVIDADE 19.02:**

**GOLPES E ATAQUES NA INTERNET**

**MARIANNE OLIVEIRA RODRIGUES**

São Paulo

2025

# **INTRODUÇÃO**

Com o avanço da digitalização e o crescente uso da internet para transações financeiras e comunicação, surgem também novas formas de golpes e ataques cibernéticos. Golpes como o do Pix por engano, o falso boleto e o pharming são exemplos claros dessa crescente ameaça. Esses golpes têm se tornado cada vez mais sofisticados, atingindo vítimas de diferentes perfis e setores da sociedade, causando prejuízos financeiros e emocionais. Além disso, os ataques cibernéticos, como os DoS/DDoS, phishing e malware, também representam um risco significativo, com impactos consideráveis em empresas e usuários. A combinação de vulnerabilidades tecnológicas e a manipulação psicológica dos indivíduos tornam esses golpes ainda mais perigosos. Compreender essas ameaças e as ferramentas utilizadas pelos criminosos é essencial para se proteger nesse ambiente digital.

**SUMÁRIO**

[INTRODUÇÃO 1](#_Toc422951694)

[Golpe do pix por engano 3](#_Toc1750856364)

[Golpe do falso boleto 4](#_Toc1646938263)

[Pharming 5](#_Toc42753618)

[Tipos de Ataques na Internet 6](#_Toc1788795531)

[Ataques de Negação de Serviço (DoS e DDoS): 6](#_Toc474863040)

[Phishing 6](#_Toc208973001)

[Malware 7](#_Toc1266418322)

[CONCLUSÃO 7](#_Toc999544216)

[REFERÊNCIAS 8](#_Toc1142988292)

**Tipos de Golpes na Internet**

## **Golpe do pix por engano**

Funciona da seguinte maneira:

* O fraudador faz uma transferência para a conta da vítima usando, normalmente, uma chave pix de número telefônico;
* Em seguida, a vítima recebe uma mensagem ou ligação do golpista no mesmo número. No contato, ele afirma ter feito a transação por engano e pede o dinheiro de volta, mas informa a chave pix de outra conta;
* Enquanto a vítima realiza o processo de devolução para a conta informada, o fraudador se utiliza de um mecanismo criado justamente para coibir golpes, o Mecanismo Especial de Devolução (MED), para pedir ao banco o dinheiro de volta na conta pela qual fez o pix inicial;

Na sexta-feira, dia 5 de julho de 2024, um professor paranaense, Luiz Cezar Lustosa Garbini devolveu um pix feito por engano e ficou no prejuízo. O golpista que inicialmente transferiu R$ 700 "por engano", no fim das contas, ficou com R$ 1.400, sendo R$ 700 da devolução do banco e R$ 700 devolvidos por Luiz. O professor, por sua vez, perdeu R$ 700. Ele foi reembolsado pelo banco depois da repercussão do caso.

## **Golpe do falso boleto**

Golpistas enviam boletos falsificados por diversos meios, como e-mail, SMS etc. Esses boletos podem conter alguns dados verídicos como nome, CPF/CNPJ e endereço, induzindo o pagamento sem perceber que o dinheiro vai diretamente para o golpista. Isso resulta em cobranças do credor ou na não entrega do produto ou serviço que você esperava pagar.

O crime aconteceu em Goiás, em maio de 2024. Criminosos, incluindo um servente de pedreiro e outros aliados, geraram boletos falsificados para enganar empresas, resultando em grandes prejuízos financeiros. As vítimas, sem perceberem o erro, realizaram pagamentos que foram direcionados para contas bancárias dos criminosos. O prejuízo total superou R$ 500 mil. O golpe foi elaborado de forma a parecer uma transação legítima, causando danos significativos às empresas lesadas.

## **Pharming**

Consiste em um fraude on-line que envolve o uso de código malicioso para direcionar as vítimas a sites falsificados na tentativa de roubar seus dados. O processo ocorre em duas etapas: primeiro o invasor instala o código malicioso no computador ou servidor da vítima que direcionará a mesma para um site falsificado, onde ela pode ser enganada para oferecer seus dados pessoais ou credenciais de login para um site ou serviço on-line.

Este golpe não requer que um usuário abra um site por conta própria, pois é redirecionado automaticamente ao site falsificado pelo invasor.

Um caso documentado de ataque de pharming ocorrido em janeiro de 2008, mostra um banco mexicano foi alvo de um ataque conhecido como "drive-by pharming". Nesse incidente, os invasores alteraram as configurações de DNS do roteador doméstico de um cliente após o recebimento de um e-mail que parecia ser de uma empresa legítima de cartões de felicitações em espanhol. Como resultado, o cliente foi redirecionado para um site falso, permitindo que os atacantes coletassem informações confidenciais.

# **Tipos de Ataques na Internet**

## **Ataques de Negação de Serviço (DoS e DDoS):**

Esses ataques visam tornar um serviço ou rede indisponível, sobrecarregando-o com tráfego excessivo. No caso de ataques DDoS (Distributed Denial of Service), a sobrecarga é gerada por múltiplas fontes simultaneamente. Em 2016, o provedor de DNS Dyn sofreu um ataque DDoS que afetou grandes sites como Twitter, Reddit e Spotify. O ataque foi atribuído ao botnet Mirai, composto por dispositivos IoT comprometidos.

Ferramentas Utilizadas:

* Mirai Botnet: Explora dispositivos IoT vulneráveis para formar uma botnet e realizar ataques DDoS.
* LOIC (Low Orbit Ion Cannon): Ferramenta de código aberto usada para realizar ataques DoS, permitindo que múltiplos usuários a utilizem simultaneamente.

## **Phishing**

Consiste em enganar usuários para que revelem informações confidenciais, como senhas e dados bancários, geralmente por meio de e-mails ou sites falsificados. Em 2016, o Comitê Nacional Democrata dos Estados Unidos foi alvo de um ataque de phishing que resultou no roubo de e-mails confidenciais. Acredita-se que o ataque tenha sido realizado por hackers russos.

Ferramentas Utilizadas:

* Gophish: Framework de código aberto para simulação de phishing, permitindo a criação e gerenciamento de campanhas de phishing.
* King Phisher: Ferramenta de código aberto projetada para testar e treinar usuários contra os ataques de phishing.

## **Malware**

Consiste em um software malicioso projetado para danificar, explorar ou obter acesso não autorizado a sistemas ou redes. Em 2017, o ransomware WannaCry afetou milhares de organizações em todo o mundo, incluindo o Sistema Nacional de Saúde do Reino Unido (NHS). O ataque explorou uma vulnerabilidade no Windows e foi atribuído ao grupo Lazarus, vinculado à Coreia do Norte.

Ferramentas Utilizadas:

* Metasploit: Framework de código aberto utilizado para desenvolver e executar exploits contra sistemas remotos.
* Cobalt Strike: Ferramenta comercial que fornece recursos avançados para testes de penetração e simulação de ataques, incluindo a criação de payloads maliciosos.

# **CONCLUSÃO**

Os golpes na internet, como o Pix por engano, o falso boleto e o pharming, têm se mostrado cada vez mais prejudiciais, afetando tanto pessoas físicas quanto empresas. A sofisticação dessas fraudes, aliada a ferramentas como o Mirai Botnet, LOIC, Gophish e King Phisher, evidencia a necessidade urgente de estratégias mais eficazes de prevenção e conscientização sobre segurança digital. O caso do professor paranaense, Luiz Cezar Lustosa Garbini, e o ataque ao Comitê Nacional Democrata dos EUA, são apenas alguns exemplos de como esses golpes podem ter consequências devastadoras. Portanto, é fundamental que os usuários estejam atentos e que as instituições invistam em mecanismos de segurança mais robustos para mitigar o impacto desses ataques, garantindo a proteção das informações e transações online.

# **REFERÊNCIAS**

* **G1.** Golpe do Pix errado: saiba como os criminosos agem e como não ser enganado. G1 Economia, 12 jul. 2024. Disponível em:

<https://g1.globo.com/economia/noticia/2024/07/12/golpe-do-pix-errado-saiba-como-os-criminosos-agem-e-como-nao-ser-enganado.ghtml>

* **BRADESCO.** Golpe do boleto falso. *Bradesco*, [s.d.]. Disponível em: <https://banco.bradesco/seguranca/prevencao-de-golpes/golpe-boleto-falso.shtm>. Acesso em: 19 fev. 2025.
* **G1.** Golpe do boleto falso: entenda como servente de pedreiro e outros comparsas enganaram empresas, causando prejuízo de mais de R$ 500 mil. *G1 Goiás*, 28 mai. 2024.

Disponível em: <https://g1.globo.com/go/goias/noticia/2024/05/28/golpe-do-boleto-falso-entenda-como-servente-de-pedreiro-e-outros-comparsas-enganaram-empresas-causando-prejuizo-de-mais-de-r-500-mil.ghtml>. Acesso em: 19 fev. 2025.

* **FORTINET.** Pharming. Fortinet. Disponível em: <https://www.fortinet.com/br/resources/cyberglossary/pharming#:~:text=O%20Pharming%20%C3%A9%20uma%20fraude,ou%20servidor%20de%20uma%20v%C3%ADtima>. Acesso em: 22 fev. 2025.
* **MESSMER,** Ellen. *Primeiro caso de "drive-by pharming" identificado na prática*. Network World, 22 jan. 2008. Disponível em: https://www.networkworld.com/article/2209070/first--drive-by-pharming--case-identified-in-the-wild.html. Acesso em: 22 fev. 2025.
* **FORTINET.** Tipos de ataque cibernético. Disponível em: <https://www.fortinet.com/br/resources/cyberglossary/types-of-cyber-attacks>. Acesso em: 22 fev. 2025.
* **INTEROP**. Os 17 tipos de ataques cibernéticos mais perigosos para 2024. Disponível em: <https://www.interop.com.br/en/tipos-de-ataques-ciberneticos/>. Acesso em: 22 fev. 2025.
* **KASPERSKY**. O que são crimes cibernéticos e como se proteger deles? Disponível em: <https://www.kaspersky.com.br/resource-center/threats/what-is-cybercrime>. Acesso em: 22 fev. 2025.