

# Emails I Can't Send: How to Identify Phishing Attacks and What You Can Do to Bolster Account Security

Mitch Spaulding, Senior Sales Engineer, SLED

University System  
of New Hampshire



# Why are we still talking about phishing attacks?

## Email is still the #1 Cybersecurity Risk

### #1 Cause of Breaches:

95% of breaches are the result of successful spear phishing attacks, including the most notable ones.

[Source: SANS]

### 3rd Largest Economy on Earth:

- **US** - \$28T
- **China** - \$18T
- **Cyber Crime** - \$9T

## Humans are the Biggest Vulnerability

### Susceptible to Deception:

Humans inherently place a lot of trust in digital communications, which is easily exploited by attackers.

### Easily Accessed Through Email:

Email is the broadest and easiest way for an attacker to engage with any employee.

# What do these phishing attacks lead to?

- Compromised Credentials
- Lateral Attacks from Compromised Accounts
- Direct Deposit / Payroll Changes
- Malware Installation
- Network Downtime
- Financial loss to users and organizations alike



# The Day and Age of Attackers "Breaking into Systems" is Over

**A 16-year-old from Oxford has been accused of being one of the leaders of cyber-crime gang Lapsus\$.**

The teenager, who is alleged to have amassed a \$14m (£10.6m) fortune from hacking, has been named by rival hackers and researchers.

City of London Police say they have arrested seven teenagers in relation to the gang but will not say if he is one.



# Higher Education Phishing Examples

# Employee Impersonation

Subject: [Ext] Kindly provide your available cell number communication to me here ok. Thanks

Sender: [REDACTED]@gmail.com>

Recipient: [REDACTED].edu>

To: [REDACTED].edu>

Jul 27, 2024, 1:23pm EDT

LM [REDACTED]  
Associate Professor & Interim Chair

You don't often get email from [REDACTED]@gmail.com. [Learn why this is important](#)

[REDACTED]  
Interim Chair,

901-[REDACTED]

Dr. [REDACTED]

It is 901-[REDACTED]

(901)-[REDACTED] Thank you.

[REDACTED]

Administrative Services Assistant

708-[REDACTED]

Here it is: 901-[REDACTED]

501-[REDACTED]

Sent from iPhone of Dr. [REDACTED]

901-[REDACTED]

248-[REDACTED]

Get Outlook for Android

Sent from my iPhone

## Campaign Activities

 Received Emails  
162 Recipients

 Forwarded by User  
29 Recipients

 Replied to Message  
32 Recipients

## Attack Breakdown

### Employee Impersonation

#### PAYLOAD

- Engaging Language in the email subject

#### TECHNIQUE

- Impersonate Assoc. Professor and Interim Chair at University
- Compose email subject to encourage users to provide their phone numbers
- Use personal gmail address
- Spray and Pray: bulk email campaign

### Why does it evade traditional security?

- Gmail domain passes sender authentication checks
- Attack is text-based with no malicious payload like a link or attachment
- Threat intelligence and known-bad solutions like M365/Google cannot stop it

# Payroll Fraud - VIP Impersonation

Subject: [Ext] Re:  
Sender: [REDACTED] Impersonated VIP [REDACTED]@aol.com>  
Recipient: [REDACTED] Human Resources [REDACTED]@edu>  
Reply-to: [REDACTED]@aol.com>  
To: [REDACTED] Human Resources [REDACTED]@edu>

MB [REDACTED] VIP  
Associate Vice Chancellor

Would Remediate  
Jul 31, 2024, 9:43am EDT

Hello FORMAL

Could either a bank FINANCIAL letter or a voided check PAYMENT be sufficient for updating my financial institution?

Thank you FORMAL

SENDER

Good morning

Thank you for contacting HR. Yes, either would suffice.

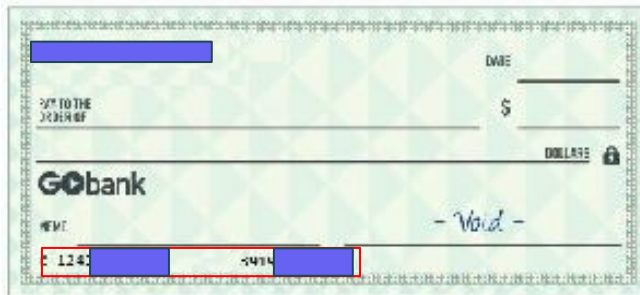
Hello FORMAL

Here you go,

Bank FINANCIAL Name: Go Bank FINANCIAL  
Routing #: 1243 [REDACTED]  
Account PERSONAL INFO #: 391 [REDACTED]  
Account PERSONAL INFO Type: Check PAYMENT img

I will like to override pre-note (Live Check PAYMENT) so the change can be effective for the current pay cycle.

Kindly FORMAL keep me posted.



## Attack Breakdown

### VIP Impersonation

#### PAYLOAD

- Persuasive Language
- Voided Check containing fraudulent bank account details

#### TECHNIQUE

- Impersonate Associate Vice Chancellor at university
- Write compelling message to get HR to act upon the email
- Leverage known-good file attachments like jpg images

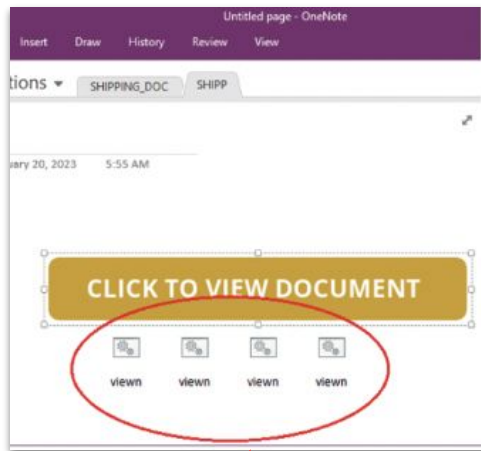
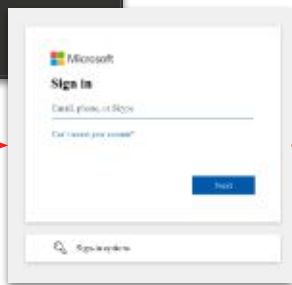
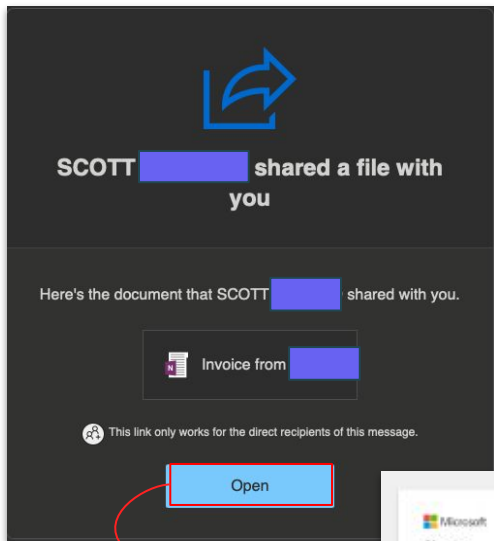
### Why does it evade traditional security?

1. AOL domain passes sender authentication checks
2. Attack is text-based with no malicious payload like a link or attachment
3. Threat intelligence and known-bad solutions M365/Google cannot stop the first email or the second one containing a known-good png image

# Credential Phishing via SharePoint

Subject: SCOTT [redacted] shared "Invoice from [redacted]" with you  
Sender: SCOTT [redacted]  
Recipient: [redacted]@edu>

TL [redacted]  
Associate VC for Public Safety



## Attack Breakdown

### Credential Phishing

#### PAYLOAD

- SharePoint link that hosts malicious content on SharePoint site

#### TECHNIQUE

- Leverage fresh M365 tenant to launch phishing attacks
- Host attack on SharePoint site
- Have users click on malicious link in OneNote File to extort credentials or install malware

### Why does it evade traditional security?


1. Domain passes sender authentication checks
2. Sharepoint links are considered "known-good" in traditional email security scans



# Job Scam from another University

Subject: [REDACTED] SIGNIFICANT INFORMATION  
Sender: [REDACTED]@[REDACTED].edu>  
Recipient: [REDACTED]@[REDACTED].edu>  
To:  
Aug 7, 2024, 2:47pm EDT

**Attachment Preview**  
[REDACTED] page-001.jpg



Part Time Administrative Assistant needed.




Dear Student, In the interest of Professor [REDACTED], you have been preferred to work as a part-time administrative assistant, which gives you the opportunity to earn (\$350 per week). Submit your full name via text message to (310) [REDACTED] for more information. Best Regards

Yes! I am interested and would like to hear more details. I sent the number provided my full name.

Thank you!

 Would Remediate  
Aug 7, 2024, 2:47pm EDT

**Campaign Activities**

-  Received Emails  
81 Recipients
-  Forwarded by User  
No Recipients
-  Replied to Message  
1 Recipient

**UNUSUAL SENDER**

The email exhibits suspicious sending behavior: Abnormal Security has rarely ever seen the email address [REDACTED].edu sending to your organization.

## Attack Breakdown

### Job Scam

#### PAYLOAD

- JPG image featuring instructions to text users' names to malicious number

#### TECHNIQUE

- Compromise another student's account at a different university
- Attach custom image with the job scam itself
- Get users outside of email where there aren't security controls
- Spray and Pray

### Why does it evade traditional security?

1. University Domain passes sender authentication checks
2. Threat intelligence and known-bad solutions like M365 and Google cannot flag a JPG image without any malicious software/content

# Internal ATO - Job Scam

Subject: Seeking adm. asst \$21.65-\$24.35/hr to start + benefits

Sender: [REDACTED].edu>

Recipient: [REDACTED].edu>

Dear Students, Faculty and Staff,

There is a pressing need for Students, Faculty, and Staff assistants. This position is available to Students, Faculty, and Staff from any department of the institution, and consideration will be given on a first-come, first-served basis. This is a remote position that you could do after school/work.

Position P.A.: Personal Assistant & Errand Carried out.

Type: Part-Time Job

Monday- Saturday: Working Days

Weekends: (Sunday OFF)

Working Hour: 5-10 hours a week

Weekly Payment: \$500

This position will be home-based or Campus/ any location and it's a flexible part time job, you can be working from home, School, or any location. How to Apply: please copy and paste the following URL into a Web browser: (forms.gle/[REDACTED])

OR SEND YOUR RESUME TO/ send a short note of interest with your Personal email address (e.g., yahoo, Gmail, Hotmail etc.) and ~~not~~ your EDU email, including your phone number to Mrs. Adrianna [REDACTED] via [REDACTED]@gmail.com

Job Placement & Student Services



**Personal Assistant Position Offer**

It's a Flexible part-time job where you will determine your working time. All the tasks are work from home/on campus job, you don't need to travel somewhere and also you don't need to have a car to get started. It's an home base office work you can be in any location and work from your home/school. Weekly pay is \$500 and the fund will be inform of a (Cashier Check).

**JOB RESPONSIBILITIES MAY INCLUDE, BUT NOT LIMITED TO:**

- \* Rin business or personal errands and perform general administrative tasks.
- \* Make travel arrangements on my behalf.
- \* Sending gifts to clients as needed.
- \* Donating 5% of my monthly profits to charity every month.
- \* Paying strict attention to detail and takes detailed notes.
- \* Filing, organizing, Some Internet research, email archive research, organizing correspondence, answering calls, organizing calendars, etc.

All fields with an asterisk are required. Your application will be eligible only if all required form fields have been completed.

Accedi a Google per salvare i risultati raggiunti. Scopri di più

\* Indica una domanda obbligatoria



Would Remediate

Aug 8, 2024, 8:36pm EDT

477 Opens

8 Forwards

2 Replies

## Campaign Activities

Received Emails  
2330 Recipients

Forwarded by User  
8 Recipients

Replied to Message  
2 Recipients

Abnormal Security has detected this as a possible Email Account Takeover attack for the following reasons:

### UNUSUAL SENDER

The email exhibits suspicious sending behavior: the sender uses language which is attempting to engage, but Abnormal Security has rarely ever seen the email address [REDACTED] sending to your organization.

### ABNORMAL RECIPIENT PATTERN

All the recipients were BCC'd, a common pattern when attackers send similar attacks to many recipients.

### UNUSUAL SENDER DOMAIN

Sender domain does not match any domains found in body links.

### SUSPICIOUS FINANCIAL REQUEST

Email appears to be a financial request, but the message body contains language that may be trying to steal money from your organization.

## Attack Breakdown

### Internal Account Takeover

#### PAYLOAD

- Google Forms link serving as credential/info harvesting site

#### TECHNIQUE

- Compromise student's account at a college
- Write compelling text to convince other students at the college to "apply" for the "job posting"
- Leverage Google forms link to capture user credentials
- Spray and Pray - Send to thousands and see who falls for it

### Why does it evade traditional security?

- Traditional email security typically isn't scanning internal to internal traffic
- Threat intelligence and known-bad solutions like M365 and Google cannot flag a known-good link from Google

# Internal ATO - Credential Phishing

Subject: LAST WARNING TO ALL STUDENTS & STAFF OF UNIVERSITY OF  
 Sender: [redacted].edu>  
 Recipient: [redacted].edu>  
 Aug 6, 2024, 6:20pm EDT

597 Opens  
 45 Forwards  
 24 Replies

### Campaign Activities

- Received Emails  
2315 Recipients
- Forwarded by User  
45 Recipients
- Replied to Message  
24 Recipients

Dear Staff/Student,

Renovation on our Servers and Administrative Software will take place. We are excited about the new capabilities and services we will be able to offer students

Our records indicate that your office 365 has two different logins with two different school portals. Kindly indicate the two info logins as soon as possible. To avoid termination of the two school portals within 24hrs, we expect you to strictly adhere and address this.

We will process your termination request shortly; You will lose all your emails associated with this account

If you have only one college account, fill in the correct username and passcode and submit.  
 Notice: Your email and password are protected.

If you have no knowledge about the request process, kindly update to cancel the request below.

Copy and paste the URL Below into the address bar of your web browser to cancel the request.  
[\(CLICK HERE\)](#)

Sincerely!  
 IT Help Desk

This site was designed with the WIX.com website builder. Create your website today. [Start Now](#)

## OFFICE 365 LOGIN FOR

We Notice that your office 365 has two different logins with two universities portal. Kindly indicates the two info logins as soon as possible. To avoid termination within 24hrs, we expect you to strictly adhere and address it. Failure to Verify will result to closure of your account.

[Redacted]

Full Name (Required)

Read this Information Carefully before you Move to Next Line. If You have attended Any Universities / College Before Enrolling to [Redacted] (YES/NO)

If Yes, Name of Other's Universities / College You have Attended Before

Kindly provide the Office 365 user email associated with the universities or colleges you have attended before

Kindly provide the Office 365 user password associated with the universities or colleges you have attended before (Password Encrypted)

Abnormal Security has detected this as a possible Email Account Takeover attack for the following reasons:

**ABNORMAL RECIPIENT PATTERN**  
 All the recipients were BCC'd, a common pattern when attackers send similar attacks to many recipients.

**UNUSUAL SENDER**  
 [Redacted] suspicious sending behavior: Abnormal Security has rarely ever seen the email address [Redacted] sending to your organization.

**UNUSUAL SENDER DOMAIN**  
 Sender domain does not match any domains found in body links.

**PERSONAL INFORMATION THEFT**  
 The email body contains language that may be trying to steal personal information.



## Attack Breakdown

### Internal Account Takeover

#### PAYLOAD

- Wix link serving as credential/info harvesting site

#### TECHNIQUE

- Compromise Student's account at large higher-ed institution
- Inform users of an IT migration and that all access will be lost if they don't interact with the link
- Develop and host attack on custom-branded Wix site with institution logos to build trust


### Why does it evade traditional security?

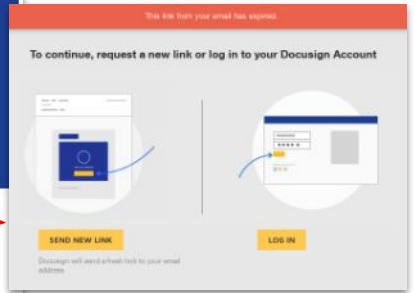
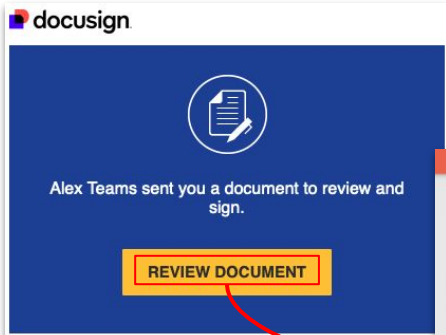
- Traditional email security typically isn't scanning internal to internal traffic
- Threat intelligence and known-bad solutions like M365 and Google cannot flag a known-good link from Wix

# Callback Scam (BazarCall)

Subject: \_Invoice# INV-28018291-Geeks Computer +1 810 [redacted]  
Sender: Alex [redacted] via DocuSign <dse\_na4@docuSign.net>  
Recipient: [redacted]@utk.edu>  
Reply-to: Alex [redacted]@googlemail.com>

Sender Domain  
docuSign.net  
  
Sender Authentication  
SPF: PASS  
DKIM: PASS  
DMARC: PASS

 Would Remediate  
Jul 25, 2024, 9:04am EDT  
  
Would Remediate by Abnormal Security  
Email in inbox



Alex [redacted]  
alexander.[redacted]@googlemail.com  
  
Dear Customer,  
  
Your invoice# INV-28018291 for 359.99 USD is attached towards renewal of 3 Years Membership.  
  
Customer Service for the USA & Canada +1 810 406 [redacted]  
  
Best\_Buy\*Geek\_Squad®- 2 Years Membership (Amount: 359.99 USD, Quantity: 1)  
Total: 359.99 USD

Scam Call Center



## Attack Breakdown

### Callback Scam (BazarCall)

#### PAYLOAD

- Fraudulent docuSign invoice featuring callback number to scam call center

#### TECHNIQUE

- Delivery of attack through legitimate invoicing service, DocuSign
- Deceive end user into calling the provided phone number
- Call leads to Credit Card/Financial Theft or Malware

### Why does it evade traditional security?

1. DocuSign Domain passes sender authentication checks
2. Link from DocuSign is a known-good link, bypassing threat intelligence checks

# Student Loan Callback Scam

Subject: [REDACTED]  
Sender: Austin Griffin <jason.[REDACTED]@hotmail.com>  
Recipient: [REDACTED].edu>  
To: [REDACTED].edu>  
Oct 3, 2024, 2:03am EDT

Scam Call Center



[REDACTED] It's Austin Griffin with the Student Loan Debt Department. This is regarding your case number 36638. We tried to contact you at your home [REDACTED] and did not hear back. Your StudentLoans have been flagged as possibly eligible for forgiveness under the new 2024 guidelines. Your file will remain open in my system for only one more day. Please give me a call on Thursday at: (888) [REDACTED] We can take your call between the hours of 8am-5pm(PST) Monday-Friday. Thank you, - Austin Griffin



Would Remediate  
Oct 3, 2024, 2:03am EDT

Would Remediate by Abnormal Security

Oct 3, 2024, 9:30am EDT

I thought those were spams! I also work for a nonprofit that was eligible for forgiveness but the Supreme Court crushed that option!  
Thank you. I will be in touch today!!! 8am pst

## Attack Breakdown

### Callback Scam

#### PAYLOAD

- Callback number and enticing message encouraging user to interact with the malicious number

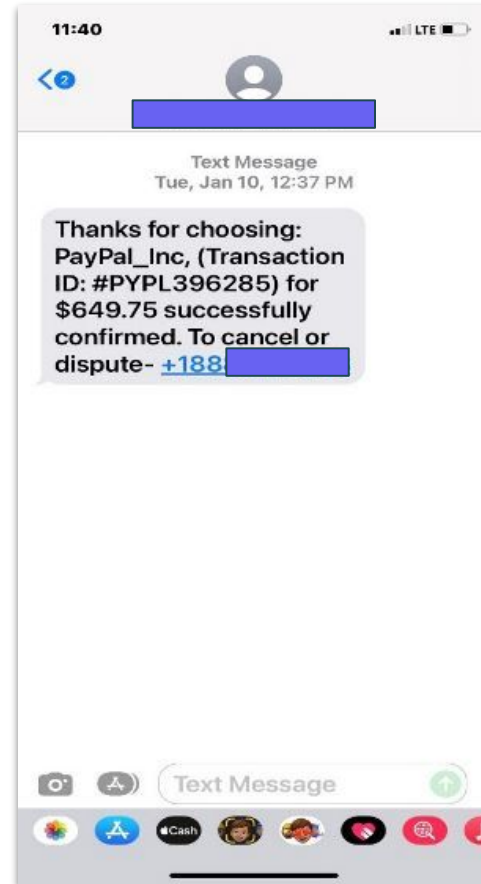
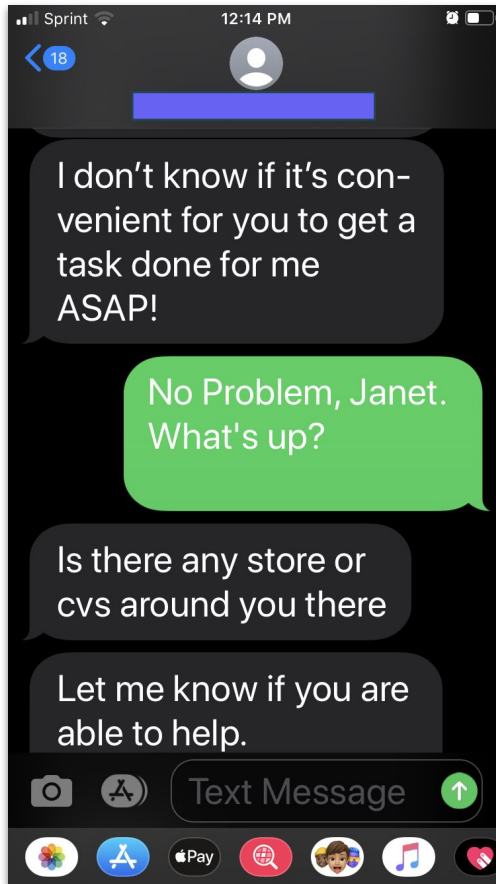
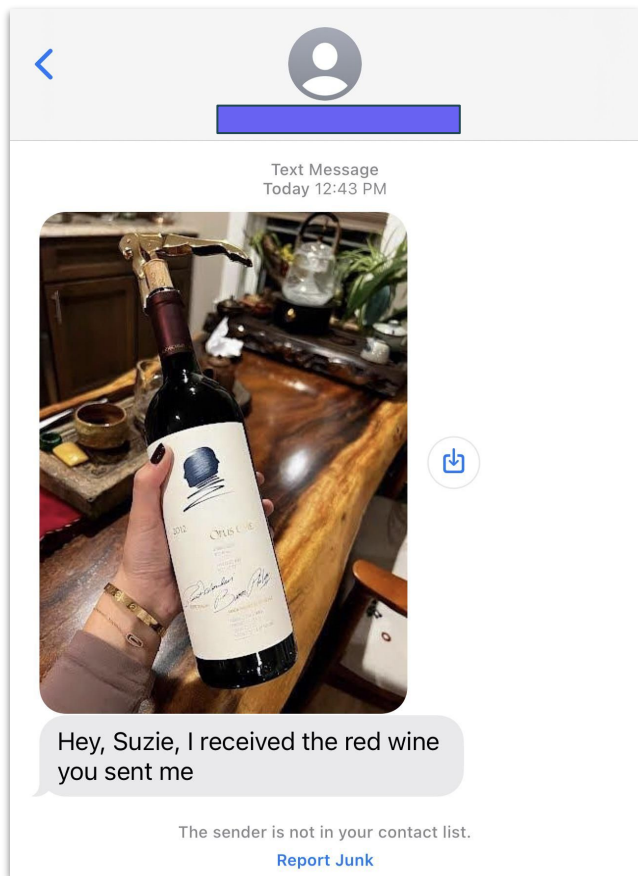
#### TECHNIQUE

- Deliver attack from hotmail account
- Frame attack as a claim for student loan forgiveness
- Attach callback number so that users can "claim" SL forgiveness
- Call leads to financial loss or malware installation

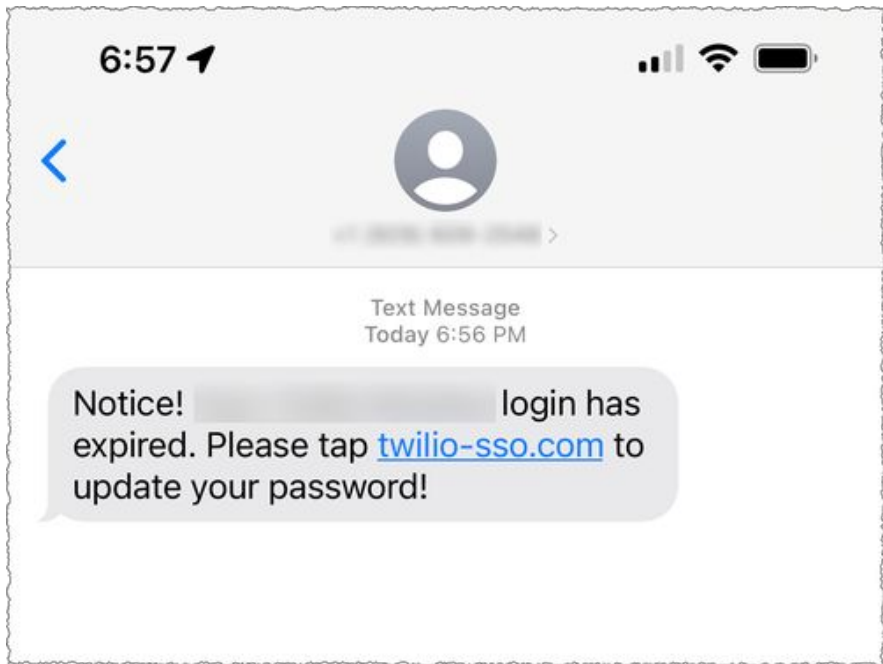
### Why does it evade traditional security?

1. Attack arrives from neutral hotmail account which doesn't fail sender authentication
2. No links or attachments included with the attack, nothing threat intelligence can identify with this attack

# Besides Email, How Else are Attackers Trying to Phish You?



# Real World SMS Phishing Attack that Led to Wide Scale Breach



## DATA BREACHES

# Twilio Confirms Data Breach After Hackers Leak 33M Authy User Phone Numbers



# What you can do to protect yourselves against phishing attacks, account compromises, or financial loss

- Trust your training, if your gut is questioning the message, don't engage with it further
- Report possible phishing attempts to the proper phishing mailbox at your school
- Utilize Multi-Factor Authentication for not just your school accounts, but also your personal accounts
- Leverage password vaults from 3rd Parties like 1Password or built-in keystores from Apple and Android
- Be open to stronger, more secure authenticators for personal use such as Passkeys
- Always double-check the URL that you're redirected to from email or SMS
- Delete and Report any texting scams or unwanted outreach as junk



# Q+A

# Thank You!