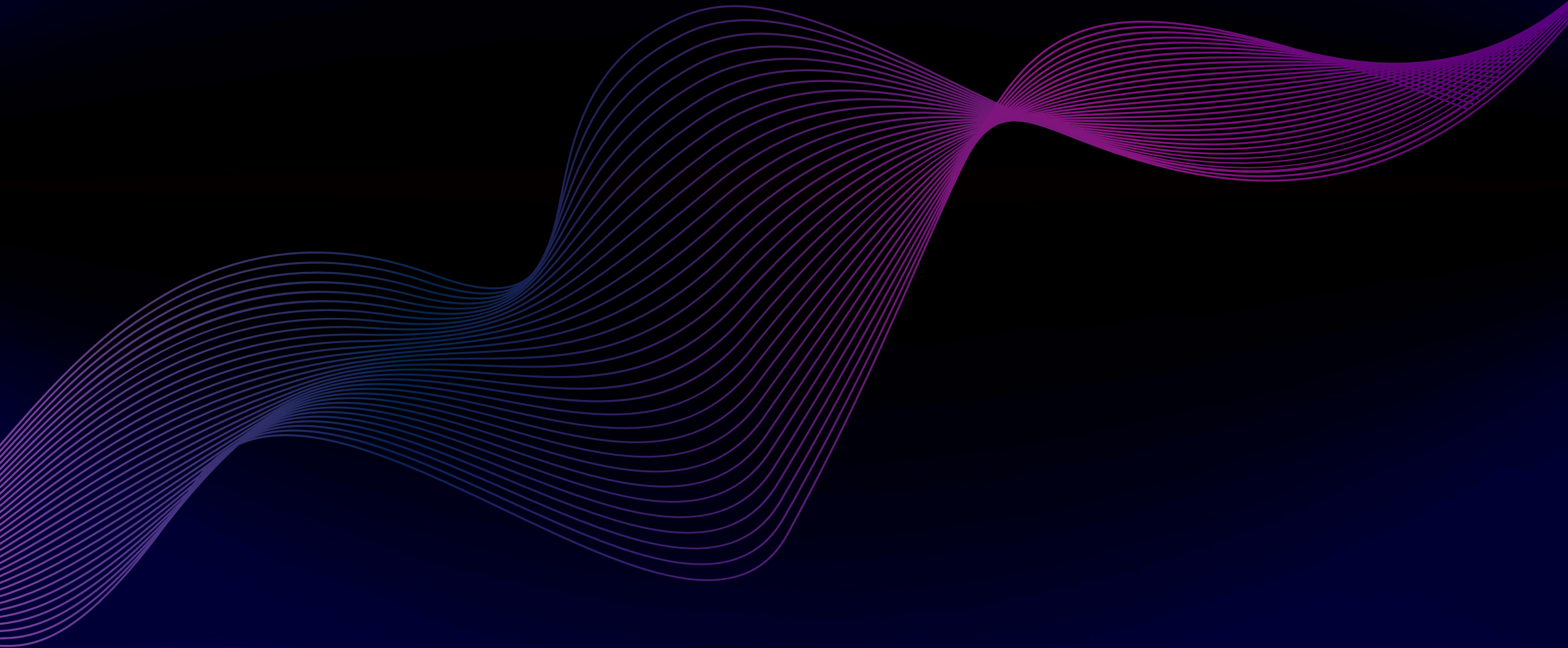
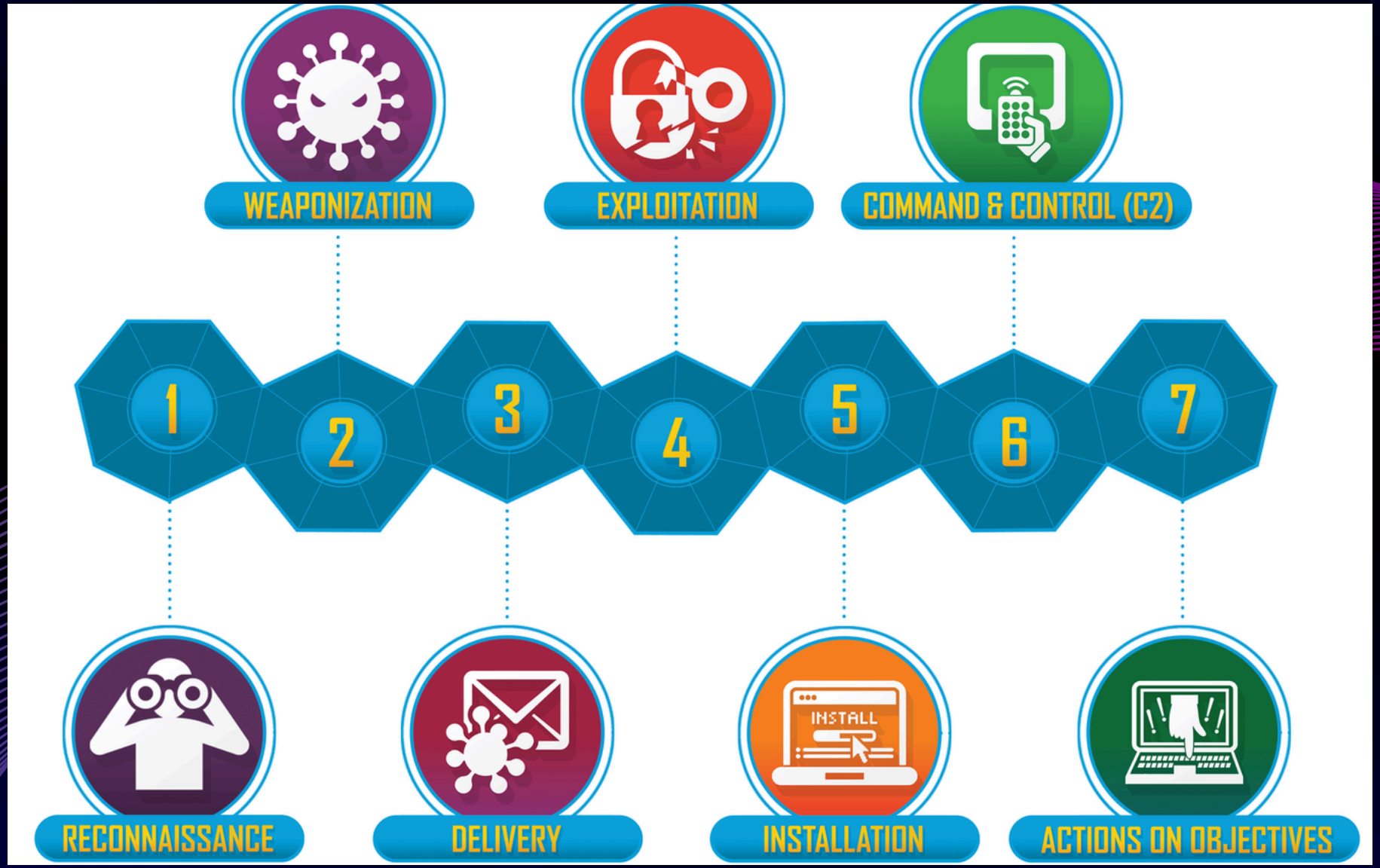
PHISHING EMAILS



The Cyber Kill Chain Framework



Phishing Emails in the Cyber Kill Chain

Phishing emails primarily operate in the Delivery stage (Stage 3) of the Cyber Kill Chain

During the Delivery phase, phishing emails serve as the primary vector for transmitting malicious payloads to targets

These emails often contain malicious links, weaponized attachments, or fraudulent forms designed to trick recipients into taking actions that advance the attacker's objectives

What Are Phishing Emails?

Phishing is a type of cyberattack where threat actors act as legitimate companies or individuals to steal sensitive information.

Phishing emails are fraudulent messages designed to trick recipients into revealing personal data, login credentials, financial information, or downloading malware

Key characteristics of phishing emails include

Impersonation

Attackers pose as trusted entities like banks, government agencies, or colleagues

Social Engineering

They exploit human psychology using urgency, fear, or authority to manipulate victims

Credential Harvesting

Primary goal is often to steal usernames, passwords, and other sensitive data

Malware Delivery

Some phishing emails contain malicious attachments or links to infected websites

How Phishing Attacks Are Executed

Domain Spoofing Techniques

Domain spoofing is a technique used in phishing where attackers make their emails or websites come from a legitimate source.

Domain Spoofing Methods

Fake “From” addresses : Making emails appear to come from trusted sources

Look-alike domains : Registering domain names that closely look like legitimate ones

Subdomain manipulation : Using legitimate-looking subdomains to deceive recipients

Typosquatting - Creating domains that exploit common typing errors

Reply-To Header Manipulation

This header specifies which email address should receive replies, and it can differ from the "From" address

How Reply-To manipulation works

Attackers set the “From” field to appear legit while directing replies to a different , attacker controlled email address.

This technique allows them to maintain the illusion of legitimacy while capturing victim responses

Email Header Analysis

what does the email header contain?

1. From

The From field indicates the sender's display name and email address. While visible in the inbox, this field is easy to spoof and doesn't guarantee authenticity.

```
From: John Smith <john.smith@company.com>
```

2. To

The To field lists the intended recipients of the message. Multiple addresses may indicate a broad campaign or targeted distribution.

```
To: jane.doe@recipient.com, marketing@recipient.com
```

3. Subject

The subject field displays the email's subject line. Though often overlooked in header analysis, threat actors frequently use urgent or alarming subjects to increase engagement.

```
Subject: Urgent: Your Account Access Will Expire
```

4. Date

The Date field shows when the message was sent, including the time zone. Irregular or mismatched timestamps can suggest manipulation or delay tactics.

```
Date: Tue, 15 Jun 2021 09:45:32 -0700 (PDT)
```

5. Message-ID

The Message-ID is a globally unique identifier for the message. Repeated or malformed IDs across emails can indicate mass phishing campaigns or spoofed messages.

```
Message-ID: <CAE5Nd+b4ZSVMvo+9=qY2cpGfG20Kt-XQcy4dVS5JxqausMnJHQ@mail.gmail.com>
```

6. Return-Path

The Return-Path specifies where undeliverable messages should be sent. If this doesn't match the domain in the From field, it may point to spoofing or unauthorized senders.

```
Return-Path: <bounce-handler@sender-domain.com>
```

7. Received

The Received fields log each server the message passed through, listed from newest to oldest. These entries help identify unusual routing paths, mismatched IPs, or forged hops.

```
Received: from mail-ej1-f68.google.com (mail-ej1-f68.google.com [209.85.218.68])
 by mx.recipient-domain.com (Postfix) with ESMTPS id 4GH2ht5ZQJz28v
 for <jane.doe@recipient.com>; Tue, 15 Jun 2021 09:45:33 -0700 (PDT)
Received: by mail-ej1-f68.google.com with SMTP id s20so12345678ejl.3
 for <jane.doe@recipient.com>; Tue, 15 Jun 2021 09:45:32 -0700 (PDT)
```

8. Reply-To

The Reply-To field defines the address for replies. This is often different from the From address in phishing campaigns. If this field points to a suspicious or unrelated domain, it's a red flag.

```
Reply-To: attacker-controlled@malicious-domain.com
```

Detecting phishing emails

-Sender verification : Check if the "From" domain matches the "Return-Path"

-Reply-To : When Reply-To addresses differ from the sender address

-Generic greetings - "Dear Customer" instead of personalized names

-Grammar and spelling errors - Professional organizations typically use proper spelling and grammar

-Suspicious attachments - Unexpected files, especially with extensions like .zip, .exe, or .scr

-Mismatched URLs - Links that don't match the claimed sender's domain

-Requests for sensitive information - Legitimate organizations don't request passwords or personal data via email

Email Authentication Protocols

SPF (Sender Policy Framework)

Specifies which IP addresses and servers are authorized to send emails on behalf of a domain. SPF helps prevent basic email spoofing by verifying that emails come from authorized sources.

DKIM (DomainKeys Identified Mail)

Uses digital signatures to verify that emails haven't been tampered with during transit. DKIM ensures email integrity and confirms the sender's authenticity through cryptographic verification.

DMARC (Domain-based Message Authentication, Reporting, and Conformance)

Combines SPF and DKIM to provide comprehensive email authentication .DMARC can block over 99% of fraudulent emails

Tips for mitigation

Authenticate your emails: A critical aspect of impersonation risk is attackers spoofing your domain and abusing your brand and reputation. Email authentication is one of the most effective ways to prevent domain spoofing. So, look for a solution that can authenticate all your emails, including user and application emails.

Empower your employees: it's important to pair your threat detection solution with a threat-driven security awareness program. Doing so will give your employees the knowledge that they need to identify impersonation tactics and themes. Also, remember to give them tools to report any suspicious messages.

Scan Attatched files before opening them via virus scanning tools

Real-World Phishing Email Attack Examples

Apple Support Spoof

Users received emails appearing to be from "support@apple.com" claiming their Apple ID was blocked, prompting them to enter credentials on a fake site for credential theft.

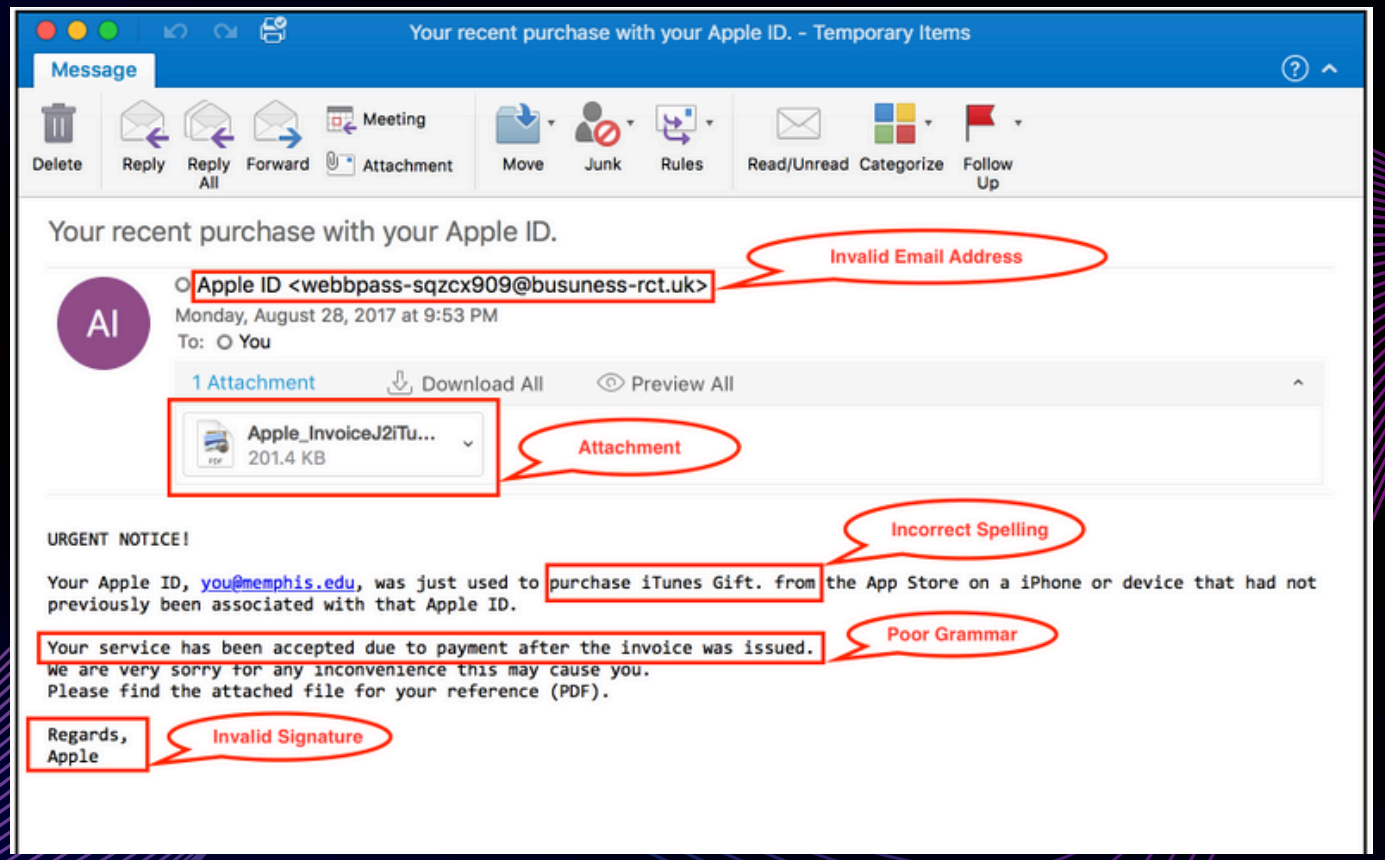
Whaling Attack on Levitas Hedge Fund

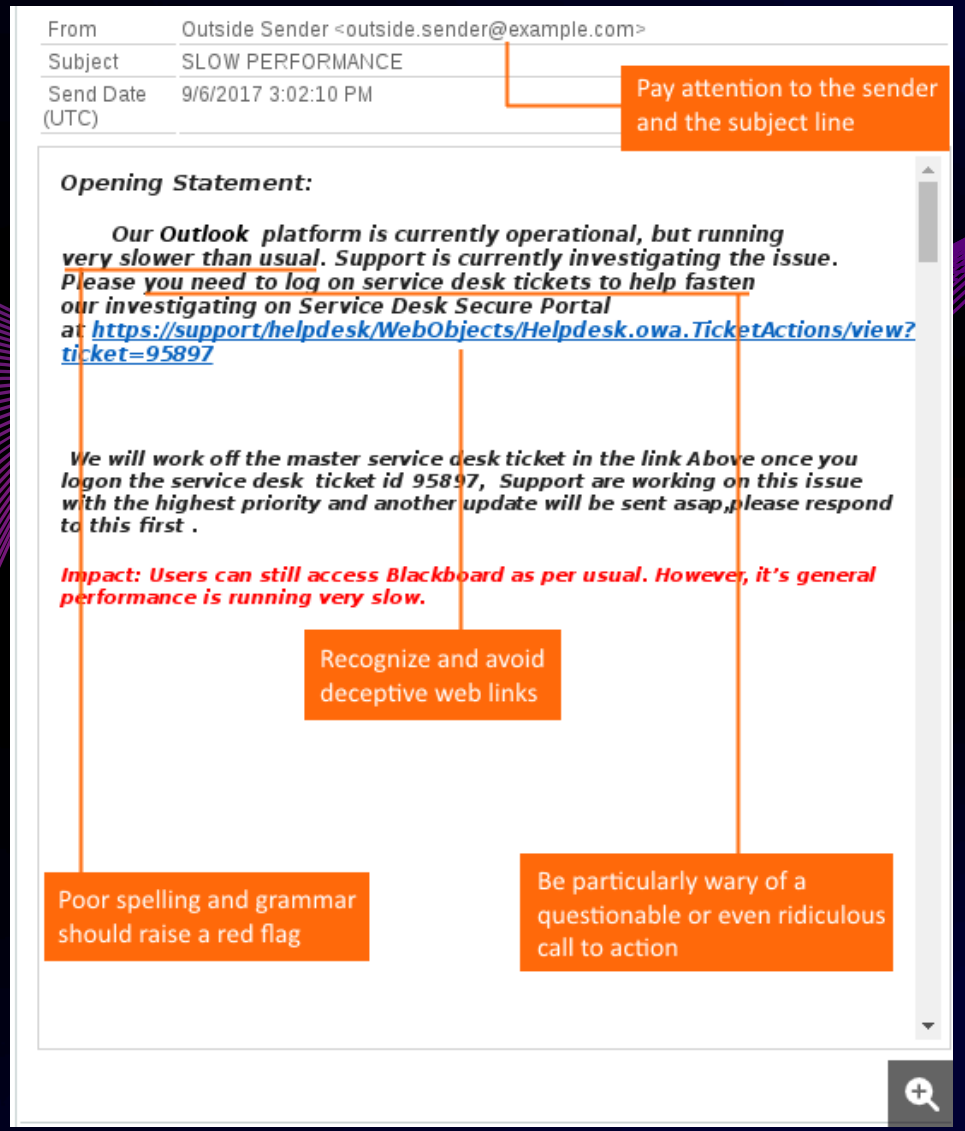
senior executive was targeted with a phishing email containing a fraudulent Zoom link. After clicking, malware was installed, resulting in an $800,000 loss.

Outlook spoof

Attackers sent fake Microsoft emails claiming your Outlook account would be deactivated, urging you to click a link and enter your password on a fake login page to steal your credentials

Examples


Your recent purchase with your Apple ID. - Temporary Items
Message
Delete
Reply
Reply All
Forward
Meeting
Attachment
Move
Junk
Rules
Read/Unread
Categorize
Follow Up
Your recent purchase with your Apple ID.
AI
Apple ID <webbpass-sqzcx909@busuness-rct.uk>
Invalid Email Address
Monday, August 28, 2017 at 9:53 PM
To: You
1 Attachment
Download All
Preview All
Apple_InvoiceJ2iTu...
201.4 KB
Attachment
URGENT NOTICE!
Incorrect Spelling
Your Apple ID, you@memphis.edu, was just used to purchase iTunes Gift. from the App Store on a iPhone or device that had not previously been associated with that Apple ID.
Your service has been accepted due to payment after the invoice was issued.
Poor Grammar
We are very sorry for any inconvenience this may cause you.
Please find the attached file for your reference (PDF).
Regards,
Apple
Invalid Signature


From
Outside Sender <outside.sender@example.com>
Subject
SLOW PERFORMANCE
Send Date (UTC)
9/6/2017 3:02:10 PM
Pay attention to the sender and the subject line
Opening Statement:
Our Outlook platform is currently operational, but running very slower than usual. Support is currently investigating the issue. Please you need to log on service desk tickets to help fasten our investigating on Service Desk Secure Portal at https://support/helpdesk/WebObjects/Helpdesk.owa.TicketActions/view?ticket=95897
We will work off the master service desk ticket in the link Above once you logon the service desk ticket id 95897, Support are working on this issue with the highest priority and another update will be sent asap,please respond to this first .
Impact: Users can still access Blackboard as per usual. However, it's general performance is running very slow.
Recognize and avoid deceptive web links
Poor spelling and grammar should raise a red flag
Be particularly wary of a questionable or even ridiculous call to action

Notable CVEs Exploited via Phishing Emails

CVE-2025-8088: WinRAR Directory Traversal

-This vulnerability in WinRAR allowed attackers to craft malicious RAR archives that, when opened, could place executables in Windows Startup folders. Phishing emails with these attachments delivered RomCom malware, enabling remote code execution and persistent access for attackers.

-Attackers craft a RAR archive that appears harmless, but actually contains hidden malicious files using a Windows feature called Alternate Data Streams (ADSes)

-These files are set up with special path traversal sequences (like ..\) that trick WinRAR into extracting them into sensitive system folders, such as the Windows Startup folder.

-Victims receive a phishing email with the malicious RAR file attached. The email may look legitimate and urge the user to open the archive.

TEAM

Ahmed Shawkat Eladl : 20236006

Khaled Mohamed Ali : 20235010

Marwan Sameh Elsayed : 20235037

Mohamed Amr Ahmed : 20236087

Phish or Legit interactive game

https://marwanmoafy11.github.io/Phis-or-legit-project/Phishorelgit2.html