

# PHISHING ATTACKS

-By Kothakapu Mounika



# Network Intrusion & Phishing Awareness

Understanding the tools and tactics used in cyber threats is the first step towards robust defence. This presentation delves into network sniffers and the critical role of phishing awareness.

# Today's Agenda: Understanding Network Intrusions and Human Vulnerabilities

01

## Network Sniffers: The Basics

Exploring how network traffic can be intercepted and analysed.

02

## Legitimate vs. Malicious Use

Distinguishing between ethical and unethical applications of sniffing technology.

03

## Phishing Awareness

Understanding the heart of digital deception and its human targets.

04

## Prevention Strategies

Best practices to protect yourself and your organisation from phishing attacks.

# What is a Network Sniffer? Peering into Your Digital Traffic

A network sniffer, also known as a packet analyser, is a tool that intercepts and logs traffic passing over a digital network. Think of it as a tap on a telephone line, allowing someone to listen in on conversations.

- Captures data packets flowing across a network.
- Can reveal sensitive information if traffic is unencrypted.
- Operates by placing the network interface card into "promiscuous mode".



# How Basic Network Sniffers Function: Packet Capture Explained



## Data Transmission

Information travels across the network in small units called packets.

## Interception

The sniffer captures these packets as they pass through its network segment.

## Analysis

It then decodes and displays the raw data within each packet, revealing details like source, destination, and payload.

Unencrypted traffic, such as HTTP requests or older protocols, is particularly vulnerable to this type of interception, making strong encryption ([HTTPS](#), VPNs) paramount.

# Legitimate Uses vs. Malicious Intent: The Dual Nature of Sniffing

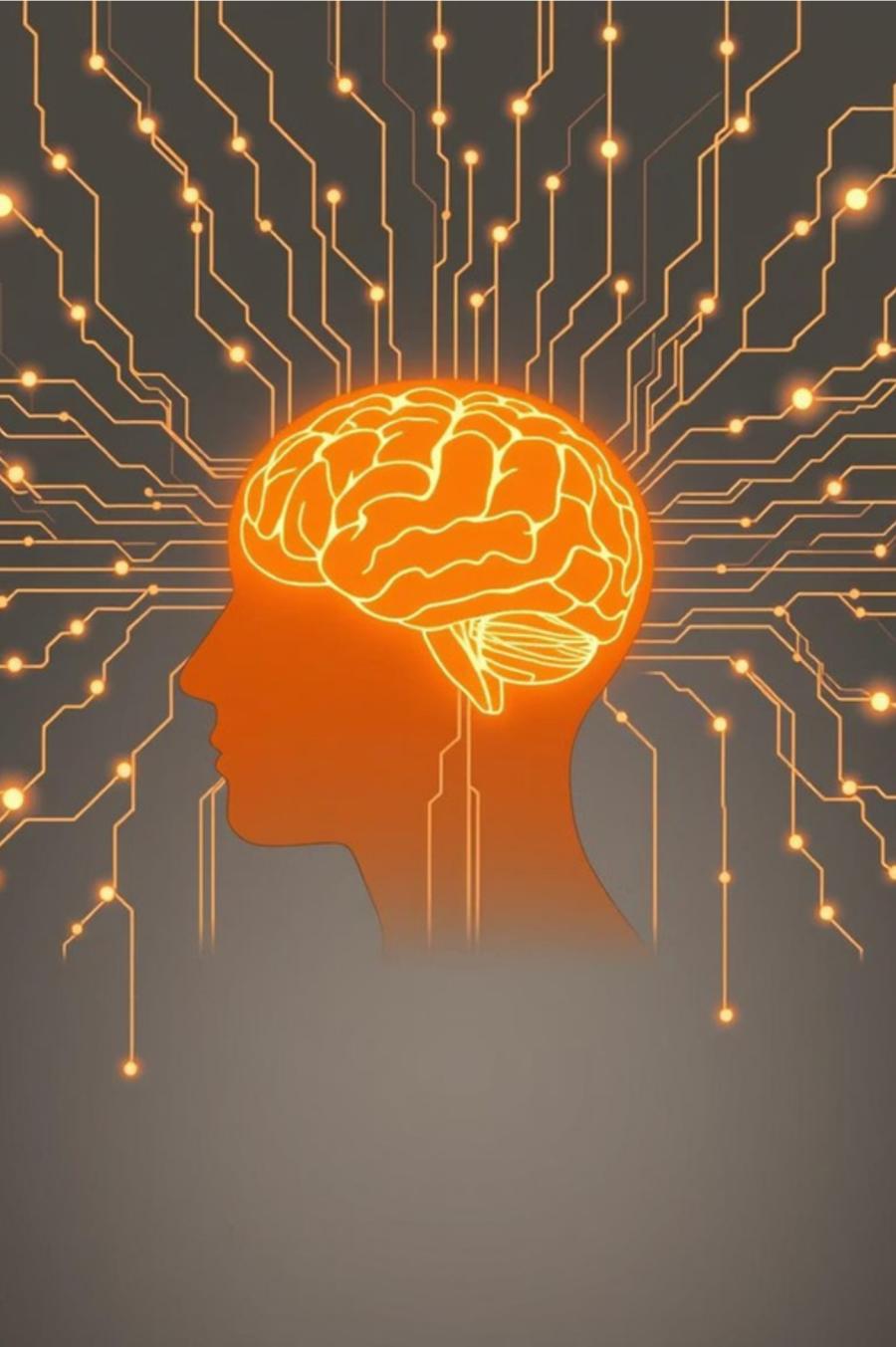
## Legitimate Uses

- Network troubleshooting and diagnostics.
- Performance monitoring and optimisation.
- Security analysis and intrusion detection.
- Protocol development and debugging.

## Malicious Intent

- Password and credential harvesting.
- Sensitive data theft (e.g., credit card numbers).
- Eavesdropping on private communications.
- Reconnaissance for further attacks.

While sniffers are essential tools for IT professionals, their power necessitates strict ethical guidelines and robust security measures to prevent misuse.



# Transitioning to Human Factors: Why Even Secure Networks Need Vigilant Users

Even with the most advanced firewalls and encryption, the human element remains the weakest link in cybersecurity. Attackers frequently bypass technical defences by exploiting user trust and behaviour. This is where phishing comes into play, targeting our psychology rather than our systems.

# Phishing Defined: The Art of Digital Deception

"Phishing is a type of social engineering where an attacker sends a fraudulent message designed to trick a person into revealing sensitive information or deploying malicious software on the victim's infrastructure."

Phishing attacks commonly masquerade as trustworthy entities, such as banks, government agencies, or even internal IT departments. They aim to create a sense of urgency, fear, or curiosity to prompt immediate action from the victim.

# Recognising Phishing Attempts: Spotting the Subtle Red Flags



## Suspicious Sender

Unfamiliar email addresses, generic greetings, or sender names that don't match the email domain.



## Poor Grammar & Spelling

Many phishing emails contain glaring errors due to non-native speakers or automated translation.



## Urgent or Threatening Language

Emails demanding immediate action or threatening consequences for inaction are classic phishing tactics.



## Unusual Links or Attachments

Hover over links to check the actual URL; avoid opening unexpected attachments, especially executables.

# Best Practices for Phishing Prevention: Safeguarding Your Digital Identity



- **Verify Sender Identity:** Always double-check who sent the email, especially if it asks for sensitive information.
- **Never Click Suspicious Links:** Type URLs directly or use trusted bookmarks.
- **Use Strong, Unique Passwords:** Implement multi-factor authentication (MFA) whenever possible.
- **Keep Software Updated:** Patches often fix security vulnerabilities that attackers exploit.
- **Report Phishing Attempts:** Inform your IT department or security team immediately.

# Key Takeaways: Fortifying Your Network & Your Mind Against Cyber Attacks



## Understand the Threat

Network sniffers can expose unencrypted data; encryption is your primary defence.



## Humans are Targets

Phishing bypasses technical controls by exploiting human trust and psychology.



## Stay Vigilant

Recognise red flags in suspicious emails and messages.



## Practice Prevention

Verify, don't click; use strong passwords and MFA; keep software updated.

Cybersecurity is a shared responsibility. Your awareness and actions are critical to protecting not just yourself, but the entire organisation.