PHISHING

Joshua Annis

Cyber Security Operations Engineer

University System Of New Hampshire

AGENDA

Introduction

What is Phishing?

Facts and Statistics on Phishing

Techniques used by Phishers

Attack Surfaces/ Vectors

Examples of Phishing Attack

Summary

What you can do to protect yourself

Q&A

INTRODUCTION

Hi, my name is Joshua Annis , I'm a Cyber Security Operations Engineer for USNH. I have worked in the IT field for the last 7 years and plan to use my experience and knowledge to help protect and aid USNH employees in their day to day.

WHAT IS PHISHING?

Phishing is a type of social engineering where an attacker sends a fraudulent (e.g., spoofed, fake, or otherwise deceptive) message designed to trick a person into revealing sensitive information (passwords, maiden names, SS numbers) to the attacker. Phishers will also try to get a monetary payment (gift cards, wire transfers or fake invoices for services) or attempt to deploy malicious software on the victim's computer like ransomware or keyloggers.

PHISHING STATISTICS AND FACTS

Here are some general facts and statistics about phishing that speak to how common and effective phishing attacks can be:

- Approximately one in every 99 emails you receive will be a phishing attempt
- 90% of data breaches occur due to phishing
- Companies reported that as a result of a successful phishing attack 31% of affected users result in a compromised password and another 28% had exposure to ransomware
- IBM's 2021 Cost of Data Breach Report found phishing to be the second most expensive attack vector costing organizations an average of 4.65 Million dollars

TECHNIQUES USED BY PHISHERS

Knowing how phishers attack is critical as it will aid in your ability to detect attacks on your own. Some of these Techniques being used are …

Link Manipulation

Some links are manipulated to look like a link or page you are familiar with but will redirect you to a fake or malicious website

Filter Evasion

Some emails will be crafted to be pictures of text, this is to avoid being caught by spam/ phishing filters that would typically block the email

Social Engineering

Most phishing attempts involve social engineering to some extent to gain your trust or play off your emotions.

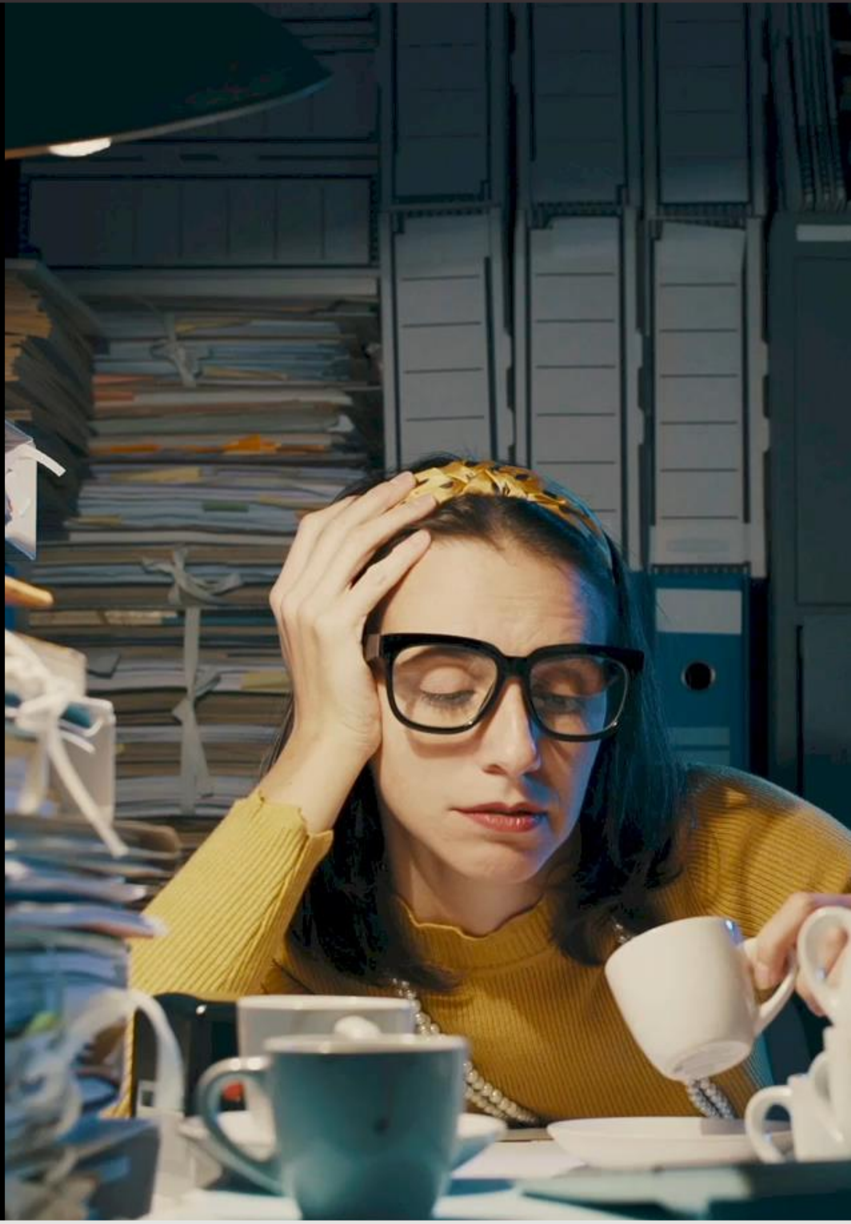
STATE OF MIND

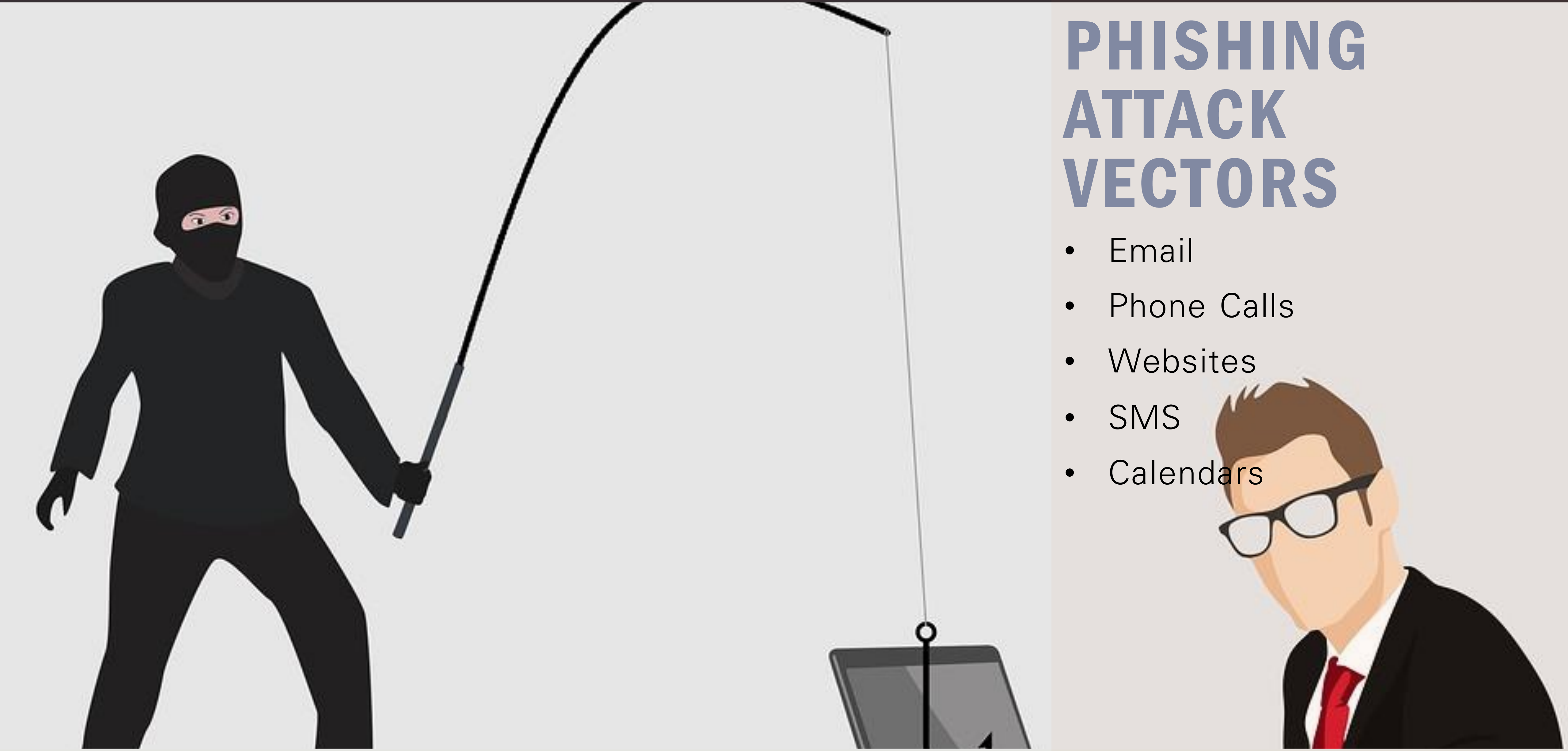
Most phishing attempts will try to affect or use your state of mind to their advantage, Oftentimes phishing attempts will try to incite a..

- Feeling of Urgency
  - They will incite a sense of urgency to encourage you to not think twice
- Feeling of Fear
  - Make you feel fear about something such as missing an important payment or having your account compromised

Other phishing attempts will try to catch you when your guard is down. Typically, when..

- You're Tired or Overworked or during off hours
  - Often phishers will try to catch you at times when you are off-guard. They will send emails out super early in the morning or late at night when you can't be bothered or are unable to contact IT.





PHISHING ATTACK VECTORS

- Email
- Phone Calls
- Websites
- SMS
- Calendars

EMAIL PHISHING

There are 3 main kinds of email phishing attempt. These being,

Spear Phishing

Attackers will directly contact a specific person that they have made a tailored email for to make it appear like a its normal request you typically get. These attacks are typically geared towards hire up or someone in charge of finances due to their ability to move money.

Whaling and CEO Fraud

Whaling attacks are geared to aim for high profile targets to and might have information interesting to the target.

CEO Fraud are typically spoofed or fake outside accounts that uses the CEO's role of power to that send emails to people within a company to get money or information sent.

Clone Phishing

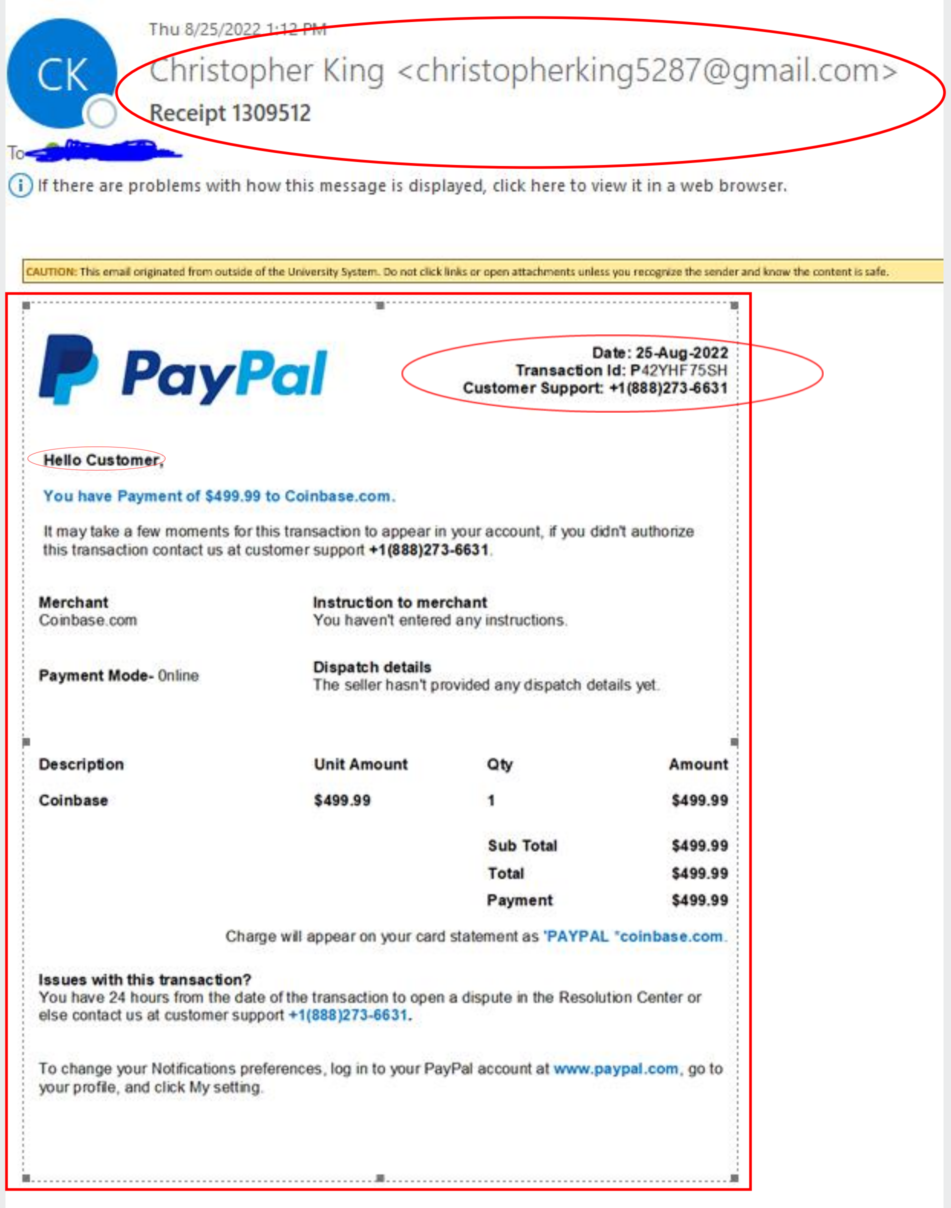
These are typically crafted emails to appear near identical to legitimate emails from companies like amazon, but these emails have false company info and fake links redirect you to a page that either give the phishers information they want or money for services or invoices that are not legitimate.

EXAMPLE

This example was extracted From USNH's email server. The Phishers used filter evasion to try to evade our safeguards ,but fortunately our system detected some questionable URLs within the message causing this message to be flagged in our system.

Not all emails can be detected and blocked. Here are some red flags to keep an eye out for…

- The From email is obviously from a generic Gmail account, this is supposed to be an email from PayPal right?
- Ambiguous "Hello Customer", Typically a bill or invoice will be directed to a specific person or address or department
- Oddly bolded letter / typo
- The "Text" in this email is a picture



Thu 8/25/2022 1:12 PM

Christopher King <christopherking5287@gmail.com>

Receipt 1309512

To [redacted]

ⓘ If there are problems with how this message is displayed, click here to view it in a web browser.

CAUTION: This email originated from outside of the University System. Do not click links or open attachments unless you recognize the sender and know the content is safe.

Date: 25-Aug-2022
Transaction Id: P42YHF75SH
Customer Support: +1(888)273-6631

Hello Customer,

You have Payment of $499.99 to Coinbase.com.

It may take a few moments for this transaction to appear in your account, if you didn't authorize this transaction contact us at customer support **+1(888)273-6631**.

Merchant
Coinbase.com

Instruction to merchant
You haven't entered any instructions.

Payment Mode- Online

Dispatch details
The seller hasn't provided any dispatch details yet.

Description	**Unit Amount**	**Qty**	**Amount**
Coinbase	**$499.99**	**1**	**$499.99**
		Sub Total	**$499.99**
		Total	**$499.99**
		Payment	**$499.99**

Charge will appear on your card statement as 'PAYPAL "coinbase.com.

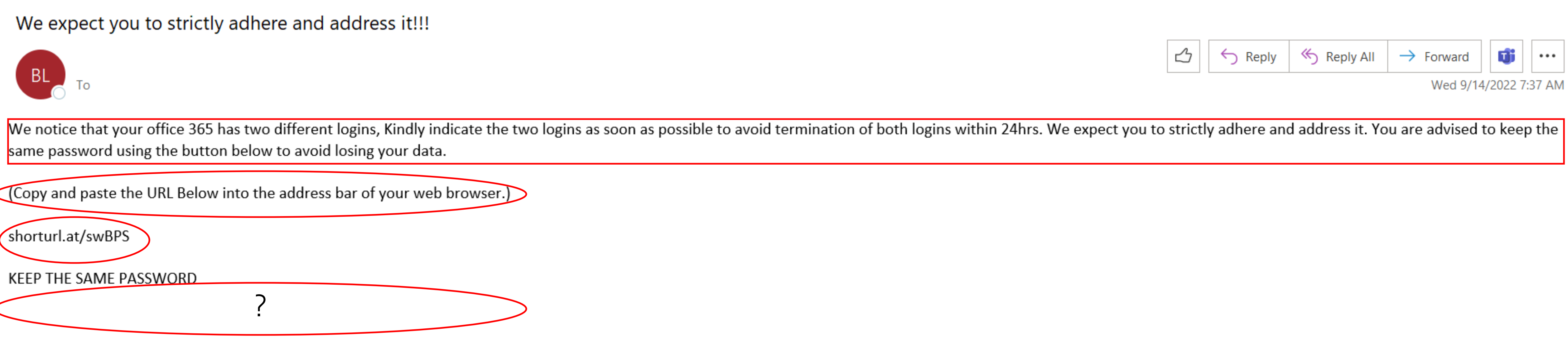
Issues with this transaction?
You have 24 hours from the date of the transaction to open a dispute in the Resolution Center or else contact us at customer support +1(888)273-6631.

To change your Notifications preferences, log in to your PayPal account at www.paypal.com, go to your profile, and click My setting.

EXAMPLE

Here is another example of an email extracted from USNH’s system. This was a spear phishing email sent from a compromised USNH account and was spear fishing employees’ emails. Phishing emails sent from an internal address can be harder to spot as they will not include the same caution header that is put on all incoming emails from outside addresses. Some things to lookout for are:

- Oddly worded message /tasks
- Non USNH links, this is also using a form of filter evasion not including a hyperlink to avoid flagging
- No official USNH/UNH Signature



We expect you to strictly adhere and address it!!!

To

Wed 9/14/2022 7:37 AM

We notice that your office 365 has two different logins, Kindly indicate the two logins as soon as possible to avoid termination of both logins within 24hrs. We expect you to strictly adhere and address it. You are advised to keep the same password using the button below to avoid losing your data.

(Copy and paste the URL Below into the address bar of your web browser.)

shorturl.at/swBPS

KEEP THE SAME PASSWORD

?

PHONE CALLS/ VOICE PHISHING

Phishing takes many forms, email is not the only medium used for these scams. Phone scams / Voice Phishing are just as common as email scams and account for 39.5 billion dollars lost by Americans in 2021 alone.

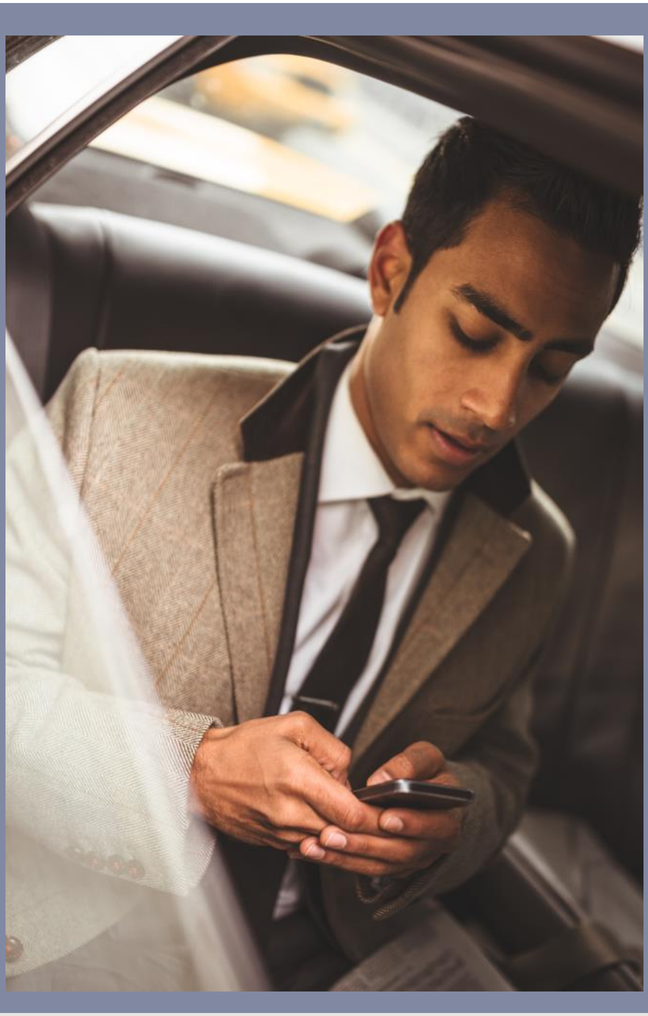
Some of the calls are as simple as the infamous “Your car's extended warranty has expired” or the “You’ve been selected to win $10,000, press 1 to continue”, but voice phishing has started using deep fake technology to dupe CEO’s into sending a quarter of a million dollars to a fraudster's bank account.

EXAMPLES

Fake IRS Call 🔊

Fake Discount 🔊

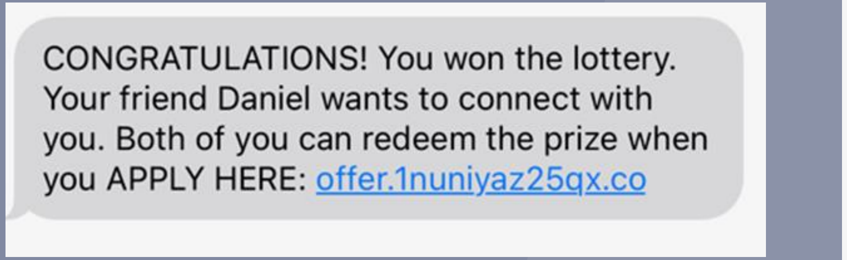
SMS / TEXT MESSAGES



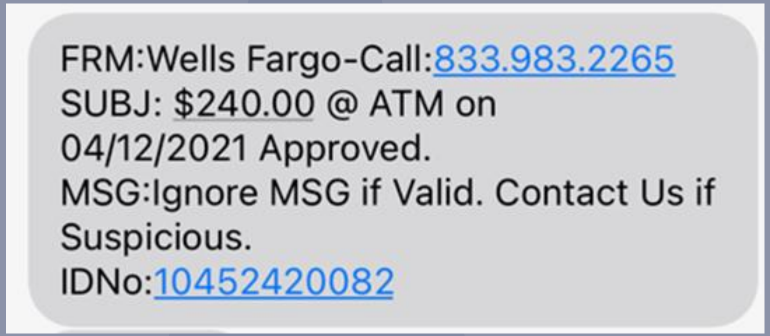
With the rapid expansion of MFA and automated messages that you are typically used to getting ,fake SMS messages are becoming more and more popular today. It’s important to always be cautious when receiving texts with links. Many of the links received are malicious and either will try to redirect you into setting up fake calendar events or redirect you to fake Web page tailored to mirror your banks, these fake pages can be used to gather logon information and steal identities.

EXAMPLES

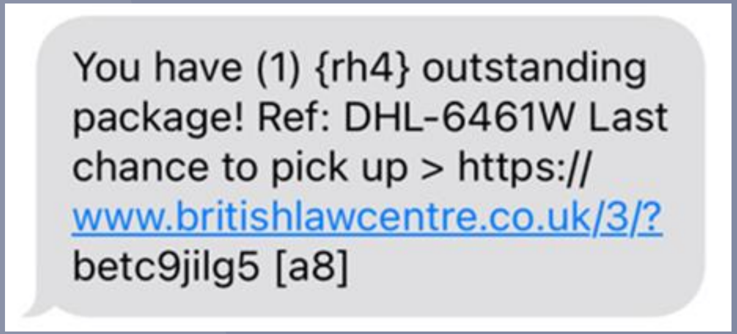
Here are a few examples of some of the phishing texts that are being sent these days. The best thing to do in this scenario is to ignore the message and block this number from ever texting you again in the future.



CONGRATULATIONS! You won the lottery. Your friend Daniel wants to connect with you. Both of you can redeem the prize when you APPLY HERE: offer.1nuniyaz25qx.co



FRM:Wells Fargo-Call:833.983.2265
SUBJ: $240.00 @ ATM on 04/12/2021 Approved.
MSG:Ignore MSG if Valid. Contact Us if Suspicious.
IDNo:10452420082



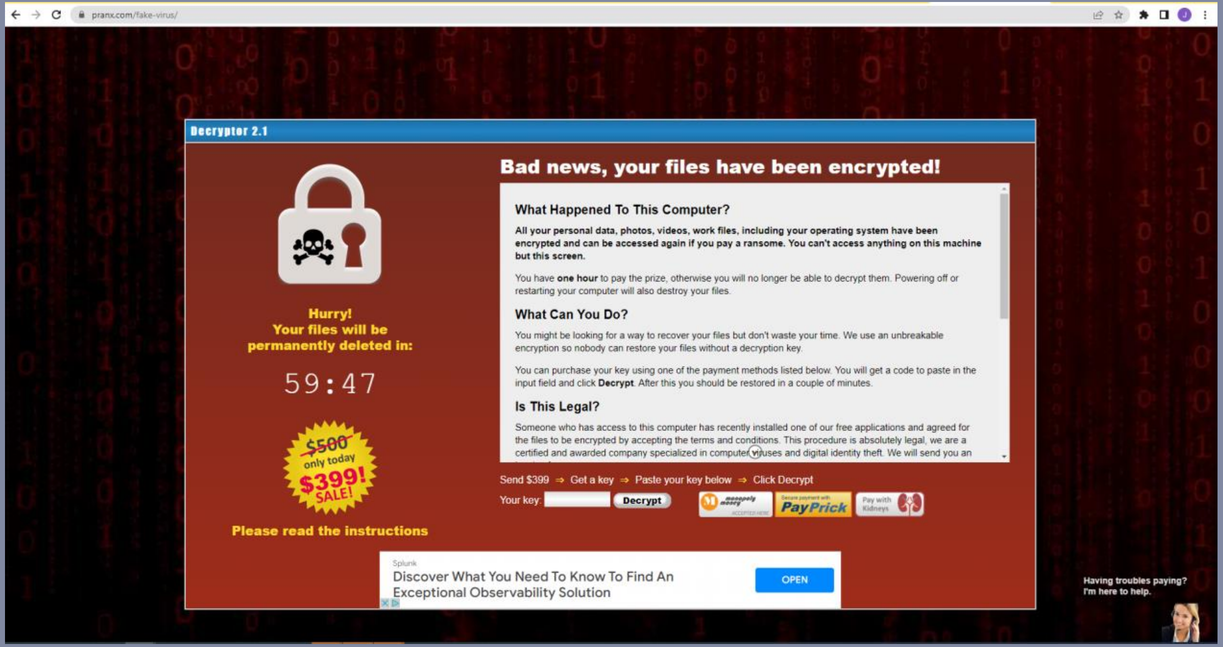
You have (1) {rh4} outstanding package! Ref: DHL-6461W Last chance to pick up > https://www.britishlawcentre.co.uk/3/?betc9jilg5 [a8]

WEBSITES

Apart from links that are sent to you via Email or SMS, you may also encounter popups or link/browser hijacking while surfing the internet.

Some of these scams will redirect you to a page that will make it appear as if you have a virus on your computer or redirect you to a page that looks near identical to the one you are attempting to go to.

It's important that when you encounter such a site, to close out of the tab you are currently on. You should refrain from clicking anywhere on these site, as clicking anywhere could open other malicious links or initiate unwanted downloads.



pranx.com/fake-virus/

Decryptor 2.1

Hurry!
Your files will be permanently deleted in:

59:47

~~$500~~ only today $399! SALE!

Please read the instructions

Bad news, your files have been encrypted!

What Happened To This Computer?

All your personal data, photos, videos, work files, including your operating system have been encrypted and can be accessed again if you pay a ransome. You can't access anything on this machine but this screen.

You have **one hour** to pay the prize, otherwise you will no longer be able to decrypt them. Powering off or restarting your computer will also destroy your files.

What Can You Do?

You might be looking for a way to recover your files but don't waste your time. We use an unbreakable encryption so nobody can restore your files without a decryption key.

You can purchase your key using one of the payment methods listed below. You will get a code to paste in the input field and click **Decrypt**. After this you should be restored in a couple of minutes.

Is This Legal?

Someone who has access to this computer has recently installed one of our free applications and agreed for the files to be encrypted by accepting the terms and conditions. This procedure is absolutely legal, we are a certified and awarded company specialized in computer viruses and digital identity theft. We will send you an

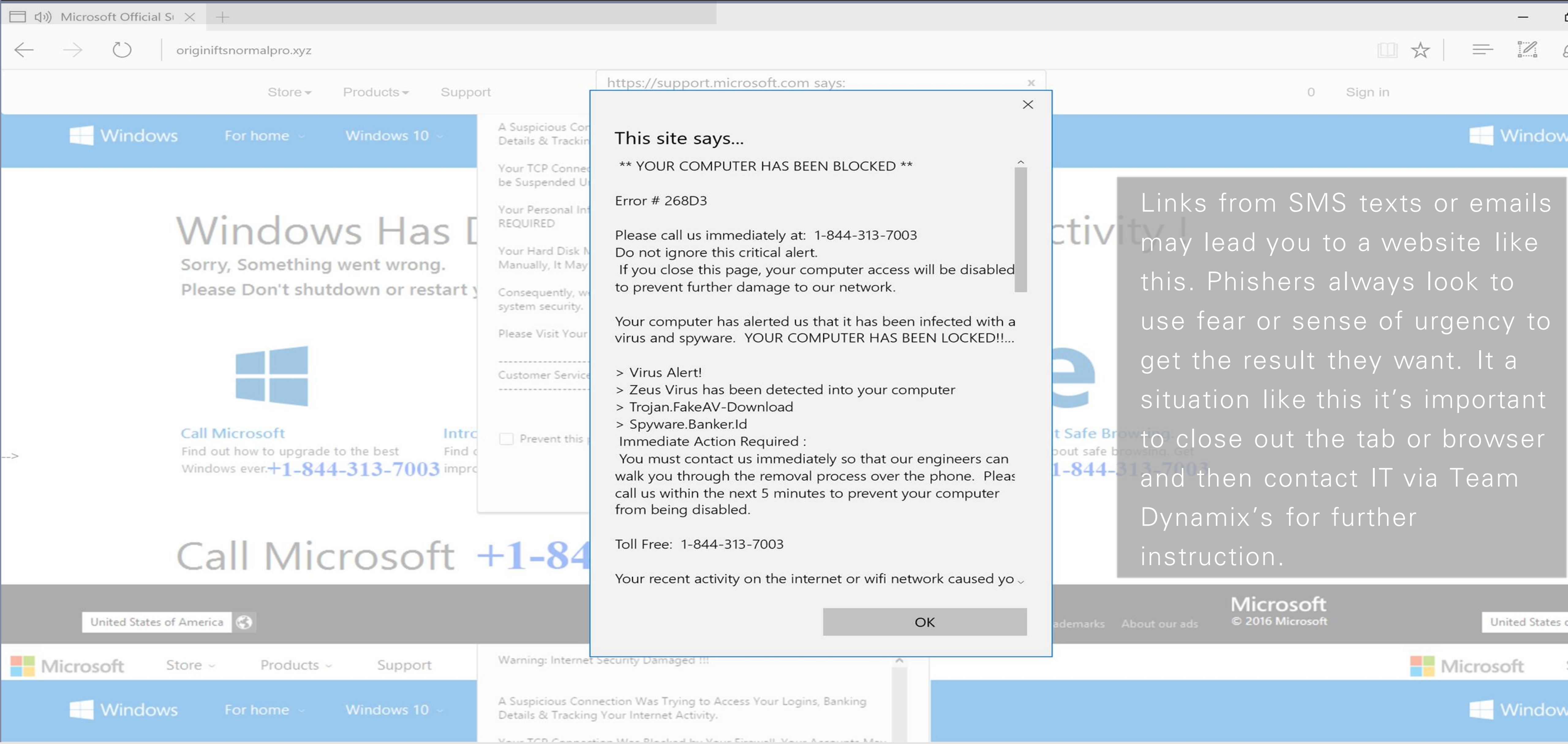
Send $399 ⇒ Get a key ⇒ Paste your key below ⇒ Click Decrypt

Your key:

Splunk
Discover What You Need To Know To Find An Exceptional Observability Solution

Having troubles paying?
I'm here to help.

EXAMPLE


Microsoft Official S
originiftsnormalpro.xyz
Store
Products
Support
Sign in
Windows
For home
Windows 10
Windows Has
Sorry, Something went wrong.
Please Don't shutdown or restart y
Call Microsoft
Find out how to upgrade to the best Windows ever.+1-844-313-7003
Call Microsoft +1-84
https://support.microsoft.com says:
Prevent this
United States of America
Microsoft
© 2016 Microsoft
About our ads
Warning: Internet Security Damaged !!!
A Suspicious Connection Was Trying to Access Your Logins, Banking Details & Tracking Your Internet Activity.

This site says...

** YOUR COMPUTER HAS BEEN BLOCKED **

Error # 268D3

Please call us immediately at: 1-844-313-7003
Do not ignore this critical alert.
If you close this page, your computer access will be disabled to prevent further damage to our network.

Your computer has alerted us that it has been infected with a virus and spyware. YOUR COMPUTER HAS BEEN LOCKED!!...

> Virus Alert!
> Zeus Virus has been detected into your computer
> Trojan.FakeAV-Download
> Spyware.Banker.Id
Immediate Action Required :
You must contact us immediately so that our engineers can walk you through the removal process over the phone. Pleas call us within the next 5 minutes to prevent your computer from being disabled.

Toll Free: 1-844-313-7003

Your recent activity on the internet or wifi network caused yo

OK

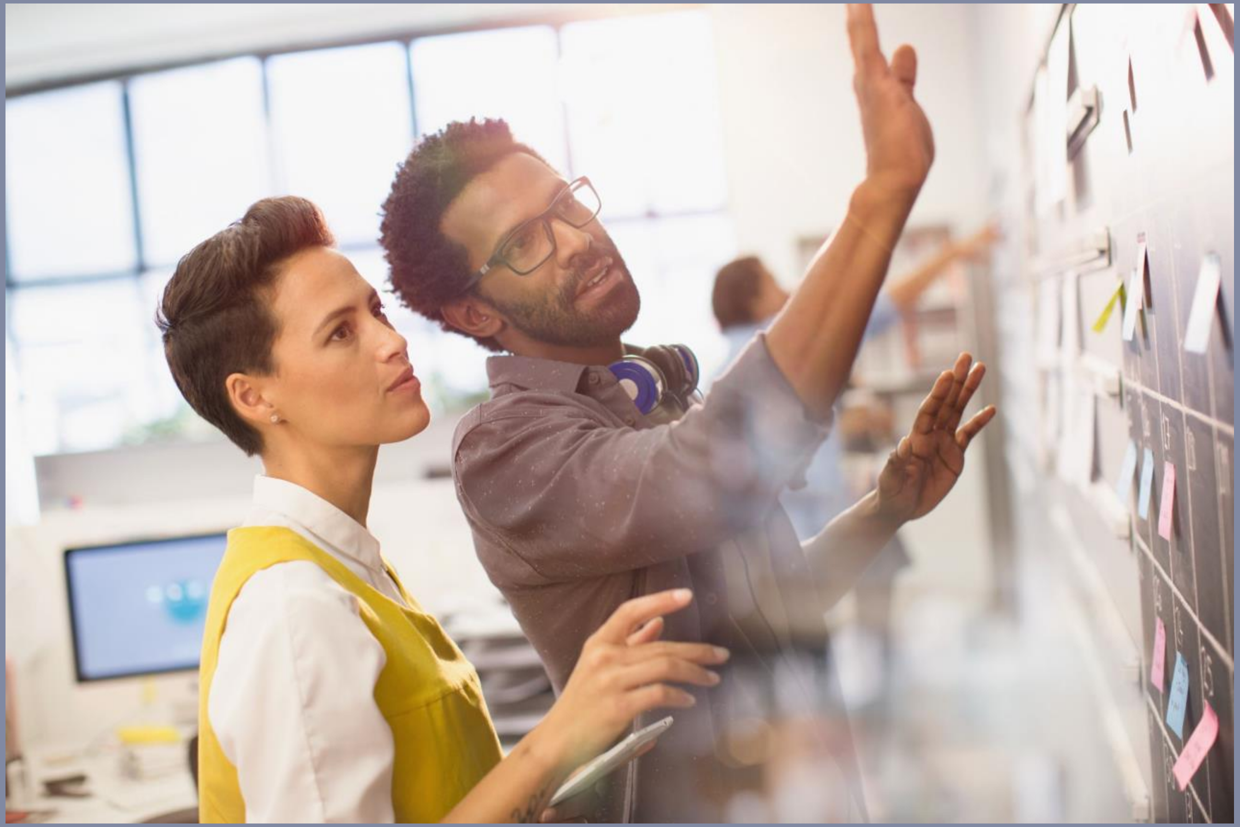
Links from SMS texts or emails may lead you to a website like this. Phishers always look to use fear or sense of urgency to get the result they want. It a situation like this it's important to close out the tab or browser and then contact IT via Team Dynamix's for further instruction.

CALENDAR

In the day of everything being digitized even Calendar events are being used as an attack surface!

Usually, these attacks will only happen if a malicious link has already been clicked on and executes a command to add an event to your calendar.

These events usually contain a malicious link or phone number or zoom links for you to call or join so they can get access to your computer.



RECAP

- A basic understanding of what phishing is
- Phishing Techniques and state of mind
  - Link Manipulation, Filter Evasion, and Social Engineering
- Various Attack Vectors and Examples
  - Email and Calendars
  - Phone (voice and text)
  - Websites

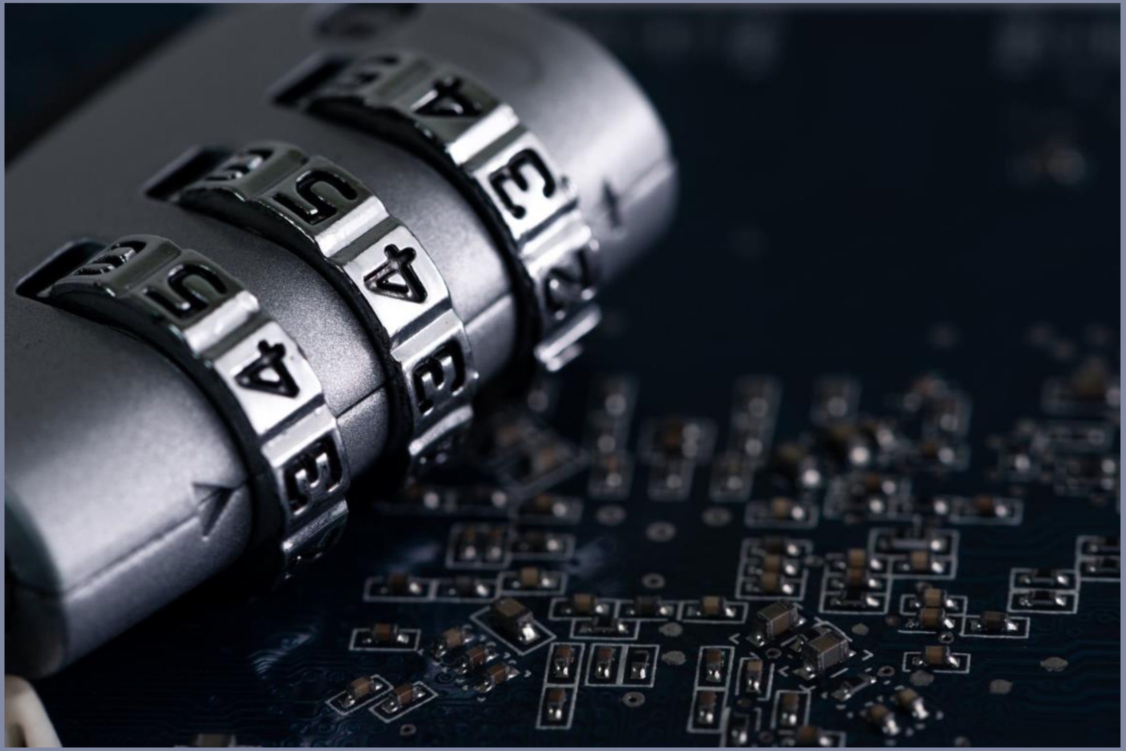
....But how am I protected?

HOW ARE YOU PROTECTED

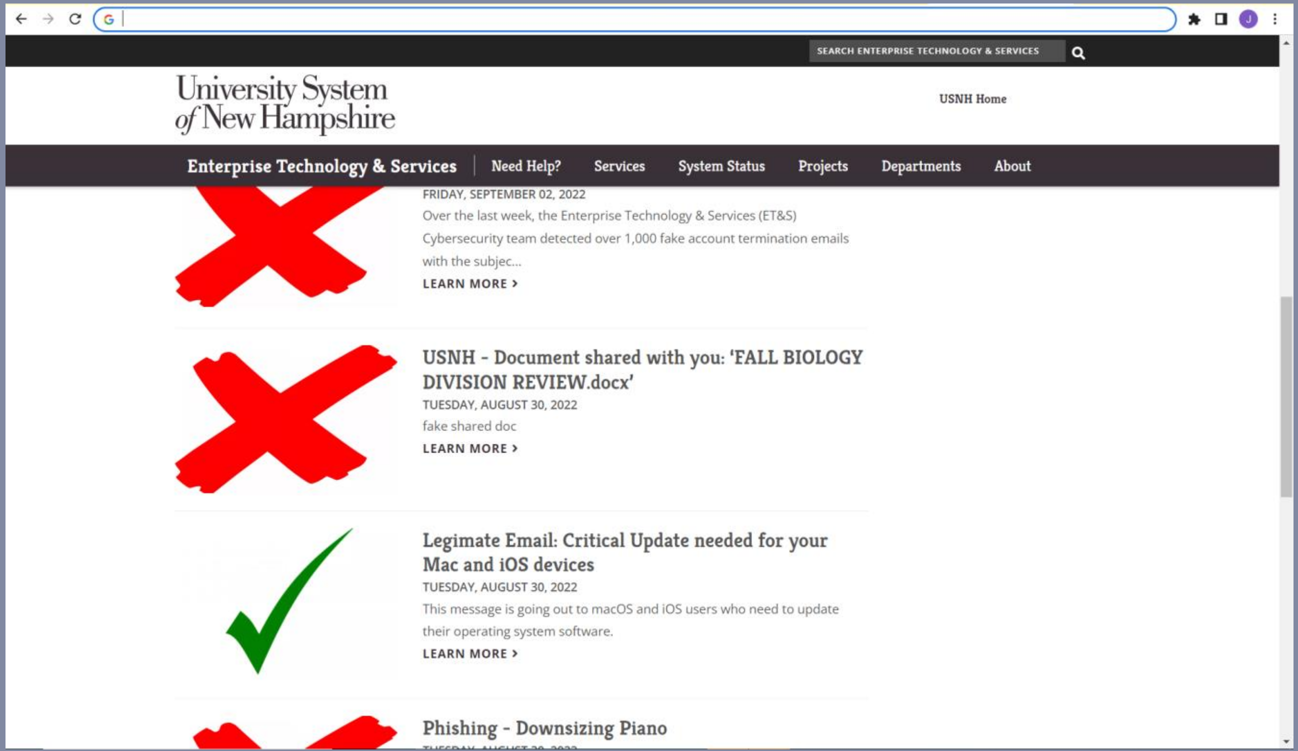
USNH has many tools at our disposal to help monitor and mitigate phishing attacks.

We primarily use Microsoft's Advanced Threat Protection for spam/ phishing email detection. In a 30 day window approximately 11.3 million emails are sent and monitored by USNH's system. Thanks to Microsoft ATP approximately 1.2 million (10.6%) emails are detected as Spam, Phishing or malware and get properly mitigated.

On top of that, we are also able to Blacklist Ip's and emails of known bad senders to help safeguard USNH students and employees from any future malicious attempts made from the same address



HOW ARE YOU PROTECTED


SEARCH ENTERPRISE TECHNOLOGY & SERVICES
University System of New Hampshire
USNH Home
Enterprise Technology & Services
Need Help?
Services
System Status
Projects
Departments
About

FRIDAY, SEPTEMBER 02, 2022

Over the last week, the Enterprise Technology & Services (ET&S) Cybersecurity team detected over 1,000 fake account termination emails with the subjec...

LEARN MORE ›

USNH - Document shared with you: 'FALL BIOLOGY DIVISION REVIEW.docx'

TUESDAY, AUGUST 30, 2022

fake shared doc

LEARN MORE ›

Legimate Email: Critical Update needed for your Mac and iOS devices

TUESDAY, AUGUST 30, 2022

This message is going out to macOS and iOS users who need to update their operating system software.

LEARN MORE ›

Phishing - Downsizing Piano

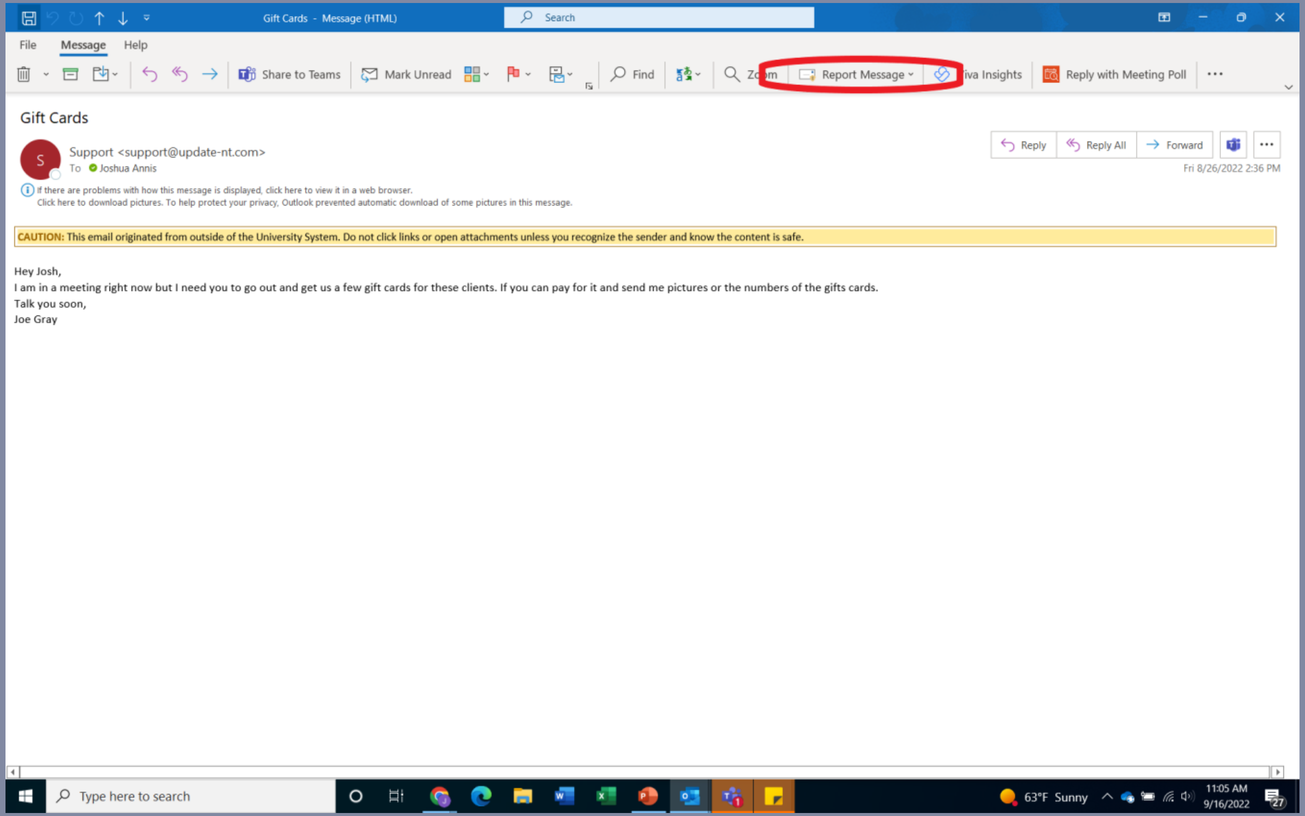
Cyber security is in a constant battle of good vs evil. Even with our best efforts in place to put up as many walls and filters to help safeguard our users , some emails will be able to dodge our roadblocks and make it through. In the end our best line of defense is YOU!

We try to spread awareness and keep people informed with the most up-to-date training and provide you with sites like USNH's Phishbowl.

The Phishbowl is a resource that cyber security provides to be as a reference and show users examples of emails that are either confirmed legitimate or spam/phishing.

HOW ARE YOU PROTECTED

If you are ever questioning the legitimacy of an email, please hit the report button in the top right-hand side of outlook or forward the email to phish.alarm@usnh.edu



Gift Cards

Support <support@update-nt.com>
To Joshua Annis
Fri 8/26/2022 2:36 PM

If there are problems with how this message is displayed, click here to view it in a web browser.
Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

CAUTION: This email originated from outside of the University System. Do not click links or open attachments unless you recognize the sender and know the content is safe.

Hey Josh,
I am in a meeting right now but I need you to go out and get us a few gift cards for these clients. If you can pay for it and send me pictures or the numbers of the gifts cards.
Talk you soon,
Joe Gray

ANY QUESTIONS?

Thank you!
for making it to the end of my presentation!

I encourage you to join us for some of the other Cyber Month Presentations!

Wi-Fi Security with Matthew Reed
October 12th|11:00 AM - 12:00 PM

Splunk's Boss of the SOC
October 13th|11:00 AM - 5:00 PM

Disinformation Campaigns with
Dr. David Yasenchock
October 18th|11:00 AM - 12:00 PM

REFERENCES

Slide 5 https://www.cybertalk.org/2022/03/30/top-15-phishing-attack-statistics-and-they-might-scare-you/

Slide 11 https://www.helpnetsecurity.com/2022/05/30/spam-phone-scams-impact/

Slide 11 https://www.forbes.com/sites/jessedamiani/2019/09/03/a-voice-deepfake-was-used-to-scam-a-ceo-out-of-243000/?sh=46c415ed2241

Slide 12 https://blog.textedly.com/spam-text-message-examples

Slide 14 https://www.digitalinformationworld.com/2019/09/google-calendar-spam-gmail.html

All Pictures, Sounds and Video were events re-created in house or were from pulled from a royalty free image repository or Microsoft's stock images/ videos