Phishing Awareness Simulation – Understanding and Identifying Email Scams

Introduction

As an aspiring cybersecurity analyst, I’m always eager to learn how real-world cyberattacks happen. One of the most common threats people face is phishing—an attack that tricks users into revealing sensitive information. To better understand this, I created my own phishing simulation project where I designed a fake phishing email for learning purposes and studied the techniques used by attackers.

What is Phishing?

Phishing is a social engineering attack where hackers send fake emails that look legitimate to trick people into: - Clicking on malicious links - Giving away passwords or credit card numbers - Downloading malware

Phishing Email Simulation

I created a sample phishing email that mimics a security alert from a popular company. Here's what it looked like: Subject: ■ Unusual Sign-in Attempt Detected From: support@microsoft-security.com Dear User, We noticed a suspicious sign-in to your account from a new device. Location: Moscow, Russia Time: 2:31 AM If this wasn’t you, please reset your password immediately: ■ [Reset Password] - Microsoft Security Team

Red Flags I Noticed

Even though it looks real, here’s how I identified it as fake: - “Dear User”: No personal name used - Fake sender email: Slightly modified domain - Urgent tone: Makes user panic - Link: Doesn’t go to a real Microsoft site - Grammar: Minor mistakes common in phishing

What I Learned

- Attackers use psychological tricks like fear and urgency. - Anyone can fall victim, even smart users. - Awareness and careful inspection can prevent disasters.

How to Stay Safe

Here are 5 easy tips to avoid phishing emails: 1. Check the sender’s full email address. 2. Hover over links before clicking. 3. Never share passwords via email. 4. Use 2-Factor Authentication (2FA) always. 5. Report phishing to your email provider or IT team.

Final Thoughts

This was my first cybersecurity project, and I learned a lot by doing it practically. I now have a better understanding of phishing and feel more prepared to educate others. Cybersecurity is not just about tools – it’s about people.