PRESENTED BY :
Fathima Zahra Sanuj Abdulla

TASK 2 REPORT

PHISHING EMAIL DETECTION & AWARENESS SYSTEM

EXECUTIVE **SUMMARY**

This report analyses multiple phishing samples ranging from harvesting credentials to financial fraud. This analysis indicates that attackers are increasingly using “High-Severity” system alerts and “Rewards” to bypass the traditional skepticism. By identifying specific the technical and psychological markers in these samples, we can reduce the risk of a successful breach.

DEEP DIVE & ANALYSIS OF **PHISHING SAMPLES**

SAMPLE A

The "System Alert" from Microsoft

High-severity alert: Phish delivered due to tenant or user override Inbox ×

Microsoft <microsoft@email-records.com>
to me

4:22 PM (14 minutes ago)

Office 365

A high-severity alert has been triggered

Phish delivered due to tenant or user override

Severity: — High
Time: 01/22/2021
Activity: Protection
Details: 1 message hit on 2aec-43aa-a943-08d7333445aee-1065783939474734-1, sent by Unknown to at time 01/22/2021 9:22 PM.

View alert details

Thank you,
The Office 365 Team

Microsoft

One Microsoft Way
Redmond, WA
98052-6399 USA

DEEP DIVE & ANALYSIS OF **PHISHING SAMPLES**

SAMPLE A

The "System Alert" from Microsoft

TACTICAL HOOK

- This email impersonates an Office 365 "High-severity alert" regarding a phish delivered due to a "tenant override".

RISK LEVEL

CRITICAL (CREDENTIAL THEFT)

THE RED FLAGS

- ***Suspicious Sender:*** The email originates from *microsoft@email-records.com.* A legitimate Microsoft alert would come from a verified *@microsoft.com* or *@office365.com domain.*

PANIC INDUCEMENT

- The use of "High-severity" and "Urgent" triggers a fear response, making the user more likely to click "View alert details" without double checking the link.

DEEP DIVE & ANALYSIS OF **PHISHING SAMPLES**

SAMPLE B

The "Password Change"

Microsoft account password change Inbox ×

Support <support@msupdate.net>
to me

4:09 PM (26 minutes ago)

Microsoft account

Your password changed

Your password for the Microsoft account ethan@hooksecurity.co was changed.

If this was you, then you can safely ignore this email.

Security info used:
Country/region: United States
Platform: iOS
Browser: Safari
IP address: 77.196.86.10

If this wasn't you, your account has been compromised. Please follow these steps:
1. Reset your password.
2. Review your security info.
3. Learn how to make your account more secure.

You can also opt out or change where you receive security notifications.

Thanks,

The Microsoft account team

DEEP DIVE & ANALYSIS OF **PHISHING SAMPLES**

SAMPLE B

The "Password Change"

TACTICAL HOOK

- Informs the user their password has been changed and provides a fake IP address (77.196.86.10) to suggest a hack.

RISK LEVEL

HIGH (ACCOUNT TAKEOVER)

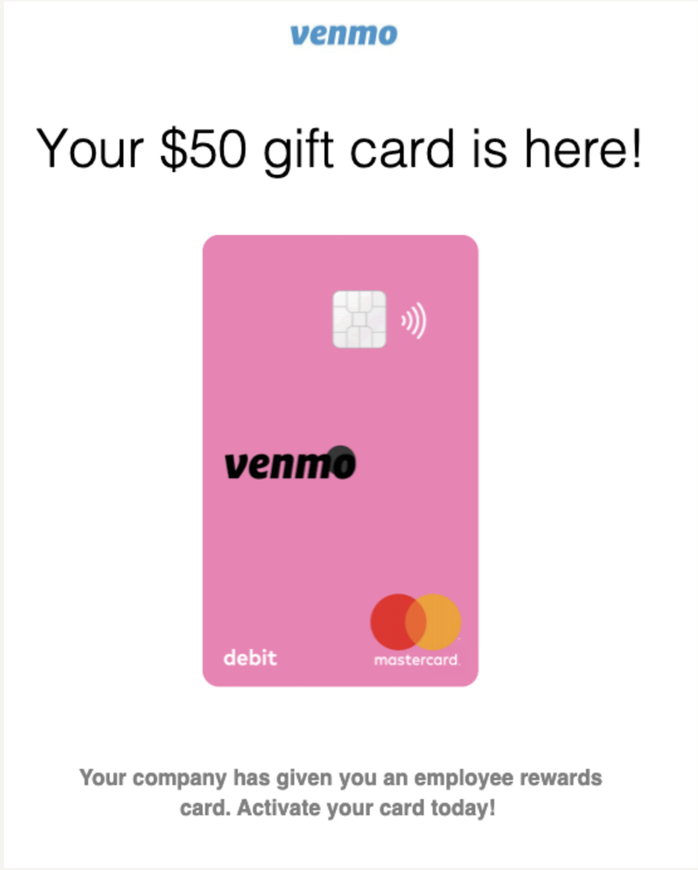
THE RED FLAGS

- ***Masked Domain:*** The sender is *support@msupdate.net*. This is a domain that seems to look alike, designed to appear official.

DEEP DIVE & ANALYSIS OF **PHISHING SAMPLES**

SAMPLE C

The "Lure of Reward"



DEEP DIVE & ANALYSIS OF **PHISHING SAMPLES**

SAMPLE C

The "Lure of Reward"

TACTICAL HOOK

- Offers a "$50 Venmo gift card" as an "employee rewards card".

RISK LEVEL

Suspicious (Identity Theft)

THE RED FLAGS

- Attackers use positive reinforcement of free money to lower the user's guard. Employees are often less cautious with "perks" than they are with "security alerts."

COMPARISON: **PHISHING VS. LEGITIMATE COMMUNICATION**

Using historical business data like Enron Samples, we can identify what "safe" internal communication looks like compared to modern threats.

Feature	Phishing Sample	Legitimate Sample
Context	Randomly offers "pandemic funds" with a login link.	Specific discussion about an offsite location.
Sender	Generic "Assistant Professor" or "Dr. Brown".	Named individuals with a clear history.
Call to Action	"Login immediately" or "Text name to (267) 522-5320".	"Call if you want to discuss" or "Please add to your schedule".

EMPLOYEE PREVENTION GUIDELINES: **SLAMS CHECKLIST**

To protect yourself and the company, apply the SLAMS test to every email

1. **S - Sender:** Check the full email address. Is it from the official company domain (e.g., @stanford.edu vs @stanford-support.com)?

2. **L - Links:** Hover your mouse over any link. If the previewed address in the bottom corner doesn't match the text, do not click.

3. **A - Attachments:** Are you expecting an "interview packet" or "invoice"? If not, contact the sender via a separate channel to verify.

4. **M - Message:** Does it demand "Immediate" or "Mandatory" action to avoid "Suspension"?

5. **S - Signature:** Look for any vague sign offs like "Admin Help Desk" or "ITS Service Team" instead of a specific person's contact information.

SECURITY
DO'S AND DON'TS

✅ ***DO***

- **Verify out-of-band:** If "HR" sends a private document link, call HR or message them on the internal chat to confirm.
- **Report suspicious emails:** Use the "Report Phishing" button in your email client immediately.
- **Check the URL:** Look for misspellings like login.uw.edu/login.login./..

❌ ***DON'T***

- **Don't trust the Display Name:** Just because it says "Apple Support" doesn't mean it is.
- **Don't provide your phone number:** Scammers often move the conversation to SMS (text) to bypass company security filters.
- **Don't login through email links:** Navigate directly to the website (e.g., type venmo.com into your browser) rather than clicking the email link.