FUTURE_CS_02

Introduction

Phishing is one of the most common cyber attacks used against organisations today, rather than exploiting technical weakness phishing attacks rely on social engineering techniques to trick users into revealing sensitive information by either clicking malicious links or downloading harmful content. This report analyses real world phishing emails examples to identify common warning signs and explain how such attacks operate. The aim of this assessment is to improve user awareness and provide guidance to help people and organizations reduce the risk of phishing attacks.

Task

Scope of Analysis

This task was done using a sample phishing email taken from Github created for cybersecurity awareness. This analysis focused on identifying phishing indicators, classifying risk level and providing prevention recommendations. No real users or systems were targeted during this task.

Sample email

Sample Phishing email used: https://github.com/rf-peixoto/phishing_pot/blob/main/email/sample-10.eml

Simulated Phishing Email (Educational Sample)

Subject: ■■ Unusual Sign-In Activity Detected

From: Account Security Team

Reply-To: security-alerts@gmail[.]com To: user@company[.]com

Date: Fri, 08 Sep 2023 05:47:04 +0000

Dear User,

We detected unusual sign-in activity on your account.

A login attempt was recorded from a new device and unfamiliar location. If this activity was not performed by you, immediate action is required to prevent account suspension.

Sign-In Details

Location: Russia / Moscow

IP Address: 103.225.77.255

Platform: Windows 10

Browser: Firefox

Time: Fri, 08 Sep 2023

If this was not you, please verify your account immediately to secure your information.

Verify Account: http://account-security-verify[.]com/login

Failure to verify within 24 hours may result in temporary account lock.

Thank you,

Account Security Team

Email header Analysis

The analysis of this email header showed that there are authentication irregularities and suspicious routing behaviour. The sender domain can not be properly verified and authentication mechanisms such as SPF have showed issues. These failures indicate that the email may have been sent from a unauthorized source which is a common characteristic in a phishing attack.

Phishing Indicators Identified

Indicator	Evidence found	Risk Level
Generic greeting	Dear User	Medium
Urgency tactic	Account suspension warning	High
Suspicious sender domain	Access accsecurity.com	High
Reply to mismatch	Gmail address used	High
Suspicious link	Account security verify[.].com	High

Risk classification

The analysed email demonstrates multiple high risk phishing characteristics which include authentication failures and suspicious verification links. Due to these indicators the email is classified as a confirmed phishing attempt which is used to deceive recipients into taking unsafe actions.

Prevention and awareness

- Verify sender email domains
- Avoid clicking links in urgent security emails
- Access accounts through official websites only
- Be cautious of unexpected security warnings
- Report suspicious emails to IT teams.
- Check for generic greetings or grammar issues

Conclusion

This report analysed a simulated phishing email and identified several warning signs which had included suspicious sender details, authentication failures, urgency based language and deceptive links. Due to these indicators the email was classified as high risk phishing. The findings emphasise the importance of user awareness when handling emails and recognizing common phishing techniques.