Tohono O'odham Nation

Department of Information & Technology

CYBERSECURITY AWARENESS MONTH 2022

Phishing & Malware

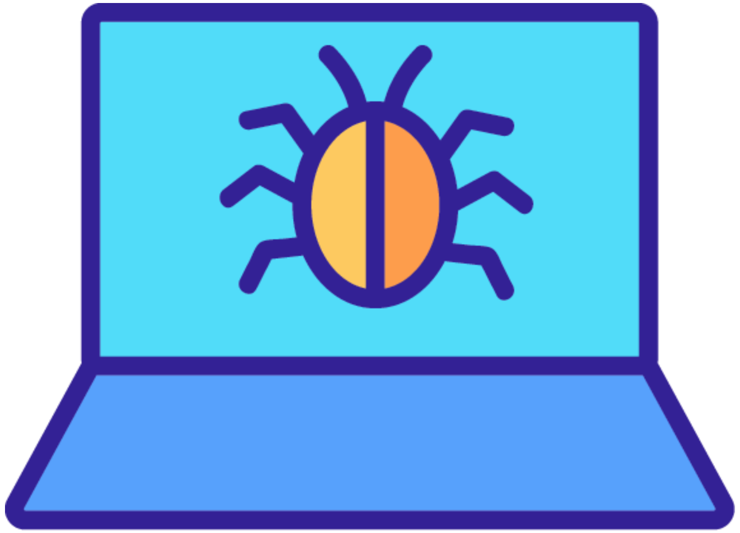
Tohono O'odham Nation
Department of Information & Technology
CYBERSECURITY AWARENESS MONTH 2022

Overview

Objectives

- Intro on Malware
  - What It Is?
  - Where Can I get it?
  - Common Types
- So Much Phishing!!!
  - What is Phishing?
  - Different Types
  - Tips on Recognizing
- How Do I Protect Myself?

What is malware?



- Malware is a catch-all term for **any type of malicious software designed to harm or exploit any programmable device, service or network.**
- It is used to harm or exploit computers and networks so that bad actors can then steal data or money
- Malware attacks are on the rise, especially in the wake of the pandemic. Malware increased 358% year over year in 2020 as the attack surface significantly increased with employees working from home.

Where can I get malware?

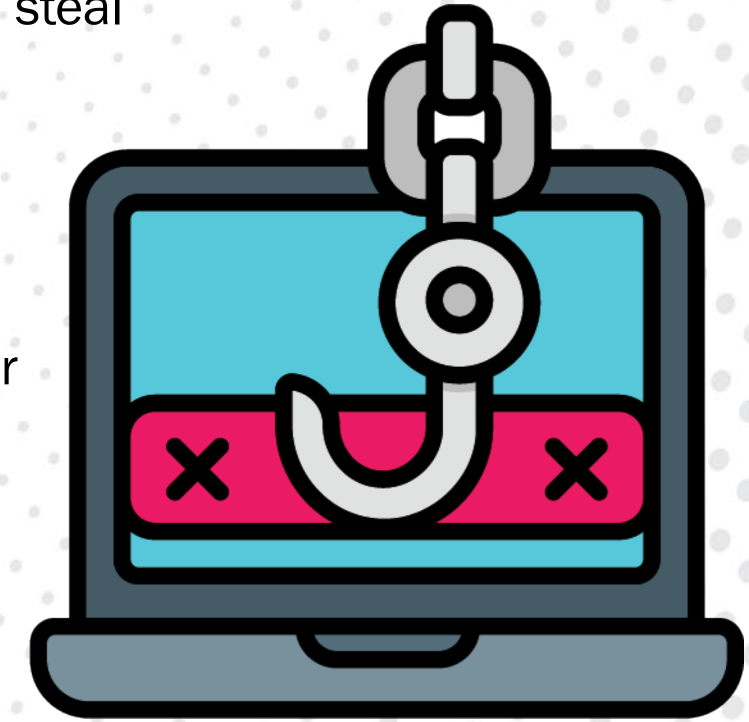
- Most of the time malware comes from compromised sites
  - Parked sites- sites closely spelled to the intended site but misspelled.
    - Gooogle.com, faccebook.com
  - Hacked legitimate sites
- Phishing
- Man in The Middle Attacks
    - Bad wi-fi access points in public places
    - It is not recommended to connect to free public access points.
- Fake Software Installations- freeware is infamous for containing malware
- Infected USB Drives- if you find a USB somewhere it may contain a virus

Common malware types

- Different types of malware
  - Viruses- malware that performs malicious action
    - Commonly a downloaded file opened by user
  - Trojans- Generally a legit application that has some type of malware inside of it.
    - Very common in freeware
  - Scareware- a pop-up or website opens and threatens you with some type of consequence if you do not install their software
  - Ransomware- a machine is encrypted (locked) by threat actor requesting payment to receive decryption key to unlock
  - Spyware- program installed without your knowledge that monitors and steals information
    - Usually form a virus attachment
  - Adware- malware that pushes advertisements to users and usually installed with freeware

Phishing

- Phishing email messages, websites, and phone calls are designed to steal money or sensitive information
    - Designed to trick you into clicking a link or providing personal or financial information
    - Often in the form of emails and websites
    - May appear to come from legitimate companies, organizations or known individuals
        - May even come from legitimate organizations
    - Take advantage of natural disasters, epidemics, health scares, political elections or timely events-
        - Covid times had a 200% increase in phishing

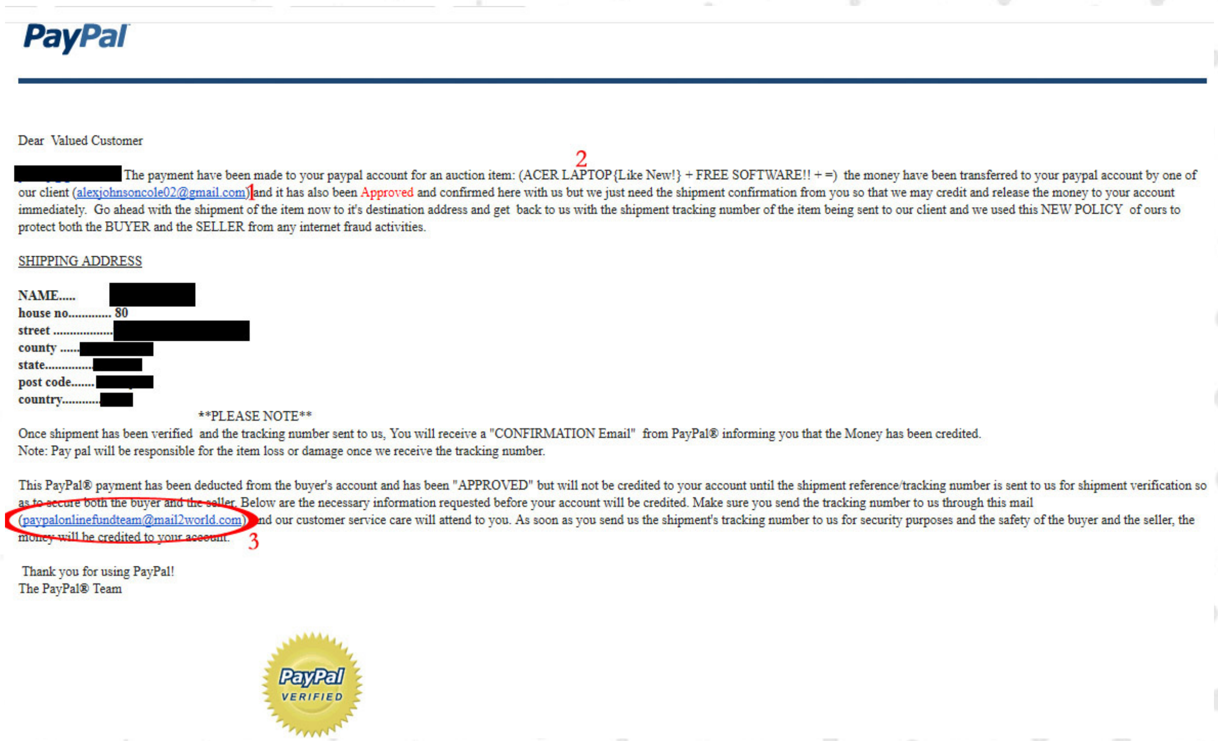


Types of Phishing

- **Spear phishing** - Phishing attempts directed at specific individuals or companies have been termed spear phishing.
  - Attackers may gather personal information (social engineering) about their targets to increase their probability of success.
  - Most successful method
- **Voice Phishing (Vishing)** - Voice phishing is the criminal practice of using social engineering over the telephone system to gain access to personal and financial information from the public for the purpose of financial reward.
  - IRS and banks are common choices to use
- **Whaling** – Type of spear phishing attack that targets “big fish,” including high-profile individuals or those with a great deal of authority or access
- **Smishing** - an attack that uses text messaging or short message service (SMS) to execute the attack. A common smishing technique is to deliver a message to a cell phone through SMS that contains a clickable link or a return phone number.
  - Very common to use bank stating your account is locked or improper withdrawals
- **Angler Phishing** - Anglers use fake social media posts to get people to provide login info or download malware.
- **Quishing** - A common tactic is to invite people to access an encrypted voice message via a QR code. The victim then uses their camera to access the QR code and open up their browser, which takes them to a phishing website.

Phishing examples

- Just like in the previous example, this email looks like a legit PayPal email that you would normally see. The first thing to do is to see if you recognize the email, or if you have done any kind of transaction with this email address. Also, look through the email for spelling and grammatical errors, as Cybercriminals will often leave these errors in the body of the email.
- Second, see if the item in question is one that you actually bought or sold. If not, delete and move on.
- Look at the email address circled, if this was an official email from PayPal, it would end in "@paypal.com" not mail2world.



Dear Valued Customer

[redacted] The payment have been made to your paypal account for an auction item: (ACER LAPTOP{Like New!} + FREE SOFTWARE!! + =) the money have been transferred to your paypal account by one of our client (alexjohnsoncole02@gmail.com) and it has also been Approved and confirmed here with us but we just need the shipment confirmation from you so that we may credit and release the money to your account immediately. Go ahead with the shipment of the item now to it's destination address and get back to us with the shipment tracking number of the item being sent to our client and we used this NEW POLICY of ours to protect both the BUYER and the SELLER from any internet fraud activities.

SHIPPING ADDRESS

NAME..... [redacted]
house no............ 80
street .... [redacted]
county ...... [redacted]
state............. [redacted]
post code....... [redacted]
country.......... [redacted]

PLEASE NOTE

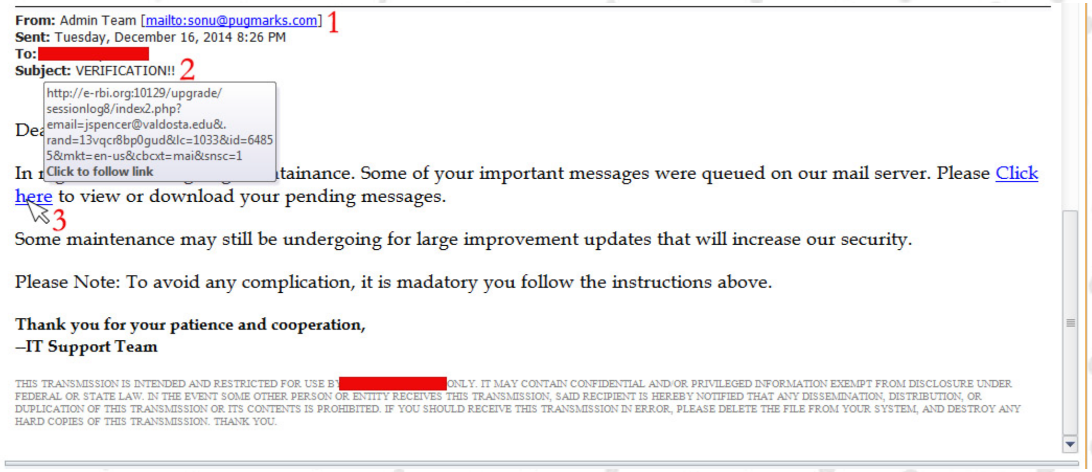
Once shipment has been verified and the tracking number sent to us, You will receive a "CONFIRMATION Email" from PayPal® informing you that the Money has been credited.
Note: Pay pal will be responsible for the item loss or damage once we receive the tracking number.

This PayPal® payment has been deducted from the buyer's account and has been "APPROVED" but will not be credited to your account until the shipment reference/tracking number is sent to us for shipment verification so as to secure both the buyer and the seller. Below are the necessary information requested before your account will be credited. Make sure you send the tracking number to us through this mail (paypalonlinefundteam@mail2world.com) and our customer service care will attend to you. As soon as you send us the shipment's tracking number to us for security purposes and the safety of the buyer and the seller, the money will be credited to your account.

Thank you for using PayPal!
The PayPal® Team

Phishing examples

- The sender is not a valid tonation-nsn.gov address, but rather a @pugmarks.com address. The name is also a generic "Admin Team" which does not match up with the email address.
- The subject line is in all capitals and using multiple exclamation marks trying to get your attention.
- **Hovering your mouse over the link**, you can see that this is not a valid valdosta.edu address, but rather an external site trying to steal your credentials or install malicious software.



From: Admin Team [mailto:sonu@pugmarks.com] 1
Sent: Tuesday, December 16, 2014 8:26 PM
To: [redacted]
Subject: VERIFICATION!! 2

http://e-rbi.org:10129/upgrade/sessionlog8/index2.php?email=jspencer@valdosta.edu&.rand=13vqcr8bp0gud&lc=1033&id=64855&mkt=en-us&cbcxt=mai&snsc=1
Click to follow link

Dea

In r tainance. Some of your important messages were queued on our mail server. Please Click here to view or download your pending messages. 3

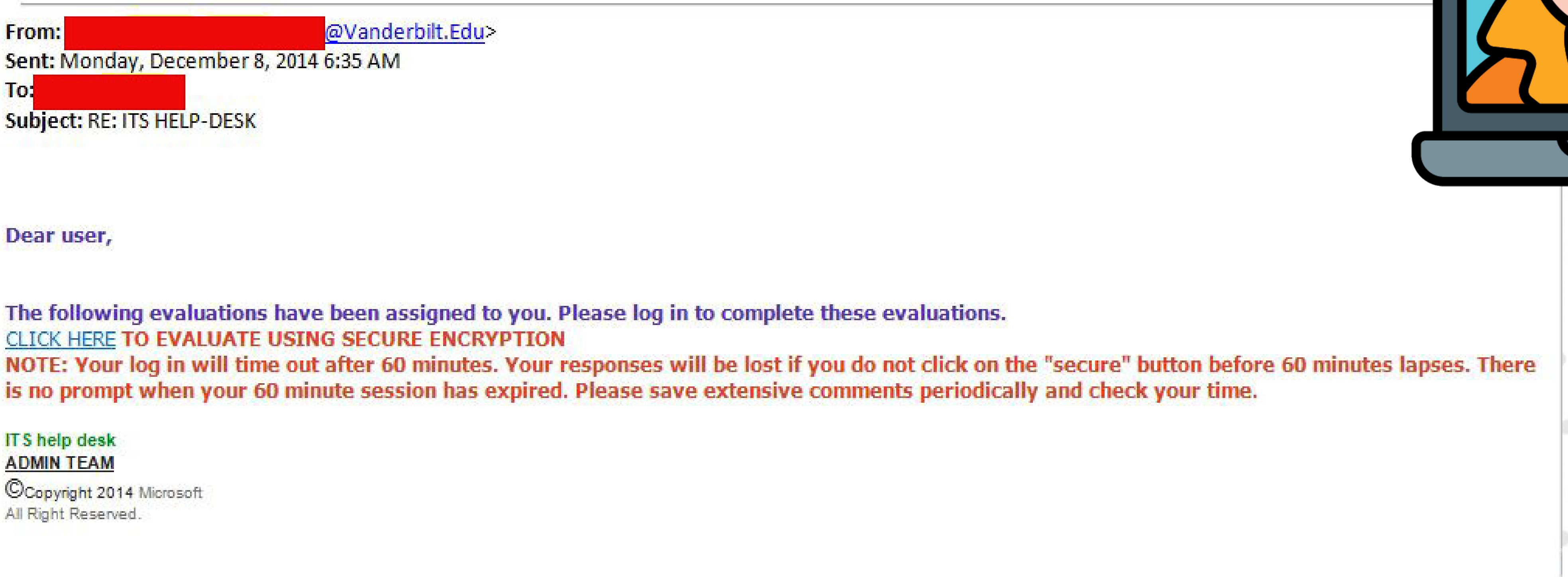
Some maintenance may still be undergoing for large improvement updates that will increase our security.

Please Note: To avoid any complication, it is madatory you follow the instructions above.

Thank you for your patience and cooperation,
–IT Support Team

THIS TRANSMISSION IS INTENDED AND RESTRICTED FOR USE BY [redacted] ONLY. IT MAY CONTAIN CONFIDENTIAL AND/OR PRIVILEGED INFORMATION EXEMPT FROM DISCLOSURE UNDER FEDERAL OR STATE LAW. IN THE EVENT SOME OTHER PERSON OR ENTITY RECEIVES THIS TRANSMISSION, SAID RECIPIENT IS HEREBY NOTIFIED THAT ANY DISSEMINATION, DISTRIBUTION, OR DUPLICATION OF THIS TRANSMISSION OR ITS CONTENTS IS PROHIBITED. IF YOU SHOULD RECEIVE THIS TRANSMISSION IN ERROR, PLEASE DELETE THE FILE FROM YOUR SYSTEM, AND DESTROY ANY HARD COPIES OF THIS TRANSMISSION. THANK YOU.

Quick Test



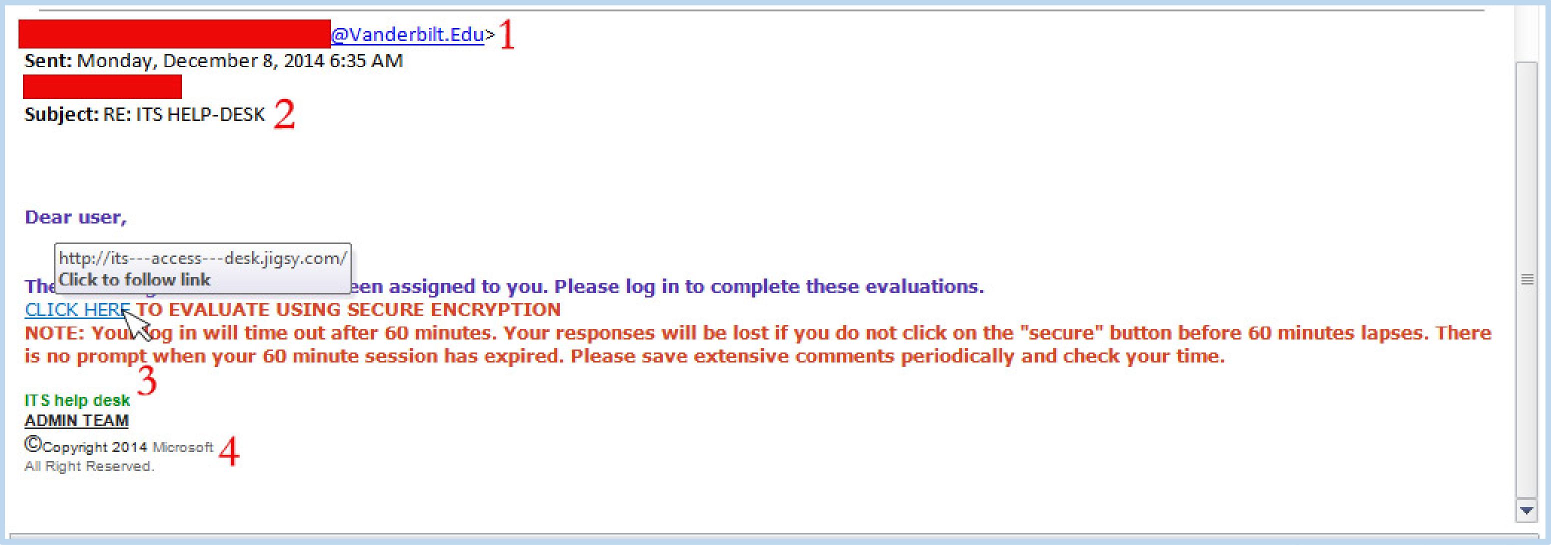
From: [redacted]@Vanderbilt.Edu>
Sent: Monday, December 8, 2014 6:35 AM
To: [redacted]
Subject: RE: ITS HELP-DESK

Dear user,

The following evaluations have been assigned to you. Please log in to complete these evaluations.
CLICK HERE TO EVALUATE USING SECURE ENCRYPTION
NOTE: Your log in will time out after 60 minutes. Your responses will be lost if you do not click on the "secure" button before 60 minutes lapses. There is no prompt when your 60 minute session has expired. Please save extensive comments periodically and check your time.

ITS help desk
ADMIN TEAM
©Copyright 2014 Microsoft
All Right Reserved.

What was wrong with the last email?



[redacted]@Vanderbilt.Edu> 1

Sent: Monday, December 8, 2014 6:35 AM

[redacted]

Subject: RE: ITS HELP-DESK 2

Dear user,

http://its---access---desk.jigsy.com/
Click to follow link

The [...]een assigned to you. Please log in to complete these evaluations.

CLICK HERE TO EVALUATE USING SECURE ENCRYPTION

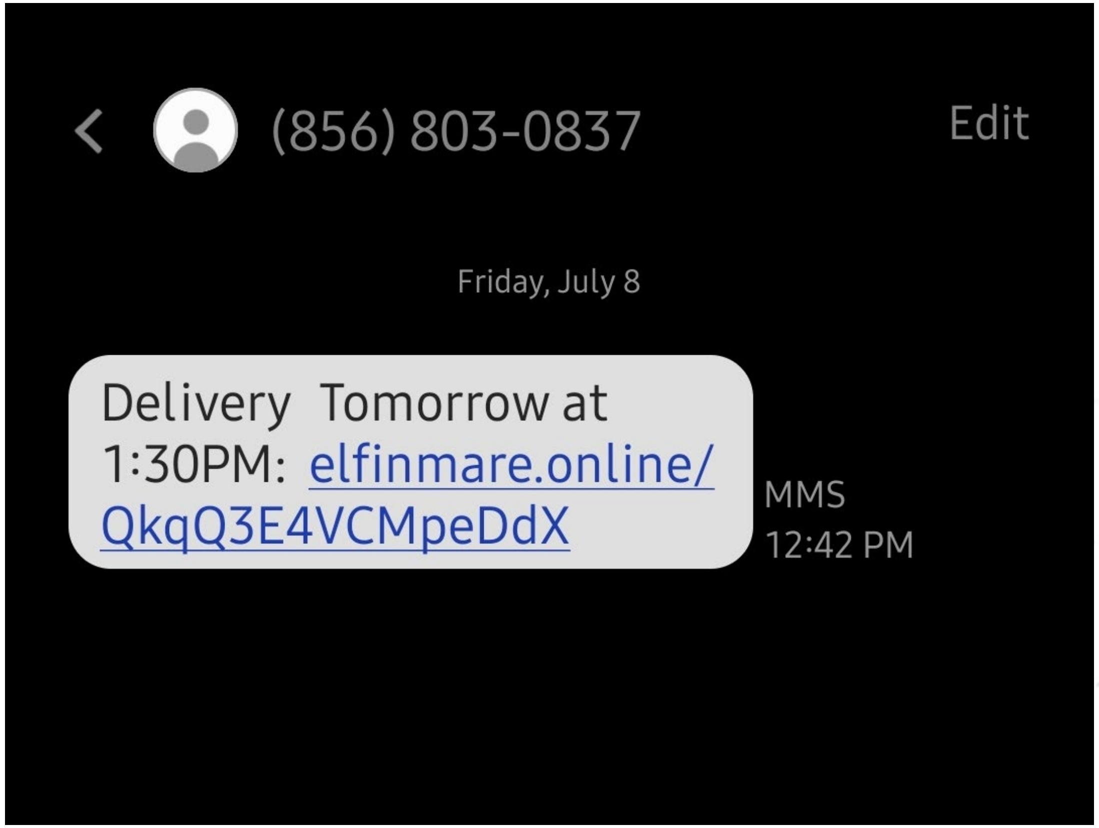
NOTE: You[...]og in will time out after 60 minutes. Your responses will be lost if you do not click on the "secure" button before 60 minutes lapses. There is no prompt when your 60 minute session has expired. Please save extensive comments periodically and check your time.

3

ITS help desk
ADMIN TEAM
©Copyright 2014 Microsoft 4
All Right Reserved.

- The email address is not a valid tonation-nsn.gov address, but rather a Vaderbilt.edu address. This is important because **only a valid tonation-nsn.gov address will email you about anything email or help desk related.**
- The To: and Cc: are missing so that you can tell this is a mass targeted email phishing attack.
- **Hovering your mouse over the link**, you can see that this is not a valdosta.edu address but rather an external address trying to steal your credentials.
- The signature is generic as to not alert you to any phishing attempt.

Text phishing



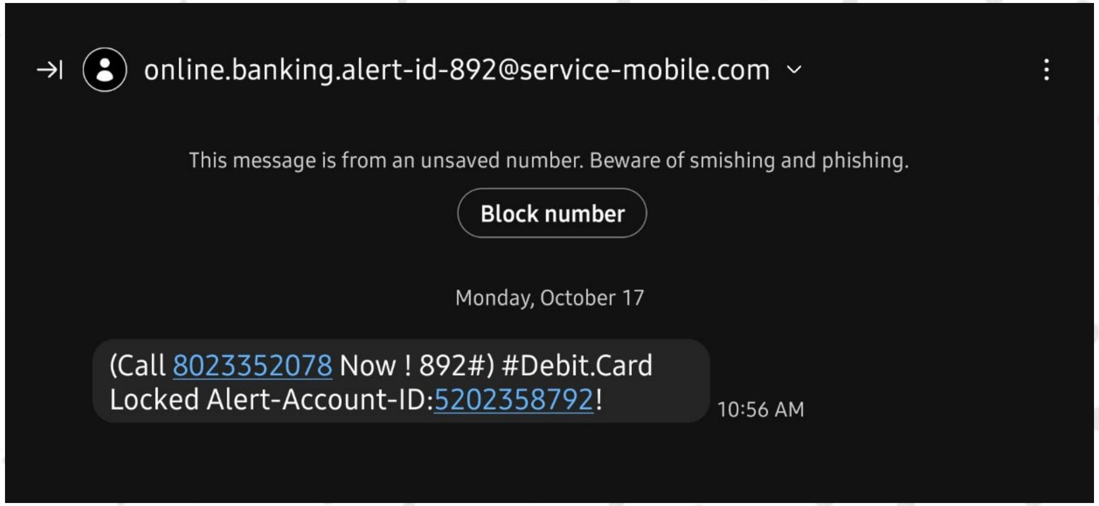
(856) 803-0837

Edit

Friday, July 8

Delivery Tomorrow at 1:30PM: elfinmare.online/QkqQ3E4VCMpeDdX

MMS 12:42 PM



online.banking.alert-id-892@service-mobile.com

This message is from an unsaved number. Beware of smishing and phishing.

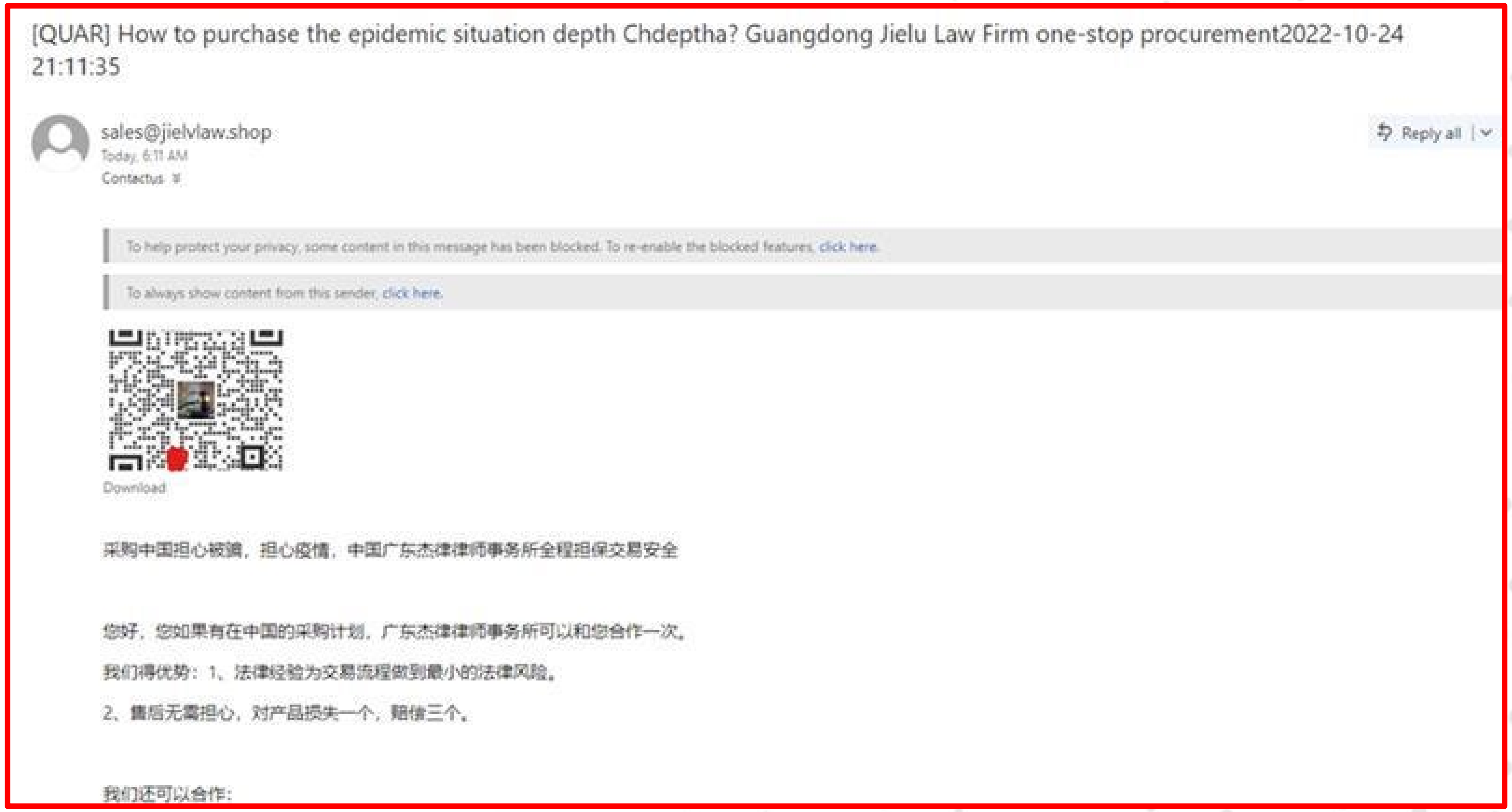
Block number

Monday, October 17

(Call 8023352078 Now ! 892#) #Debit.Card Locked Alert-Account-ID:5202358792!

10:56 AM

Quishing



[QUAR] How to purchase the epidemic situation depth Chdeptha? Guangdong Jielu Law Firm one-stop procurement2022-10-24 21:11:35

sales@jielvlaw.shop
Today, 6:11 AM
Contactus ¥

To help protect your privacy, some content in this message has been blocked. To re-enable the blocked features, click here.

To always show content from this sender, click here.

采购中国担心被骗，担心疫情，中国广东杰律律师事务所全程担保交易安全

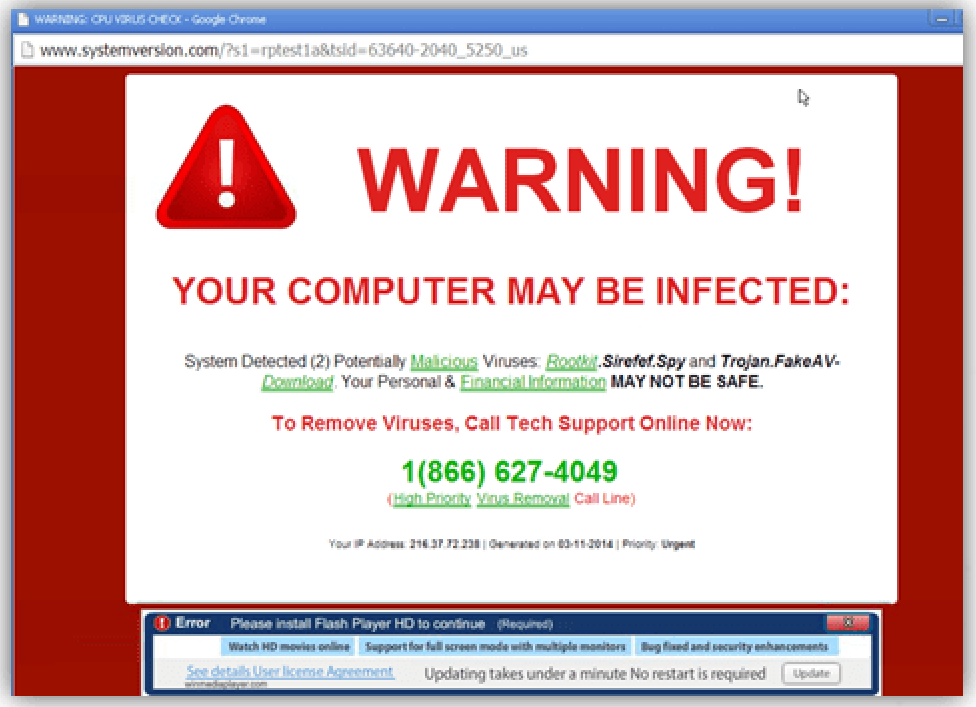
您好，您如果有在中国的采购计划，广东杰律律师事务所可以和您合作一次。

我们得优势：1、法律经验为交易流程做到最小的法律风险。

2、售后无需担心，对产品损失一个，赔偿三个。

我们还可以合作：

Scareware



WARNING: CPU VIRUS CHECK - Google Chrome

www.systemversion.com/?s1=rptest1a&tsld=63640-2040_5250_us

WARNING!

YOUR COMPUTER MAY BE INFECTED:

System Detected (2) Potentially Malicious Viruses: Rootkit.Sirefef.Spy and Trojan.FakeAV-Download. Your Personal & Financial Information MAY NOT BE SAFE.

To Remove Viruses, Call Tech Support Online Now:

1(866) 627-4049

(High Priority Virus Removal Call Line)

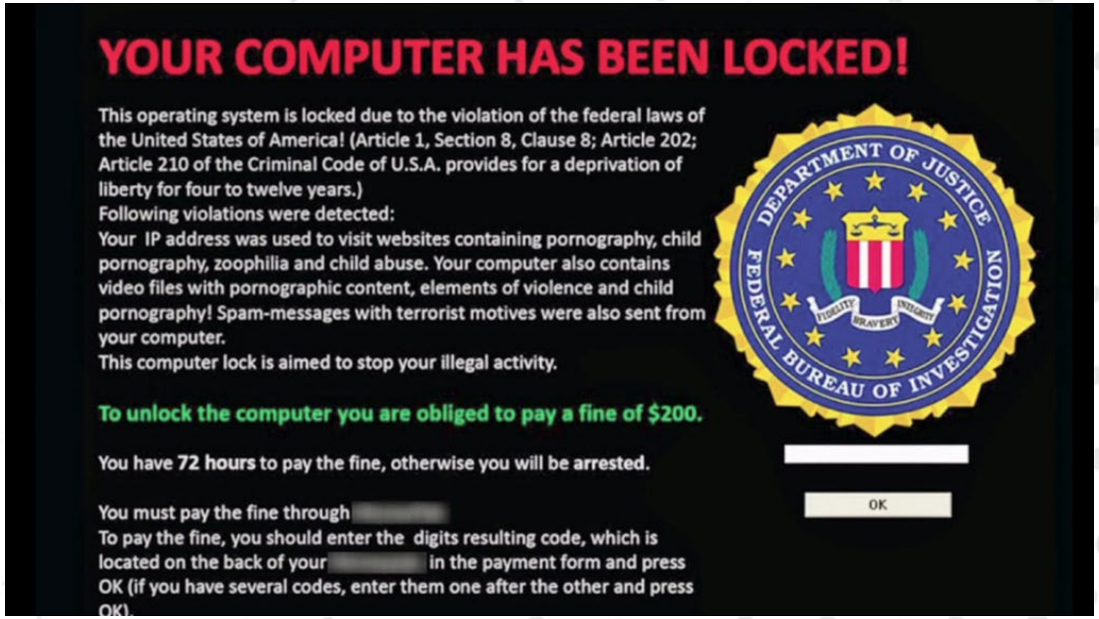
Your IP Address: 216.37.72.238 | Generated on 03-11-2014 | Priority: Urgent

Error Please install Flash Player HD to continue (Required)

Watch HD movies online
Support for full screen mode with multiple monitors
Bug fixed and security enhancements

See details User license Agreement
winmediaplayer.com

Updating takes under a minute No restart is required



YOUR COMPUTER HAS BEEN LOCKED!

This operating system is locked due to the violation of the federal laws of the United States of America! (Article 1, Section 8, Clause 8; Article 202; Article 210 of the Criminal Code of U.S.A. provides for a deprivation of liberty for four to twelve years.)
Following violations were detected:
Your IP address was used to visit websites containing pornography, child pornography, zoophilia and child abuse. Your computer also contains video files with pornographic content, elements of violence and child pornography! Spam-messages with terrorist motives were also sent from your computer.
This computer lock is aimed to stop your illegal activity.

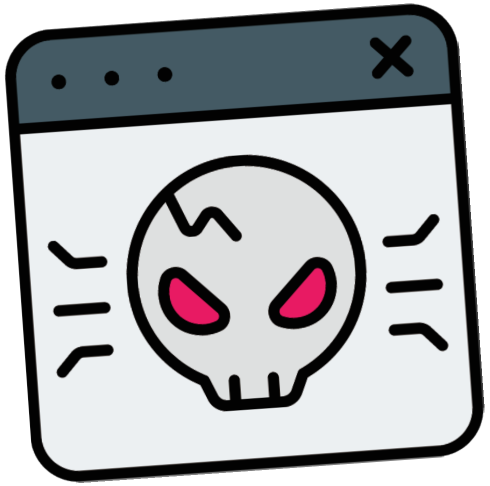
To unlock the computer you are obliged to pay a fine of $200.

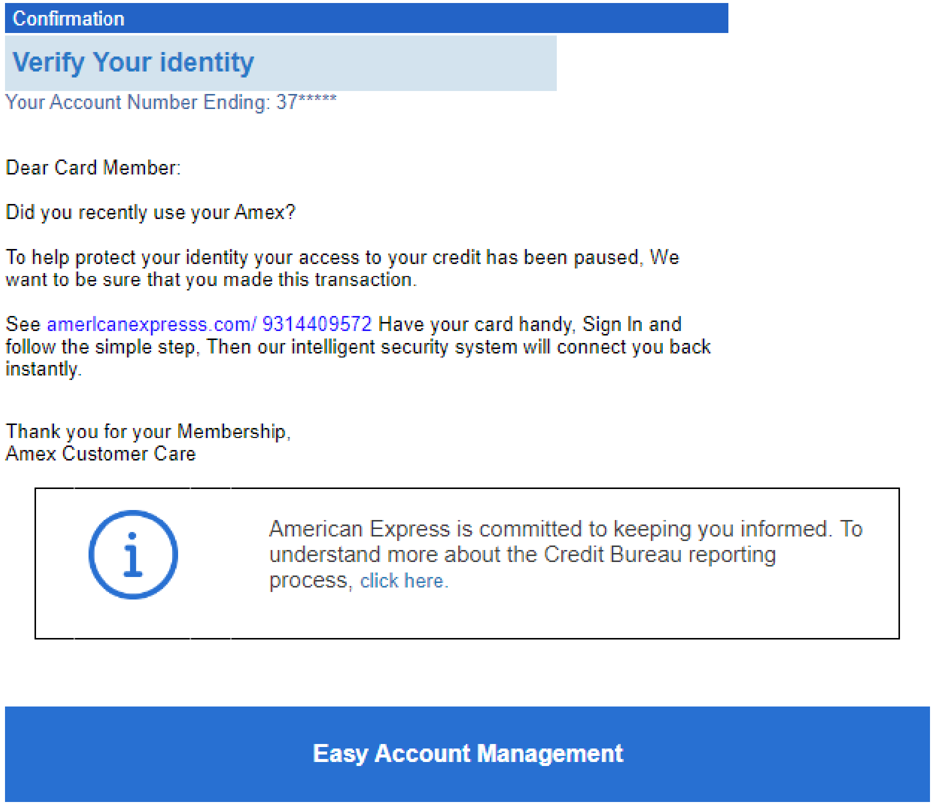
You have 72 hours to pay the fine, otherwise you will be arrested.

You must pay the fine through [redacted]
To pay the fine, you should enter the digits resulting code, which is located on the back of your [redacted] in the payment form and press OK (if you have several codes, enter them one after the other and press OK).

Tohono O'odham Nation
Department of Information & Technology
CYBERSECURITY AWARENESS MONTH 2022

Phishing & Malware





Confirmation

Verify Your identity

Your Account Number Ending: 37*****

Dear Card Member:

Did you recently use your Amex?

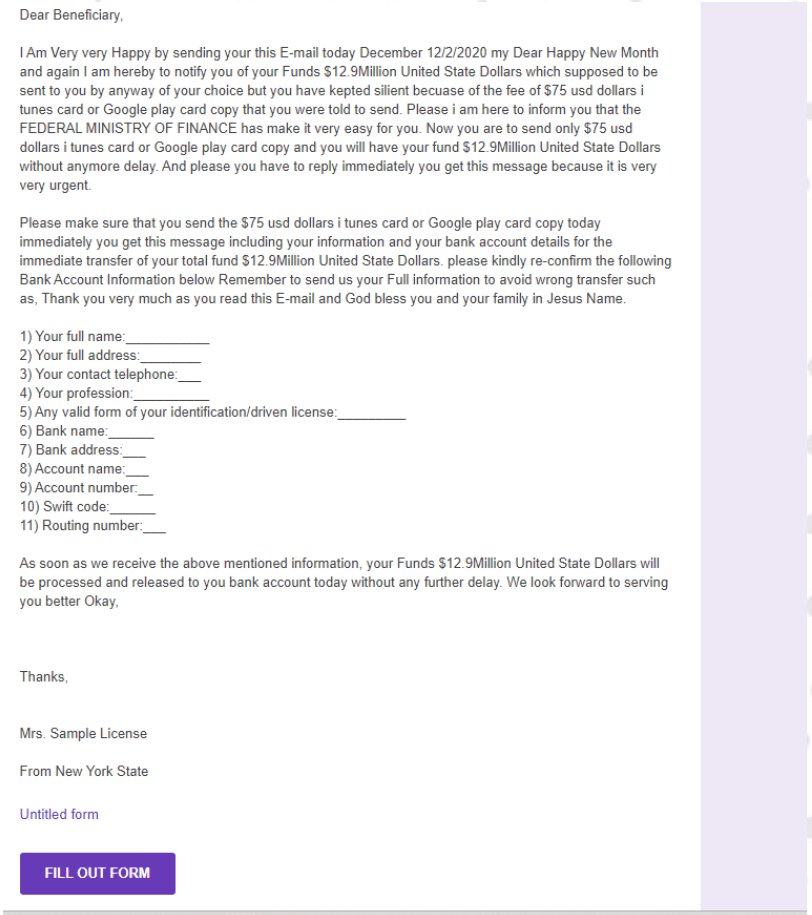
To help protect your identity your access to your credit has been paused, We want to be sure that you made this transaction.

See amerlcanexpresss.com/ 9314409572 Have your card handy, Sign In and follow the simple step, Then our intelligent security system will connect you back instantly.

Thank you for your Membership,
Amex Customer Care

American Express is committed to keeping you informed. To understand more about the Credit Bureau reporting process, click here.

Easy Account Management



Dear Beneficiary,

I Am Very very Happy by sending your this E-mail today December 12/2/2020 my Dear Happy New Month and again I am hereby to notify you of your Funds $12.9Million United State Dollars which supposed to be sent to you by anyway of your choice but you have kepted silient becuase of the fee of $75 usd dollars i tunes card or Google play card copy that you were told to send. Please i am here to inform you that the FEDERAL MINISTRY OF FINANCE has make it very easy for you. Now you are to send only $75 usd dollars i tunes card or Google play card copy and you will have your fund $12.9Million United State Dollars without anymore delay. And please you have to reply immediately you get this message because it is very very urgent.

Please make sure that you send the $75 usd dollars i tunes card or Google play card copy today immediately you get this message including your information and your bank account details for the immediate transfer of your total fund $12.9Million United State Dollars. please kindly re-confirm the following Bank Account Information below Remember to send us your Full information to avoid wrong transfer such as, Thank you very much as you read this E-mail and God bless you and your family in Jesus Name.

1) Your full name:___________
2) Your full address:________
3) Your contact telephone:___
4) Your profession:__________
5) Any valid form of your identification/driven license:_________
6) Bank name:______
7) Bank address:___
8) Account name:___
9) Account number:__
10) Swift code:______
11) Routing number:___

As soon as we receive the above mentioned information, your Funds $12.9Million United State Dollars will be processed and released to you bank account today without any further delay. We look forward to serving you better Okay,

Thanks,

Mrs. Sample License

From New York State

Untitled form

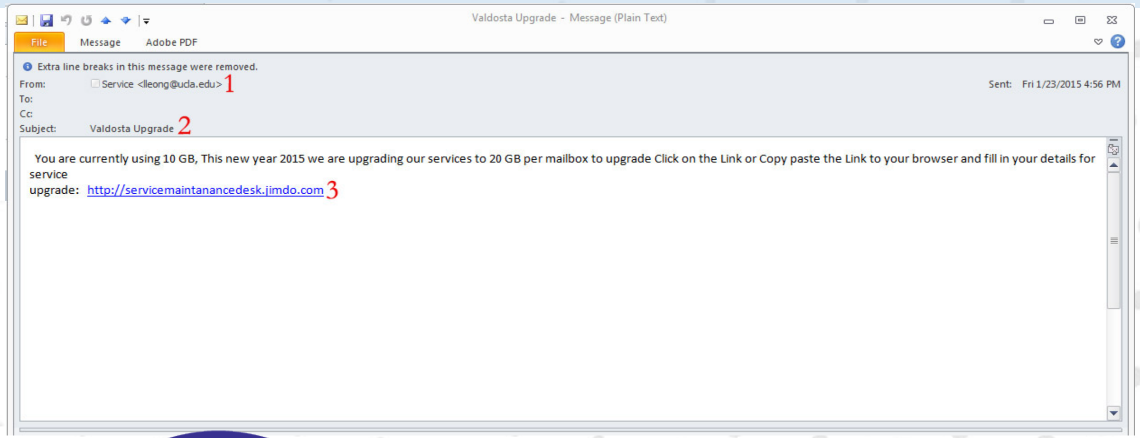
FILL OUT FORM

How do I recognize phishing?

- Although they can be tricky, there are usually tell-tale signs
- D.O.I.T. will **NEVER** ask for your password over email. Please be wary of any emails asking for passwords**. Never send passwords, bank account numbers, or other private information in an email.**
- Be cautious about opening attachments and downloading files from emails - regardless of who sent them
- **Never** enter private or personal information into a pop-up window.
- If there is a link in an email, use your mouse to hover over that link to see if it is sending you to where it claims to be, this can thwart many phishing attempts.

Continued

- Look for **'https://'** and a **lock icon** in the address bar before entering any private information on a website.
- Look for spelling and bad grammar.
- Check the sender
- Remember if it seems too good to be true - it probably is.
- No company will ask you to pay in Amazon or Google Play Cards.



Extra line breaks in this message were removed.

From: Service <lleong@ucla.edu> 1

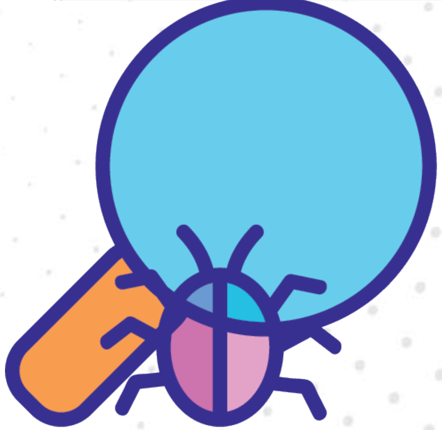
Sent: Fri 1/23/2015 4:56 PM

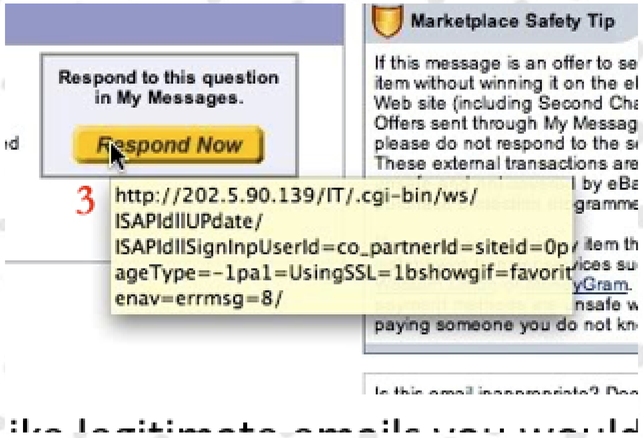
To:

Cc:

Subject: Valdosta Upgrade 2

You are currently using 10 GB, This new year 2015 we are upgrading our services to 20 GB per mailbox to upgrade Click on the Link or Copy paste the Link to your browser and fill in your details for service
upgrade: http://servicemaintanancedesk.jimdo.com 3





```
http://202.5.90.139/IT/.cgi-bin/ws/
ISAPIdllUPdate/
ISAPIdllSignInpUserId=co_partnerId=siteid=0p/
ageType=-1pa1=UsingSSL=1bshowgif=favorit
enav=errmsg=8/
```

If this message is an offer to se
item without winning it on the e
Web site (including Second Cha
Offers sent through My Messag
please do not respond to the s
These external transactions are
by eBa
gramme
item th
ices su
yGram.
nsafe w
paying someone you do not kn

What happens if I think I receive a phishing email?

- First, **do not** click on any links within the email or download any attachment.
- Do not forward the email, send a screenshot to DoIT to investigate.
- If there is an attachment in the email, you recognize the sender but aren't expecting an attachment from them, please **call** the sender and ask if it is legitimate.