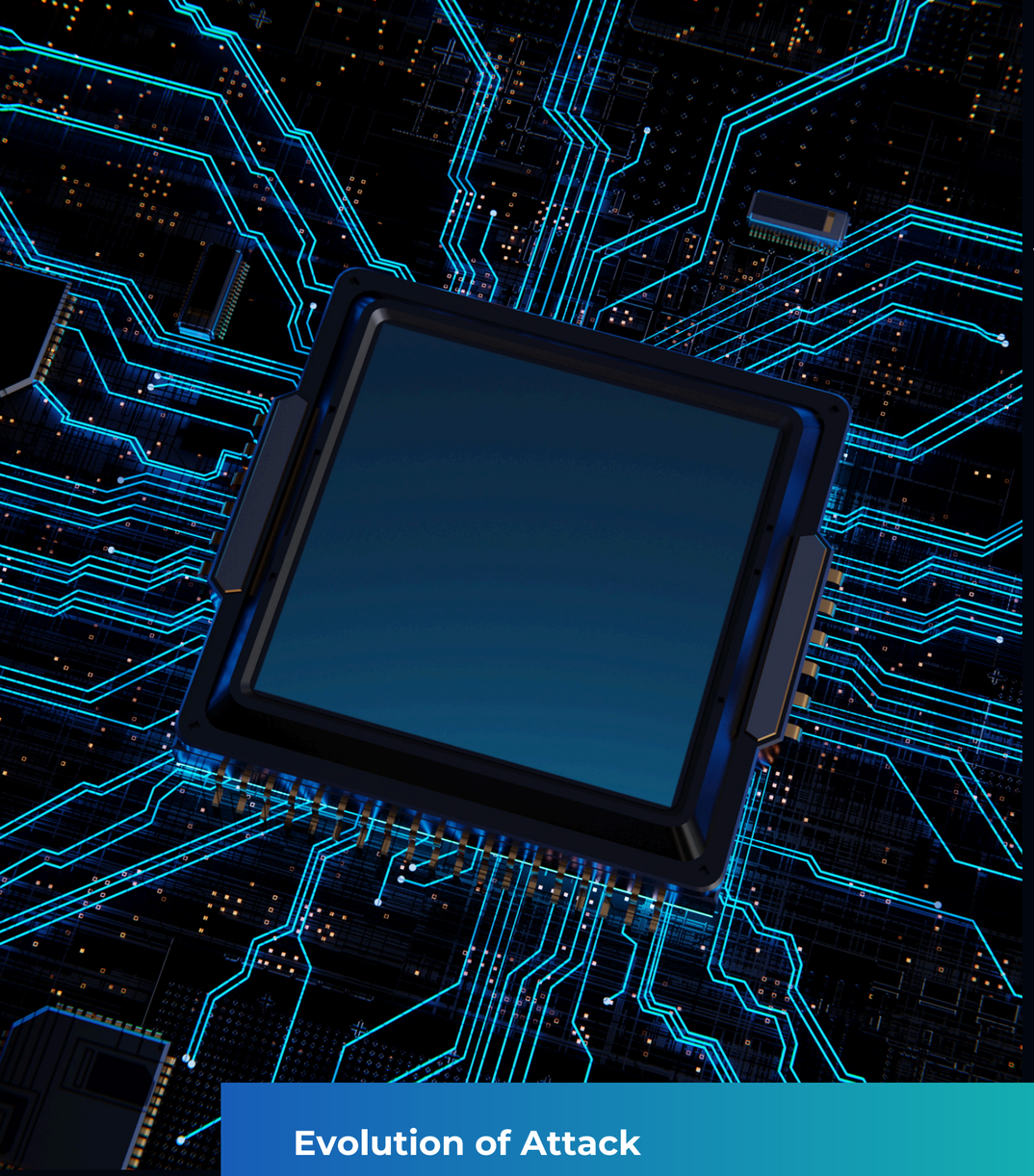
CYBER SECURITY

Outsmarting Cyber Scammers in the Digital Age

🎣 **Phishing Awareness Training: Unmasked**

By Zwivhuya Tshutshu | CodeAlpha Internship



WHAT IS PHISING?

-Phishing is a cyberattack where criminals trick you into revealing sensitive info.

-Disguised as a trusted sender (banks, IT admin, delivery service).

-Goal: steal passwords, credit cards, or personal info.

Evolution of Attack **90%**

REAL-WORLD EXAMPLE

- 🚨 **Fake PayPal Email:** “Your account will be suspended. Click here to verify.”
- ✅ **Real PayPal Email**: Professional, secure domain, no urgency.
-
- **Spot the difference:**
- Wrong sender domain.
- Urgent/fear tone.
- Suspicious link (hover reveals fake URL).

Protection

Comprehensive security covering all vulnerabilities.

Real-Time

Continuous monitoring to instantly neutralize threats.

Secure Data

Ensure the safety of sensitive data with robust encryption

Advanced

Protection against cyber attacks with cutting-edge detection.

SOCIAL ENGINEERING TACTICS

Cybercriminala exploit human psychology:

- ⏰ Urgency: “Update now or lose access!”
- 🏛️ Authority: “Message from IT Admin.”
- 👀 Curiosity: “See attached invoice.”
- 😱 Fear: “Suspicious login attempt detected.”

Solutions

24/7 Support

Round-the-clock assistance to ensure your security.

Tailored Solutions

Customized security strategies for your specific needs.

Proactive Monitoring

Continuous threat detection and prevention.

MODERN INFORMATION PROTECT FROM HACKERS

Utilizing cutting-edge encryption to safeguard data from hackers.

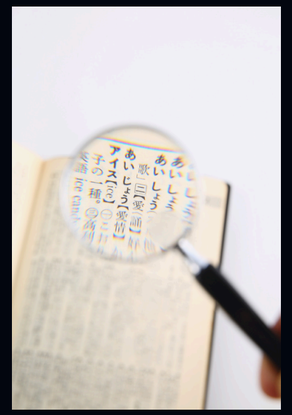
Threat Detection

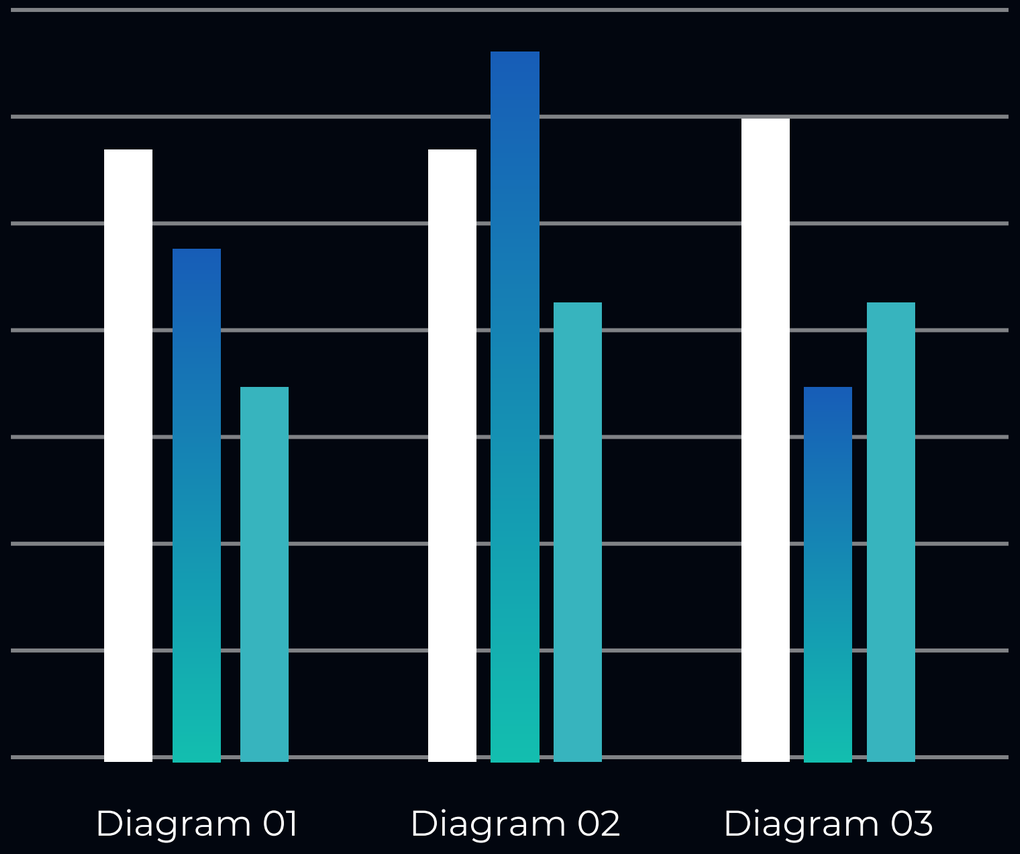
Firewall Defense

Security Updates

HOW TO SPOT PHISHING

- ✅ Double-check sender’s email domain.
- ✅ Hover over links before clicking.
- ✅ Look for grammar/spelling mistakes.
- ✅ Don’t trust unrequested attachments.
- ✅ Does it create fear or urgency?





COLUMN CHART ANALYSIS SLIDE

Compliance Metrics

Track and analyze adherence to industry security standards and regulations to ensure compliance.

User Awareness

Assess the effectiveness of security training programs by measuring reductions in user-related incidents.

Threat Sources

Identify and analyze the origins of security threats to improve defenses and prevention strategies.

BEST PRACTICES

🔐USE TWO-FACTOR AUTHENTICATION (2FA)

🛡️ Don’t reuse passwords.

📨 Report suspicious emails to IT/security team.

💻 Keep antivirus & filters updated.

- 2016 US Election: A simple spear phishing email compromised key campaign staff

- COVID-19 Scams: Fake vaccine registration emails targeted anxious populations.

- CEO Fraud: Attackers impersonated CEOs to request fraudulent wire transfers, costing companies millions

- Bank SMS Scam: Victims received messages with fake links leading to credential theft.

INTERACTIVE QUIZZES

Quiz

Q1: What should you do first if you suspect phishing?

Report it ✅

Q2: Which is a phishing attempt?

- A: support@paypa1.com → **FAKE**
- B: support@paypal.com → **REAL**

Q3: • Spot-the-Phish:

Analyze sample emails to identify signs of phishing.

Q4: • URL Challenge:

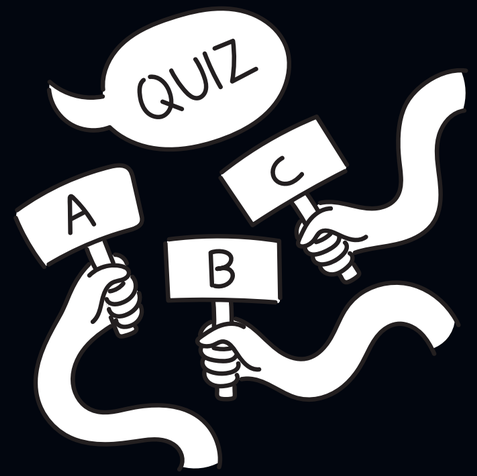
Decide which URLs are genuine and which are fraudulent

Q5: • Scenario Roleplay:

Practice how to respond when your 'boss' urgently asks for sensitive information.

Q6: • • Live Phish Simulation:

Optional corporate exercise to test readiness



SUMMARY & TAKEAWAYS

Key Reminder:

Think Before You Click: Always pause and verify.

Verify Sources: Contact organizations using official contact information.

Report Quickly: Immediate reporting reduces risk for everyone.

- Continuous Vigilance: Cyber threats evolve; stay updated on the latest tactics.

Resource:

Helpful Links:

- Anti-Phishing Working Group: https://www.antiphishing.org

- **Cybersecurity & Infrastructure Security Agency**: https://www.cisa.gov

- Your Company Security Policy and IT Department Contact.

Use these resources to stay informed and prepared.

THANK YOU!!

“Trust is earned — links are verified.”

💡 Always think before you click.

CodeAlpha Cybersecurity Internship | Zwivhuya Tshutshu