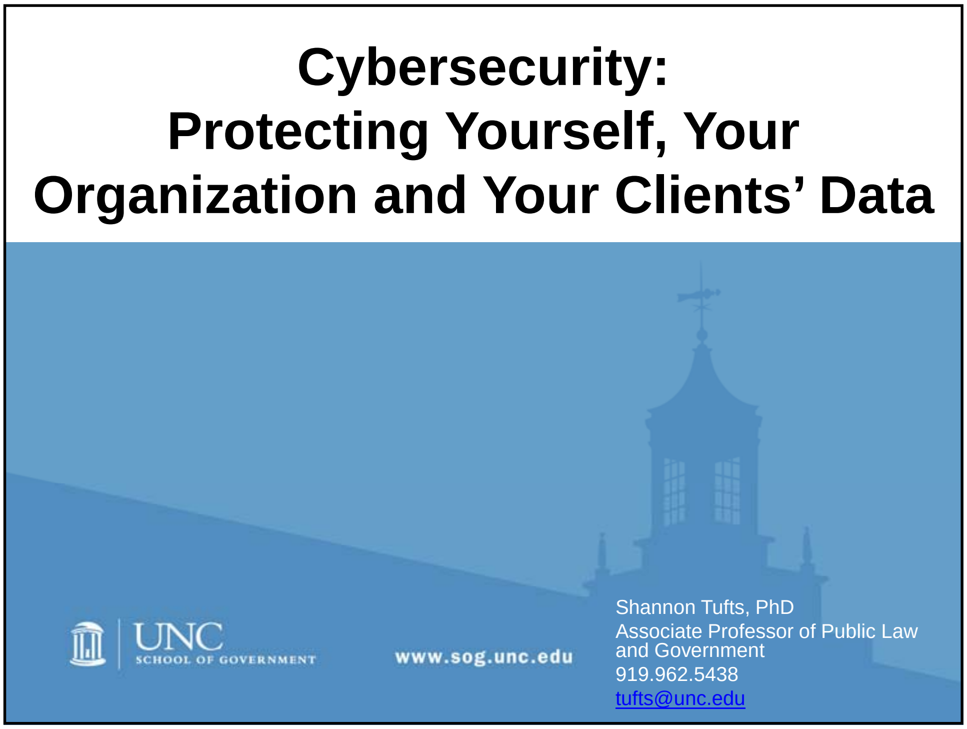


Cybersecurity: Protecting Yourself, Your Organization and Your Clients' Data

Shannon Tufts, PhD
Associate Professor of Public Law and Government
919.962.5438
tufts@unc.edu

www.sog.unc.edu

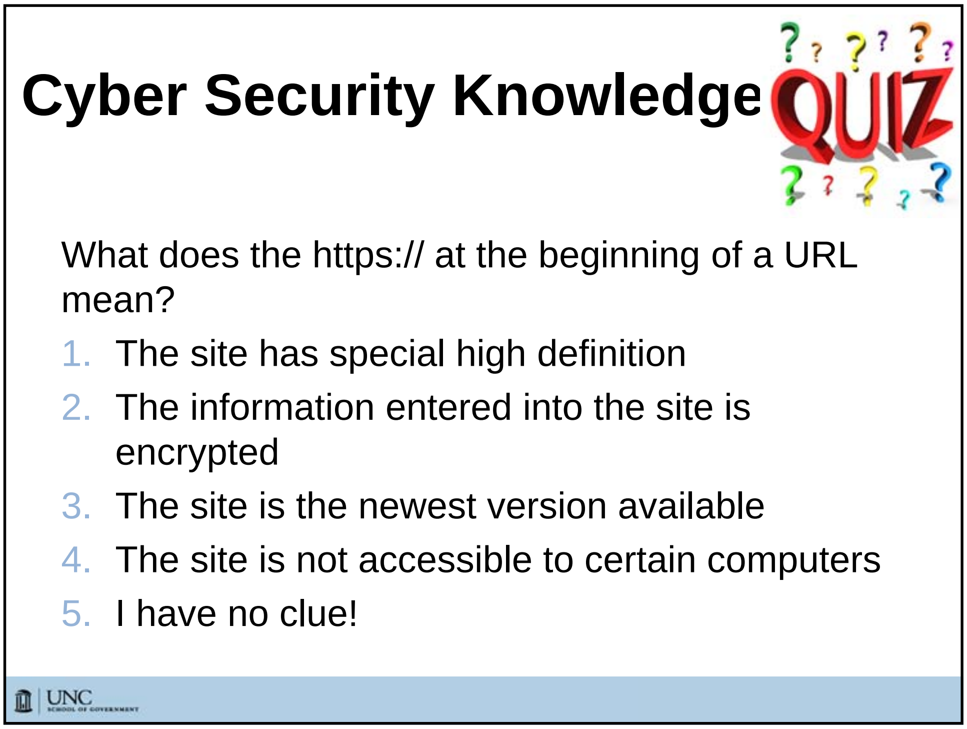
1

AGENDA

- Cybersecurity – Why It Matters
- Social Engineering
- Types/Strategies of Attacks
  - Ransomware/Malware
  - Phishing
  - Business Email Compromise
- What to Look For: Protect Your Data
- NC Breaches and More

*If you get bored, go to https://haveibeenpwned.com

2



Cyber Security Knowledge

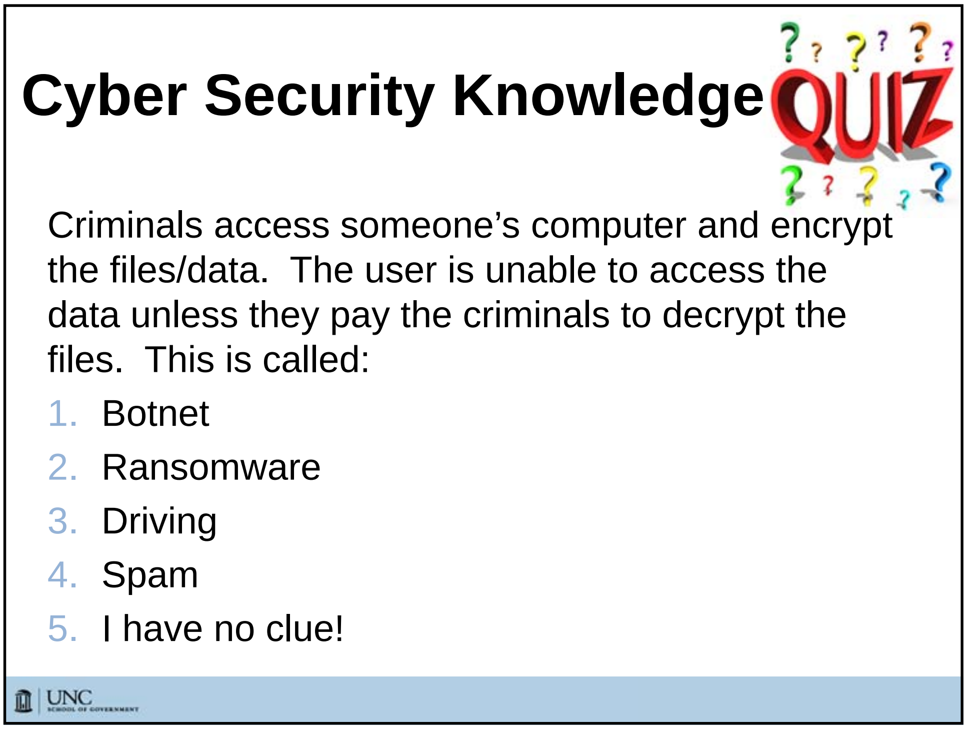
What does the https:// at the beginning of a URL mean?

1. The site has special high definition
2. The information entered into the site is encrypted
3. The site is the newest version available
4. The site is not accessible to certain computers
5. I have no clue!

3

All Financial, PII, PHI (and more) Collections Must Use HTTPS://

4



Cyber Security Knowledge

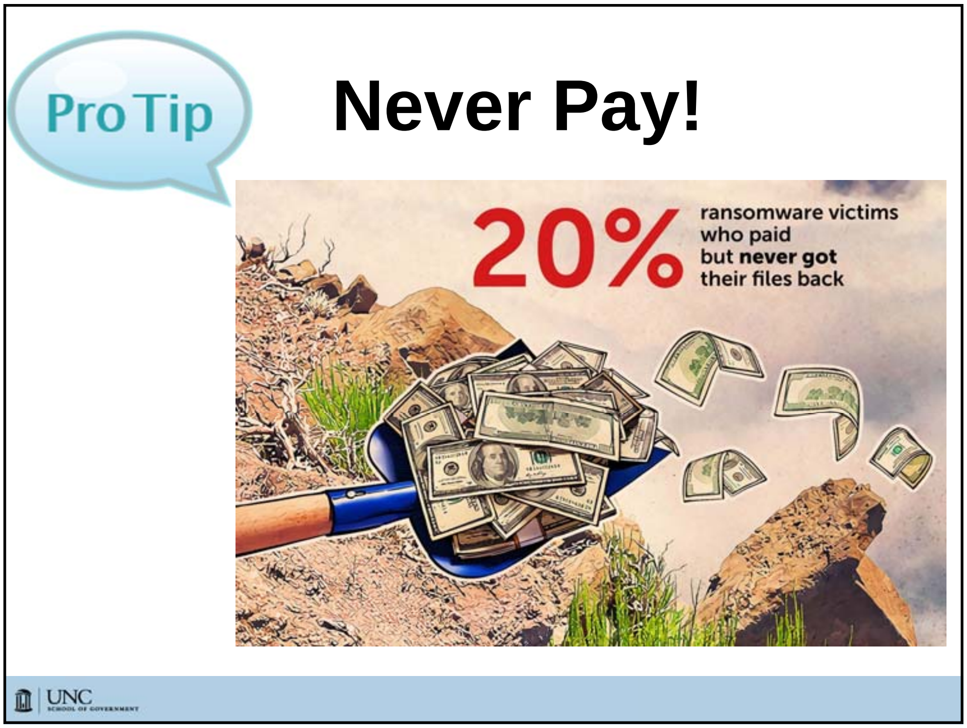
QUIZ

Criminals access someone's computer and encrypt the files/data. The user is unable to access the data unless they pay the criminals to decrypt the files. This is called:

1. Botnet
2. Ransomware
3. Driving
4. Spam
5. I have no clue!

UNC School of Government

5



Never Pay!

6

Polling Question

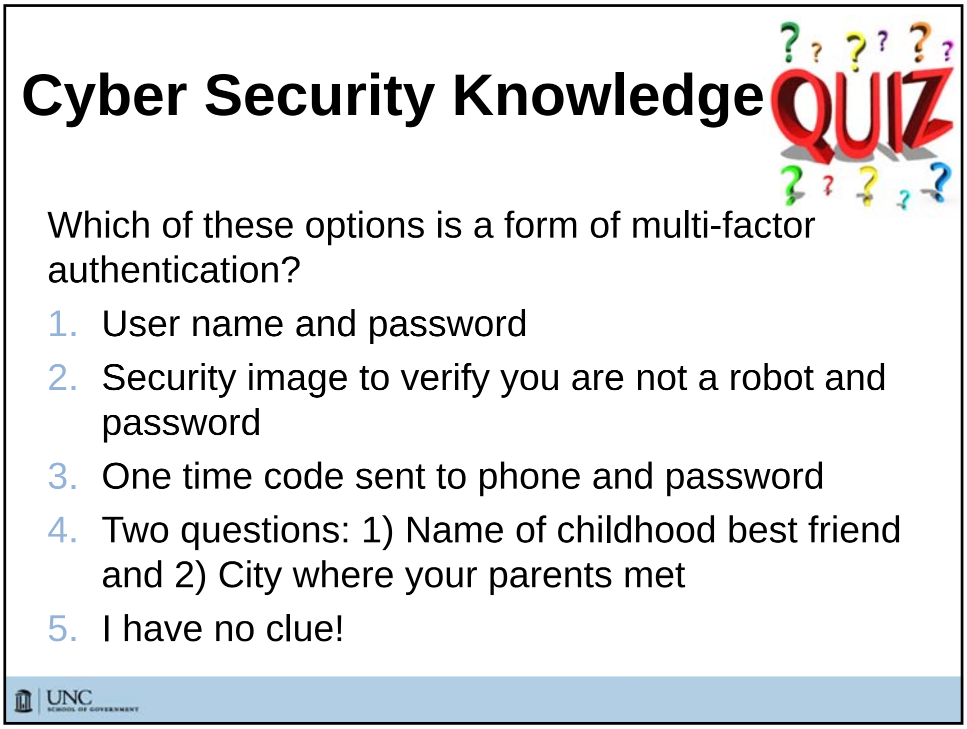
Which of the following passwords is most secure?

7

Pro Tip

- 15 character non-complex passwords are more secure than 8 character complex passwords
- The space bar at the end of your password is very hard to hack (at least by brute force attacks or harvesting of credentials via a bot)

8

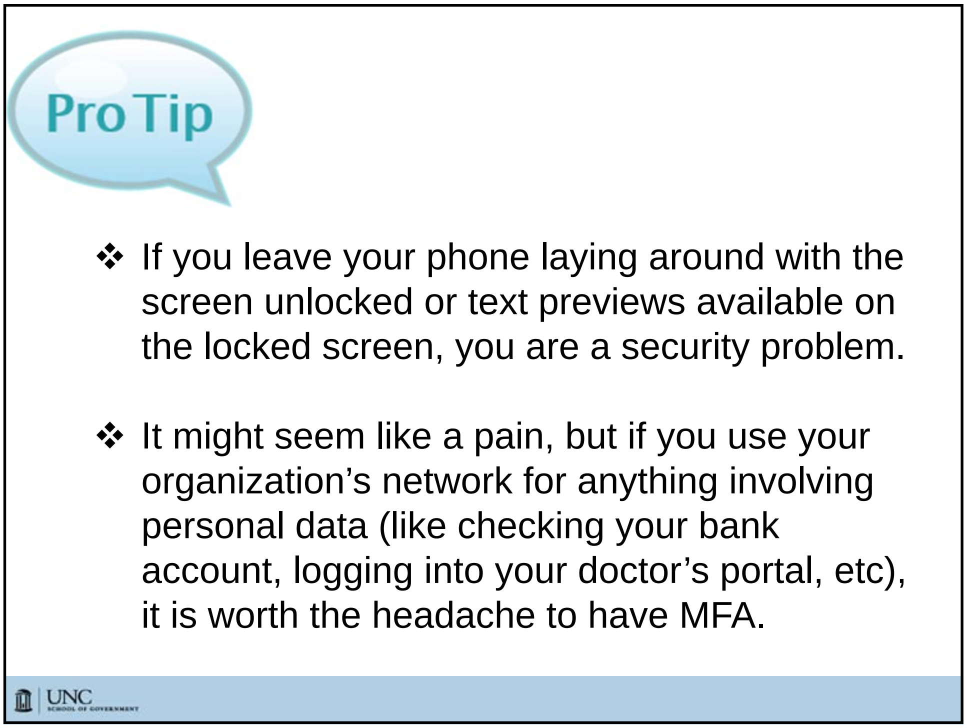


Cyber Security Knowledge

Which of these options is a form of multi-factor authentication?

1. User name and password
2. Security image to verify you are not a robot and password
3. One time code sent to phone and password
4. Two questions: 1) Name of childhood best friend and 2) City where your parents met
5. I have no clue!

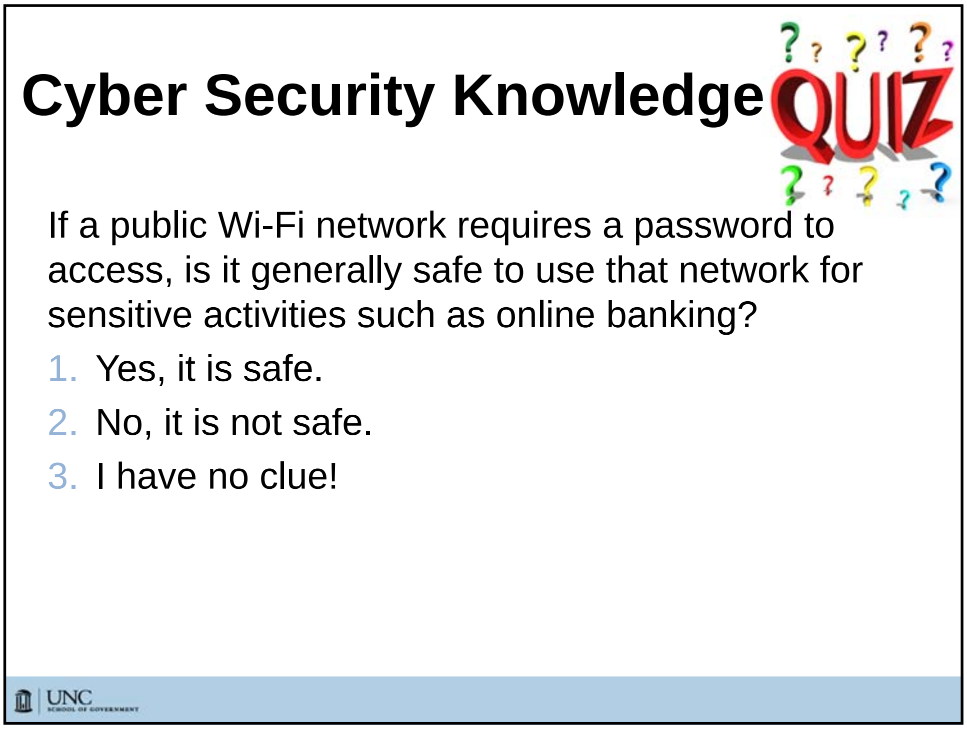
9



❖ If you leave your phone laying around with the screen unlocked or text previews available on the locked screen, you are a security problem.

❖ It might seem like a pain, but if you use your organization’s network for anything involving personal data (like checking your bank account, logging into your doctor’s portal, etc), it is worth the headache to have MFA.

10

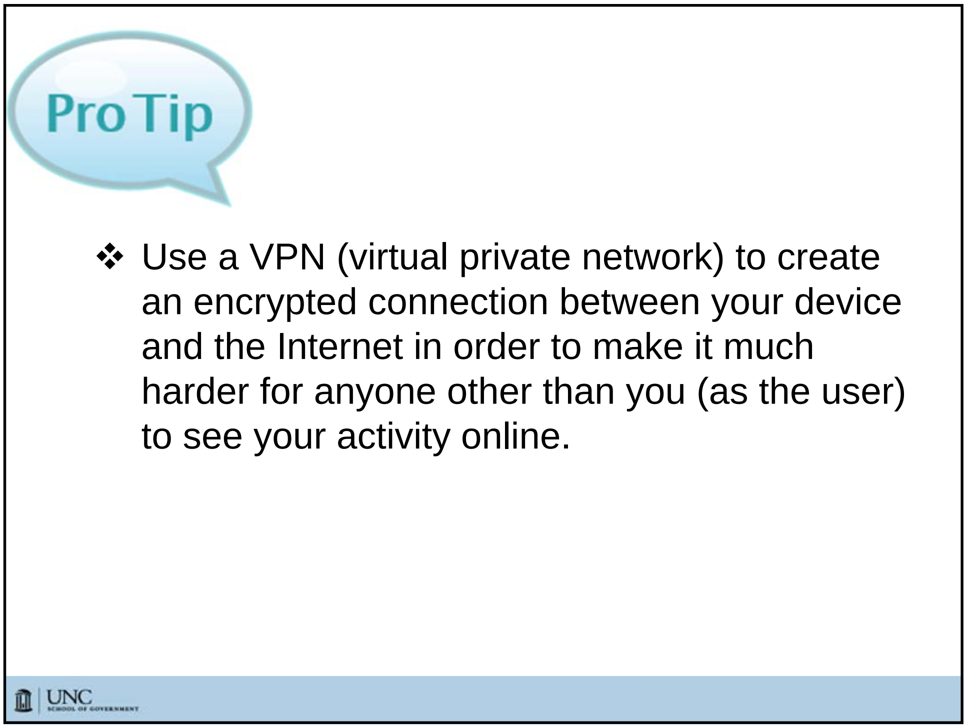


Cyber Security Knowledge QUIZ

If a public Wi-Fi network requires a password to access, is it generally safe to use that network for sensitive activities such as online banking?

1. Yes, it is safe.
2. No, it is not safe.
3. I have no clue!

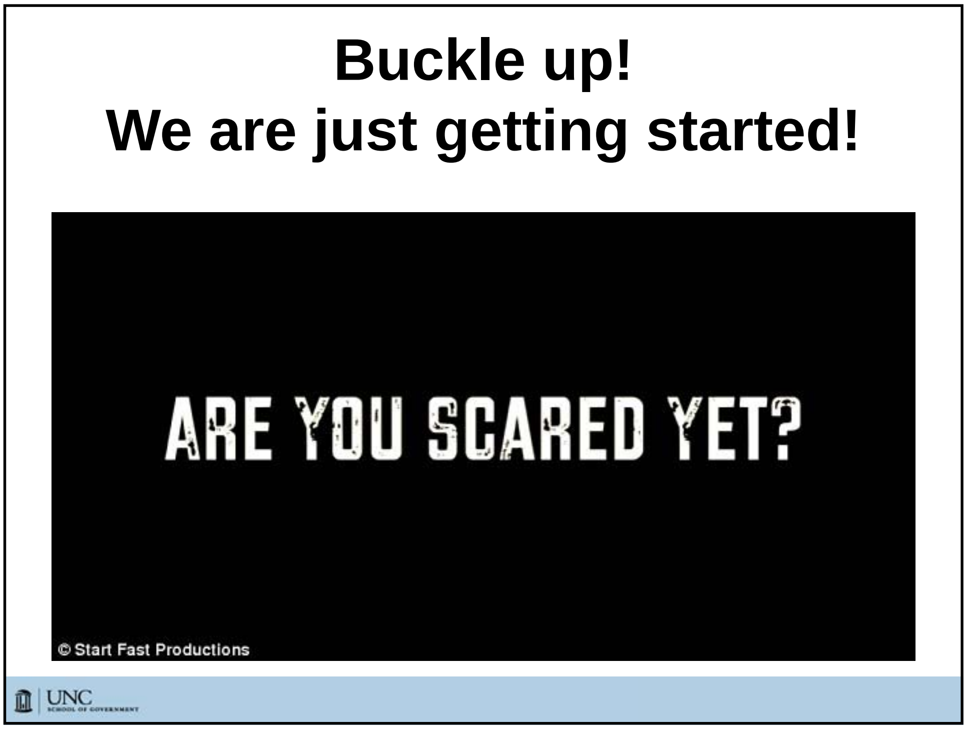
11



Pro Tip

- ❖ Use a VPN (virtual private network) to create an encrypted connection between your device and the Internet in order to make it much harder for anyone other than you (as the user) to see your activity online.

12



Buckle up!
We are just getting started!

ARE YOU SCARED YET?

© Start Fast Productions

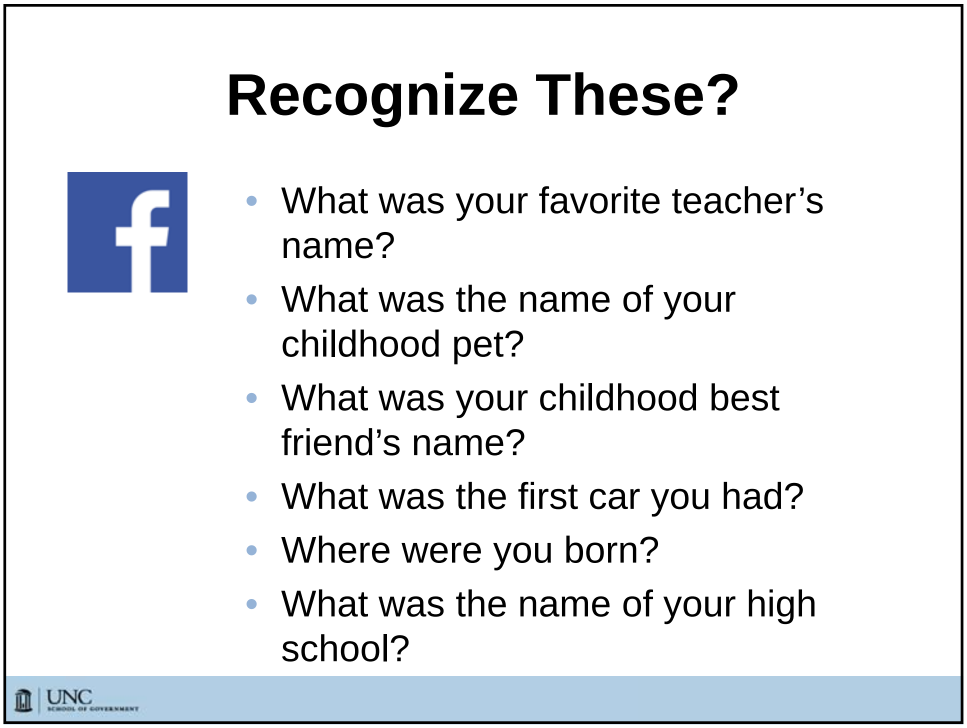
13

SOCIAL ENGINEERING

The clever manipulation of the natural human tendency to trust.

14

15



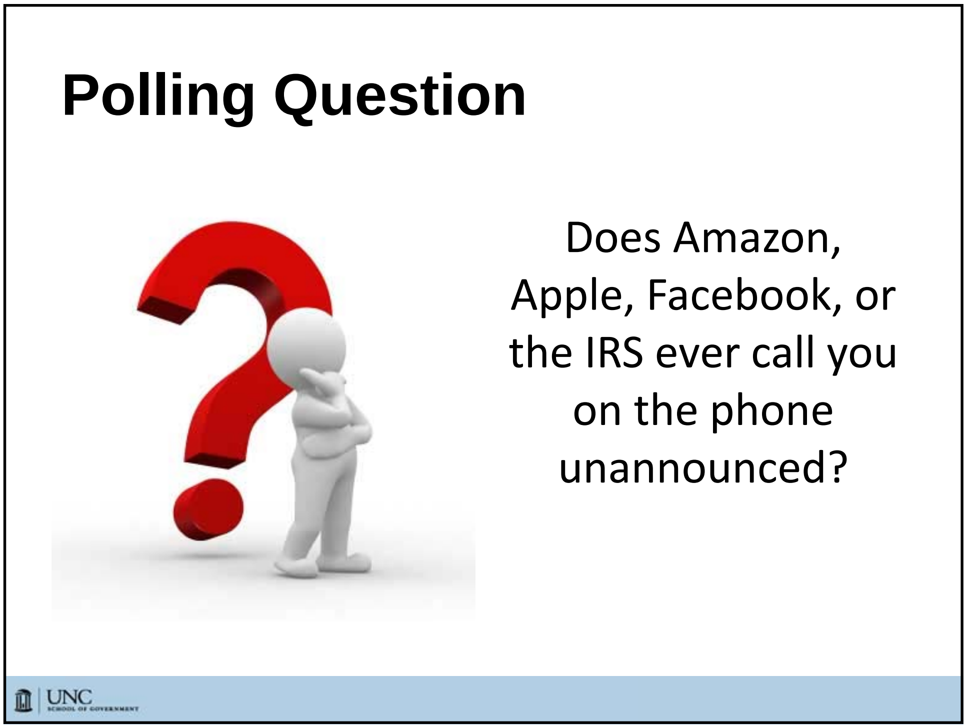
Recognize These?

- What was your favorite teacher's name?
- What was the name of your childhood pet?
- What was your childhood best friend's name?
- What was the first car you had?
- Where were you born?
- What was the name of your high school?

16

Spreading Holiday Cheer!

17



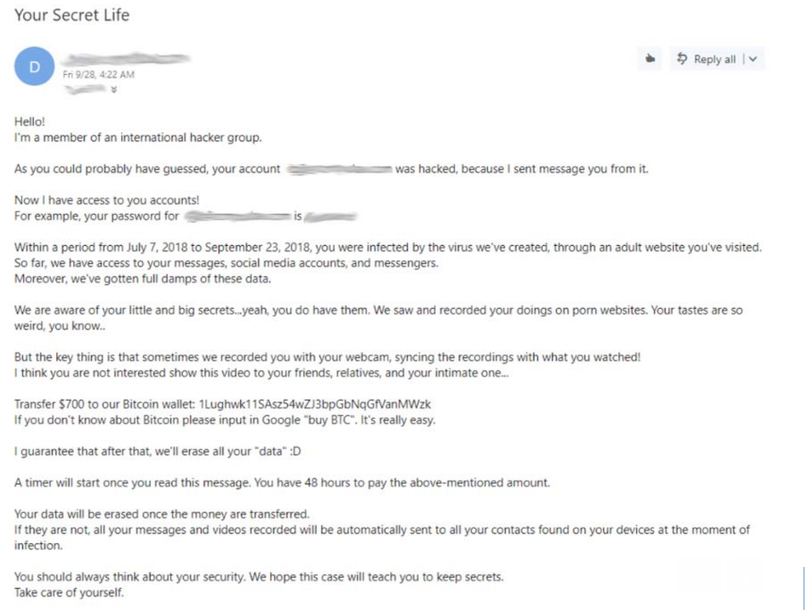
Polling Question

Does Amazon, Apple, Facebook, or the IRS ever call you on the phone unannounced?

18

19

Webcam Blackmail/Sextortion - Click Here



Your Secret Life

D [redacted]
Fri 9/28, 4:22 AM
[redacted]

Hello!
I'm a member of an international hacker group.

As you could probably have guessed, your account [redacted] was hacked, because I sent message you from it.

Now I have access to you accounts!
For example, your password for [redacted] is [redacted]

Within a period from July 7, 2018 to September 23, 2018, you were infected by the virus we've created, through an adult website you've visited.
So far, we have access to your messages, social media accounts, and messengers.
Moreover, we've gotten full damps of these data.

We are aware of your little and big secrets...yeah, you do have them. We saw and recorded your doings on porn websites. Your tastes are so weird, you know..

But the key thing is that sometimes we recorded you with your webcam, syncing the recordings with what you watched!
I think you are not interested show this video to your friends, relatives, and your intimate one...

Transfer $700 to our Bitcoin wallet: 1Lughwk11SAsz54wZJ3bpGbNqGfVanMWzk
If you don't know about Bitcoin please input in Google "buy BTC". It's really easy.

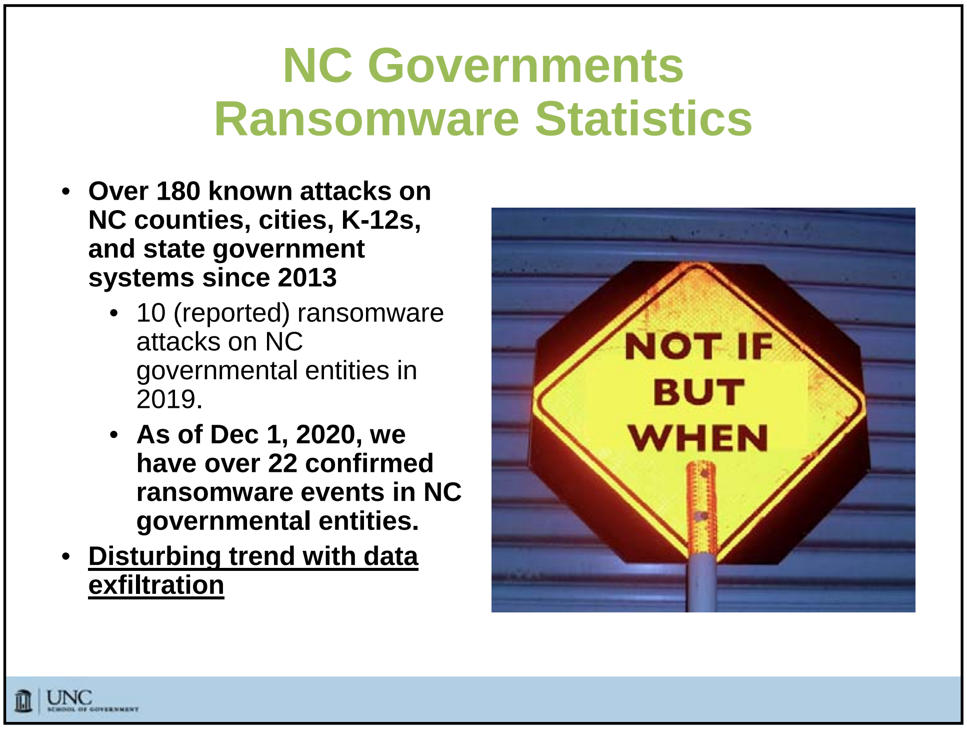
I guarantee that after that, we'll erase all your "data" :D

A timer will start once you read this message. You have 48 hours to pay the above-mentioned amount.

Your data will be erased once the money are transferred.
If they are not, all your messages and videos recorded will be automatically sent to all your contacts found on your devices at the moment of infection.

You should always think about your security. We hope this case will teach you to keep secrets.
Take care of yourself.

20



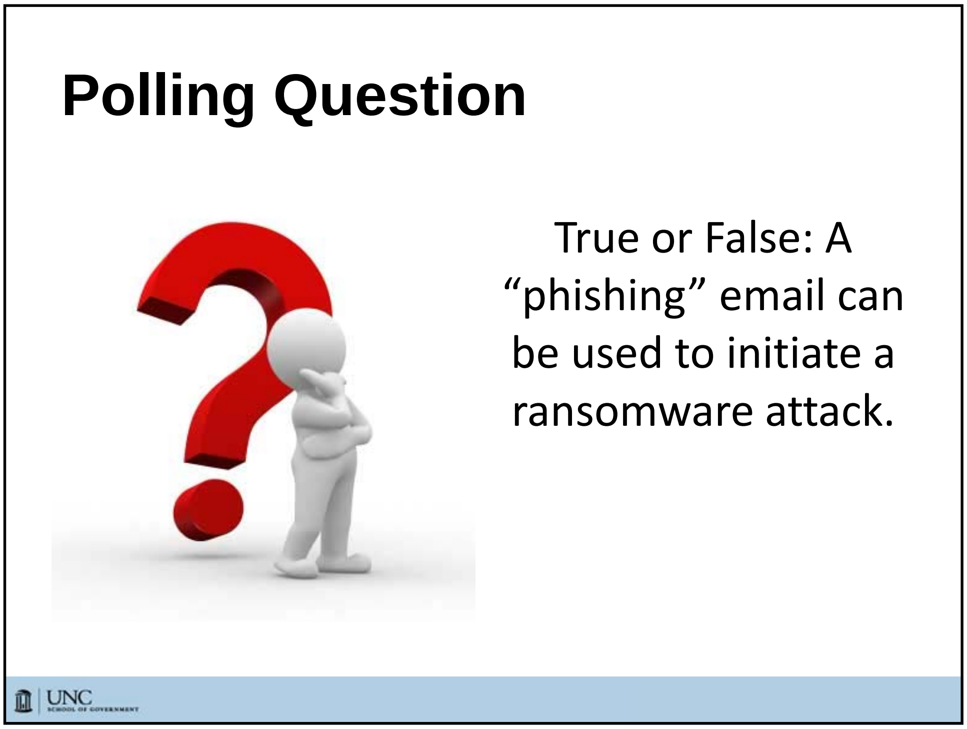
NC Governments Ransomware Statistics

- **Over 180 known attacks on NC counties, cities, K-12s, and state government systems since 2013**
  - 10 (reported) ransomware attacks on NC governmental entities in 2019.
  - **As of Dec 1, 2020, we have over 22 confirmed ransomware events in NC governmental entities.**
- **<u>Disturbing trend with data exfiltration</u>**

NOT IF
BUT
WHEN
UNC
SCHOOL OF GOVERNMENT

21

22

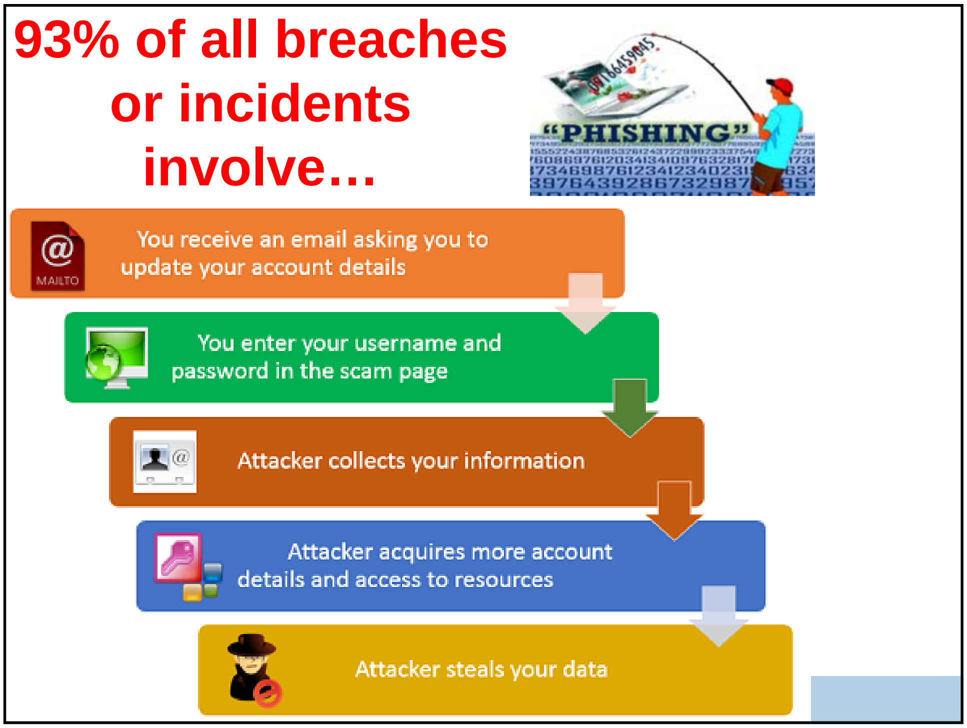


Polling Question

True or False: A "phishing" email can be used to initiate a ransomware attack.

UNC SCHOOL OF GOVERNMENT

23



93% of all breaches or incidents involve…

You receive an email asking you to update your account details

You enter your username and password in the scam page

Attacker collects your information

Attacker acquires more account details and access to resources

Attacker steals your data

24

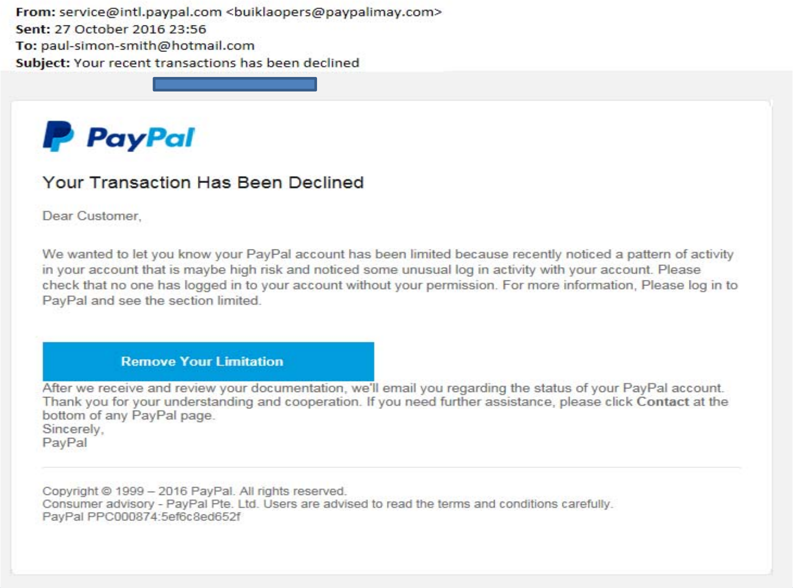
Hacker 101: Build Trust

- Spear phishers personalize emails to try to gain your trust
  - Full name
  - Mailing address
  - Name of your employer
  - Personal Data (SSN, Banking Account Number, etc)

*Even if the email or text message appears to be from someone you know, use caution.

UNC SCHOOL OF GOVERNMENT

25



From: service@intl.paypal.com <buiklaopers@paypalimay.com>
Sent: 27 October 2016 23:56
To: paul-simon-smith@hotmail.com
Subject: Your recent transactions has been declined

[redacted]

PayPal

Your Transaction Has Been Declined

Dear Customer,

We wanted to let you know your PayPal account has been limited because recently noticed a pattern of activity in your account that is maybe high risk and noticed some unusual log in activity with your account. Please check that no one has logged in to your account without your permission. For more information, Please log in to PayPal and see the section limited.

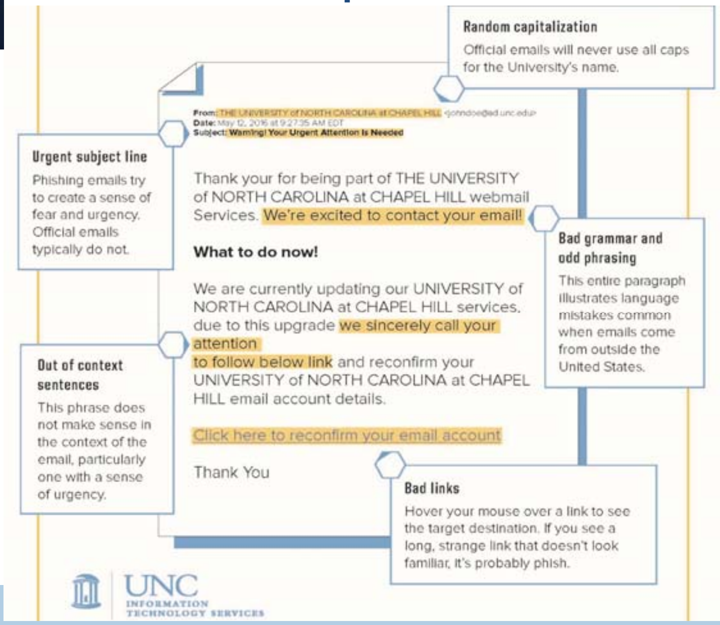
After we receive and review your documentation, we'll email you regarding the status of your PayPal account. Thank you for your understanding and cooperation. If you need further assistance, please click **Contact** at the bottom of any PayPal page.
Sincerely,
PayPal

Copyright © 1999 – 2016 PayPal. All rights reserved.
Consumer advisory - PayPal Pte. Ltd. Users are advised to read the terms and conditions carefully.
PayPal PPC000874:5ef6c8ed652f

UNC SCHOOL OF GOVERNMENT

26

How to Spot a Phish



Random capitalization
Official emails will never use all caps for the University's name.

From: THE UNIVERSITY of NORTH CAROLINA at CHAPEL HILL <johndoe@ad.unc.edu>
Date: May 12, 2016 at 9:27:35 AM EDT
Subject: Warning! Your Urgent Attention Is Needed

Urgent subject line
Phishing emails try to create a sense of fear and urgency. Official emails typically do not.

Thank your for being part of THE UNIVERSITY of NORTH CAROLINA at CHAPEL HILL webmail Services. We're excited to contact your email!

What to do now!

We are currently updating our UNIVERSITY of NORTH CAROLINA at CHAPEL HILL services, due to this upgrade we sincerely call your attention to follow below link and reconfirm your UNIVERSITY of NORTH CAROLINA at CHAPEL HILL email account details.

Click here to reconfirm your email account

Thank You

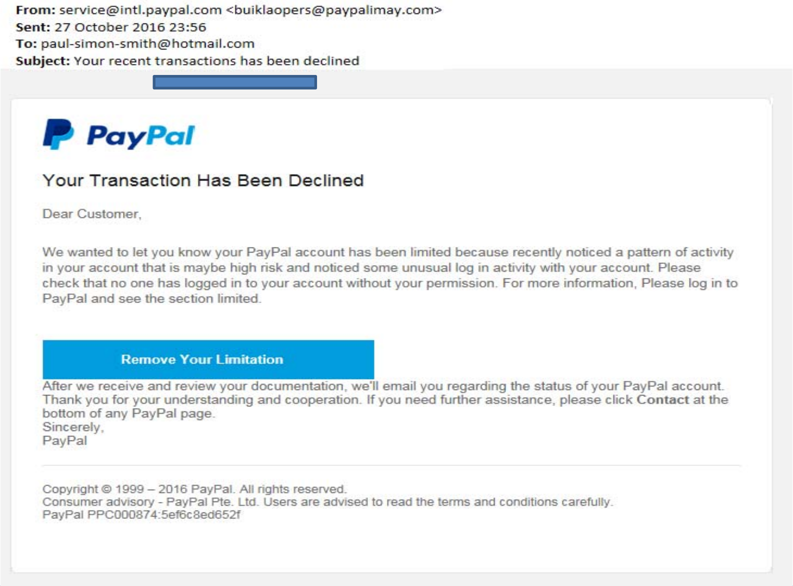
Bad grammar and odd phrasing
This entire paragraph illustrates language mistakes common when emails come from outside the United States.

Out of context sentences
This phrase does not make sense in the context of the email, particularly one with a sense of urgency.

Bad links
Hover your mouse over a link to see the target destination. If you see a long, strange link that doesn't look familiar, it's probably phish.

UNC INFORMATION TECHNOLOGY SERVICES

27



From: service@intl.paypal.com <buiklaopers@paypalimay.com>
Sent: 27 October 2016 23:56
To: paul-simon-smith@hotmail.com
Subject: Your recent transactions has been declined

PayPal

Your Transaction Has Been Declined

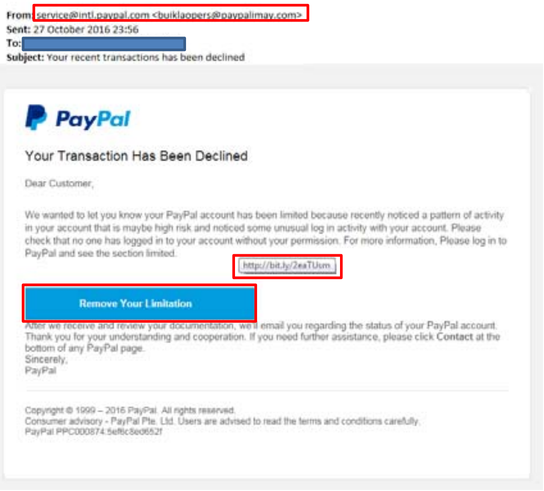
Dear Customer,

We wanted to let you know your PayPal account has been limited because recently noticed a pattern of activity in your account that is maybe high risk and noticed some unusual log in activity with your account. Please check that no one has logged in to your account without your permission. For more information, Please log in to PayPal and see the section limited.

After we receive and review your documentation, we'll email you regarding the status of your PayPal account. Thank you for your understanding and cooperation. If you need further assistance, please click **Contact** at the bottom of any PayPal page.
Sincerely,
PayPal

Copyright © 1999 – 2016 PayPal. All rights reserved.
Consumer advisory - PayPal Pte. Ltd. Users are advised to read the terms and conditions carefully.
PayPal PPC000874:5ef6c8ed652f

28



From: service@intl.paypal.com <buiklaopers@paypalimay.com>
Sent: 27 October 2016 23:56
To: [redacted]
Subject: Your recent transactions has been declined

PayPal

Your Transaction Has Been Declined

Dear Customer,

We wanted to let you know your PayPal account has been limited because recently noticed a pattern of activity in your account that is maybe high risk and noticed some unusual log in activity with your account. Please check that no one has logged in to your account without your permission. For more information, Please log in to PayPal and see the section limited.

http://bit.ly/2eaTUsm

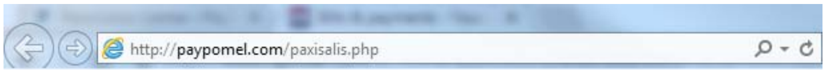
Remove Your Limitation

After we receive and review your documentation, we'll email you regarding the status of your PayPal account. Thank you for your understanding and cooperation. If you need further assistance, please click **Contact** at the bottom of any PayPal page.
Sincerely,
PayPal

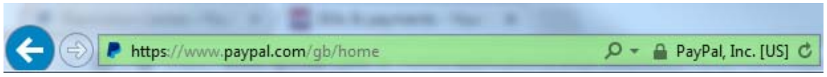
Copyright © 1999 – 2016 PayPal. All rights reserved.
Consumer advisory - PayPal Pte. Ltd. Users are advised to read the terms and conditions carefully.
PayPal PPC000874:5ef6c8ed652f

29

Scam Link, Incorrect Domain Name, NO Https & NO Padlock



Legitimate Link, Correct Domain Name, Https & The Padlock



30

Polling Question

Which of the following are signs of a phishing email?

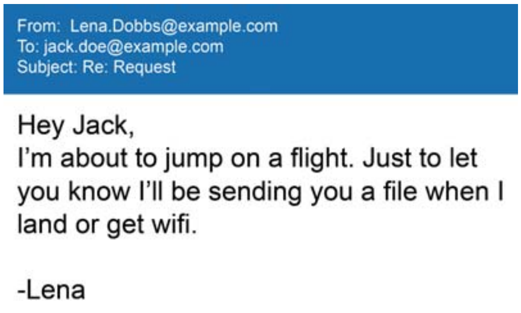
31

Another Approach

The Double Barrel attack uses multiple emails to create a believable narrative.

Stage One: The Lure

1st Email builds trust



From: Lena.Dobbs@example.com
To: jack.doe@example.com
Subject: Re: Request

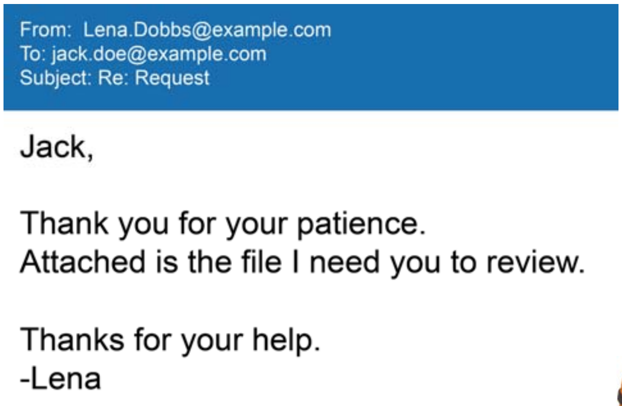
Hey Jack,
I'm about to jump on a flight. Just to let you know I'll be sending you a file when I land or get wifi.

-Lena

32

Stage Two: The Phish

The second email contains malicious attachments or links



From: Lena.Dobbs@example.com
To: jack.doe@example.com
Subject: Re: Request

Jack,

Thank you for your patience.
Attached is the file I need you to review.

Thanks for your help.
-Lena

33

Voice Phishing Example

34

35

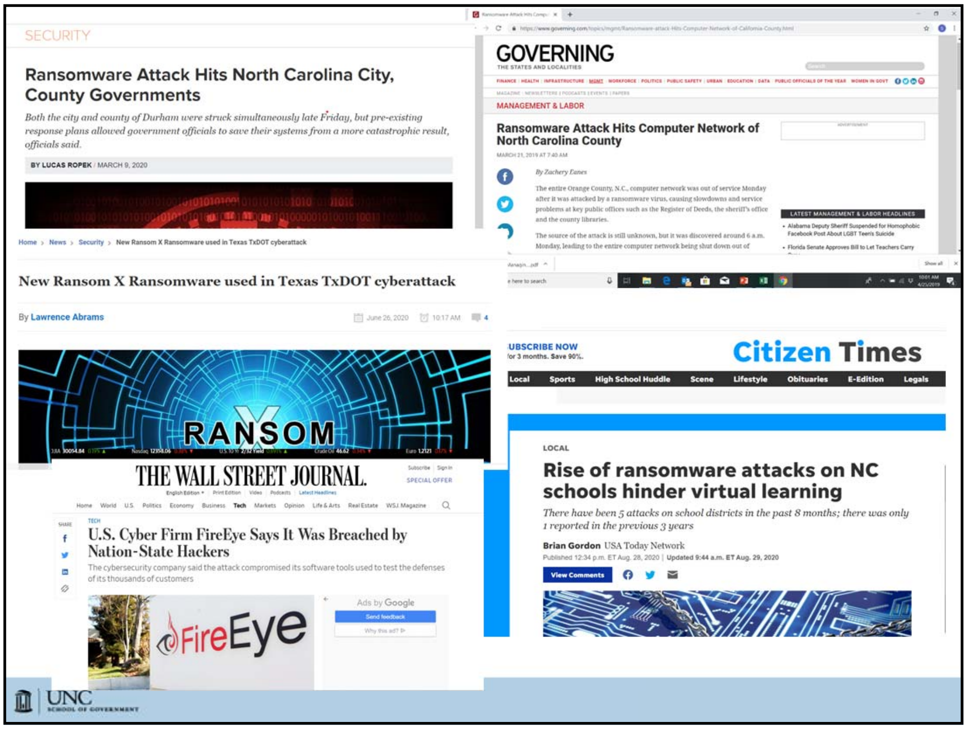
Ransomware: What Is It?

Ransomware is a type of malware that attempts to extort money from user or organization by infecting or taking control of the victim’s computer, files, servers, etc.

Ransomware usually encrypts files, folders, machines, servers to prevent access and use unless the ransom is paid to receive the decryption key.

Data exfiltration has become more widespread as part of ransomware events in the past 6-9 months.

36



SECURITY

Ransomware Attack Hits North Carolina City, County Governments

Both the city and county of Durham were struck simultaneously late Friday, but pre-existing response plans allowed government officials to save their systems from a more catastrophic result, officials said.

BY LUCAS ROPEK / MARCH 9, 2020

GOVERNING
THE STATES AND LOCALITIES

FINANCE | HEALTH | INFRASTRUCTURE | MGMT | WORKFORCE | POLITICS | PUBLIC SAFETY | URBAN | EDUCATION | DATA | PUBLIC OFFICIALS OF THE YEAR | WOMEN IN GOVT

MAGAZINE | NEWSLETTERS | PODCASTS | EVENTS | PAPERS

MANAGEMENT & LABOR

Ransomware Attack Hits Computer Network of North Carolina County

MARCH 21, 2019 AT 7:40 AM

By Zachery Eanes

The entire Orange County, N.C., computer network was out of service Monday after it was attacked by a ransomware virus, causing slowdowns and service problems at key public offices such as the Register of Deeds, the sheriff's office and the county libraries.

The source of the attack is still unknown, but it was discovered around 6 a.m. Monday, leading to the entire computer network being shut down out of

LATEST MANAGEMENT & LABOR HEADLINES

- Alabama Deputy Sheriff Suspended for Homophobic Facebook Post About LGBT Teen's Suicide
- Florida Senate Approves Bill to Let Teachers Carry

Home › News › Security › New Ransom X Ransomware used in Texas TxDOT cyberattack

New Ransom X Ransomware used in Texas TxDOT cyberattack

By Lawrence Abrams June 26, 2020 10:17 AM 4

THE WALL STREET JOURNAL.

English Edition | Print Edition | Video | Podcasts | Latest Headlines

Home World U.S. Politics Economy Business Tech Markets Opinion Life & Arts Real Estate WSJ Magazine

TECH

U.S. Cyber Firm FireEye Says It Was Breached by Nation-State Hackers

The cybersecurity company said the attack compromised its software tools used to test the defenses of its thousands of customers

UBSCRIBE NOW
for 3 months. Save 90%.

Citizen Times

Local Sports High School Huddle Scene Lifestyle Obituaries E-Edition Legals

LOCAL

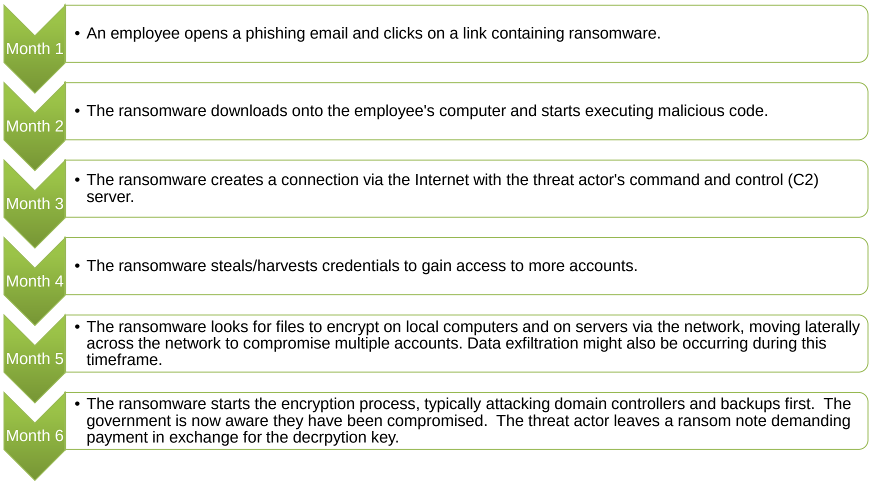
Rise of ransomware attacks on NC schools hinder virtual learning

There have been 5 attacks on school districts in the past 8 months; there was only 1 reported in the previous 3 years

Brian Gordon USA Today Network
Published 12:34 p.m. ET Aug. 28, 2020 | Updated 9:44 a.m. ET Aug. 29, 2020

37

Timeline of A Ransomware Attack



Month 1
- An employee opens a phishing email and clicks on a link containing ransomware.

Month 2
- The ransomware downloads onto the employee's computer and starts executing malicious code.

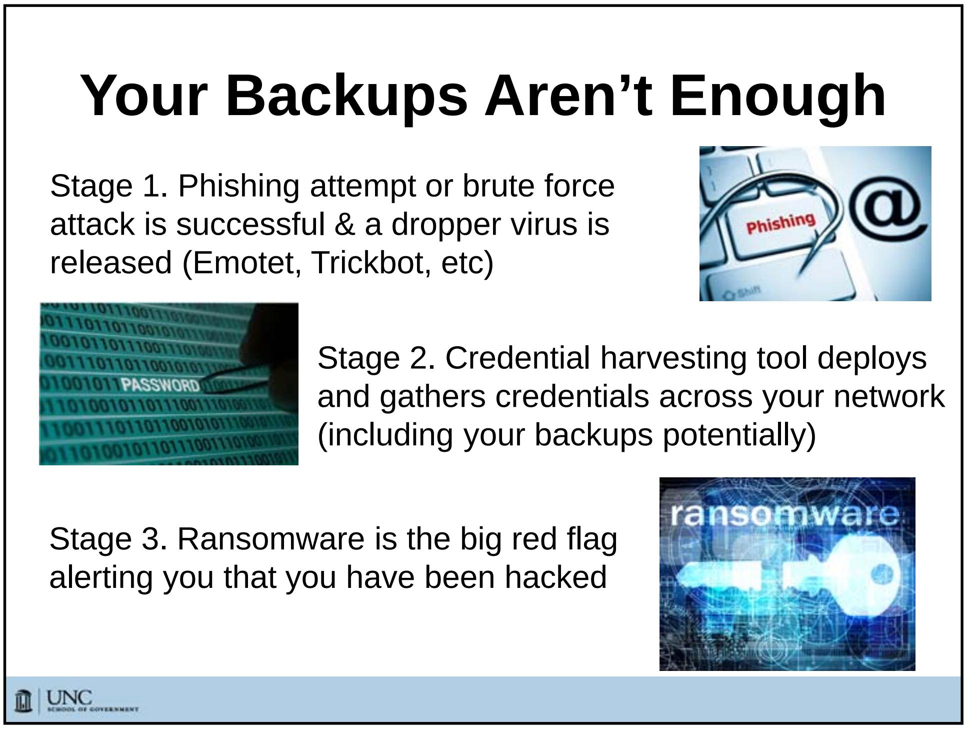
Month 3
- The ransomware creates a connection via the Internet with the threat actor's command and control (C2) server.

Month 4
- The ransomware steals/harvests credentials to gain access to more accounts.

Month 5
- The ransomware looks for files to encrypt on local computers and on servers via the network, moving laterally across the network to compromise multiple accounts. Data exfiltration might also be occurring during this timeframe.

Month 6
- The ransomware starts the encryption process, typically attacking domain controllers and backups first. The government is now aware they have been compromised. The threat actor leaves a ransom note demanding payment in exchange for the decrpytion key.

38



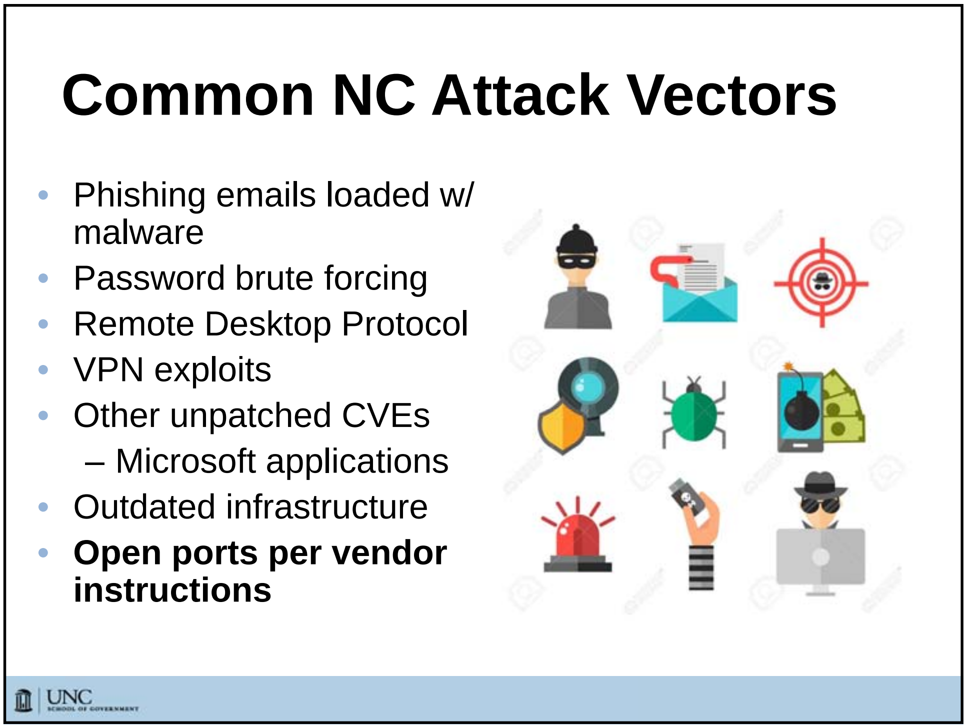
Your Backups Aren’t Enough

Stage 1. Phishing attempt or brute force attack is successful & a dropper virus is released (Emotet, Trickbot, etc)

Stage 2. Credential harvesting tool deploys and gathers credentials across your network (including your backups potentially)

Stage 3. Ransomware is the big red flag alerting you that you have been hacked

39



Common NC Attack Vectors

- Phishing emails loaded w/ malware
- Password brute forcing
- Remote Desktop Protocol
- VPN exploits
- Other unpatched CVEs
  - Microsoft applications
- Outdated infrastructure
- **Open ports per vendor instructions**

40

Polling Question

Be honest!

Do any of your vendors have persistent tunnels to “support” your software?

41

Business Email Compromise:

The $9 Billion Security Threat You Can’t Ignore

42

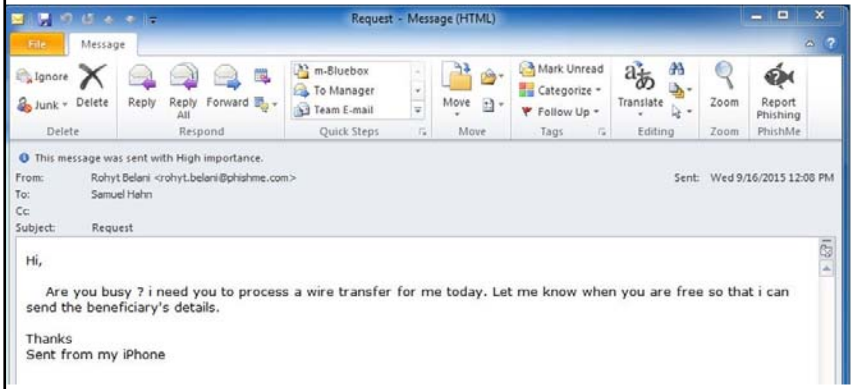
COUNTY & LOCAL

North Carolina county lost $1.7 million in email scam

- Cabarrus County, North Carolina, was the victim of an email scheme that diverted $2.5 million meant for the construction of a new high school in December of 2018.
- Though the county has recovered $776,518, more than $1.7 million remains unaccounted for.
- Most cyber insurance policies do not cover Business Email Compromise (BEC).

43

What Does it Look Like?



This message was sent with High importance.

From: Rohyt Belani <rohyt.belani@phishme.com>

Sent: Wed 9/16/2015 12:08 PM

To: Samuel Hahn

Cc:

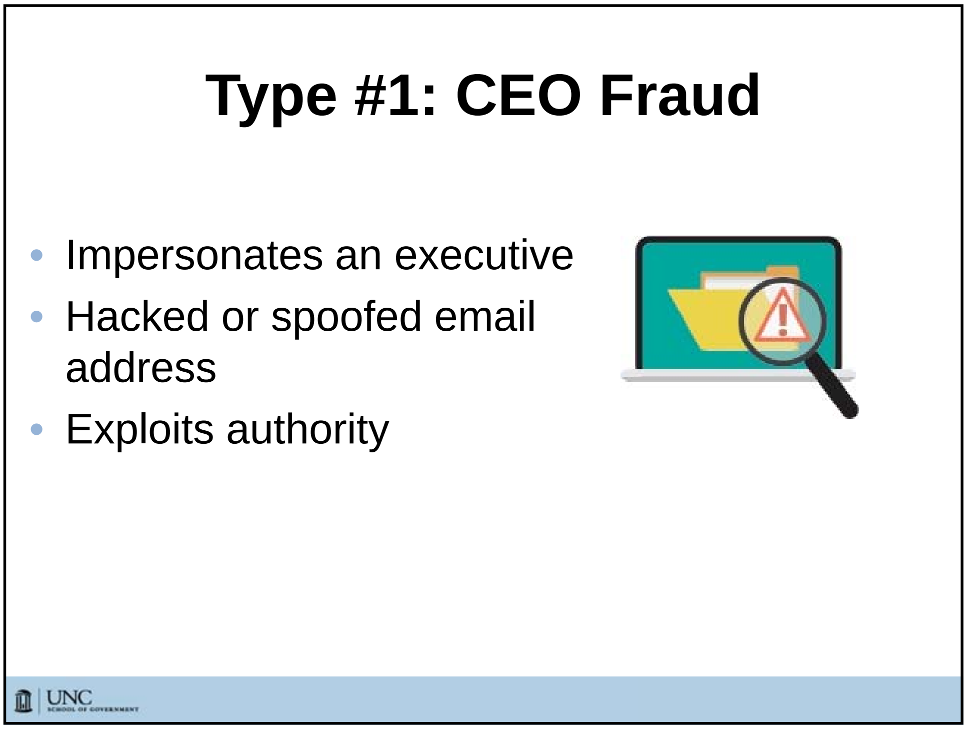
Subject: Request

Hi,

Are you busy ? i need you to process a wire transfer for me today. Let me know when you are free so that i can send the beneficiary's details.

Thanks
Sent from my iPhone

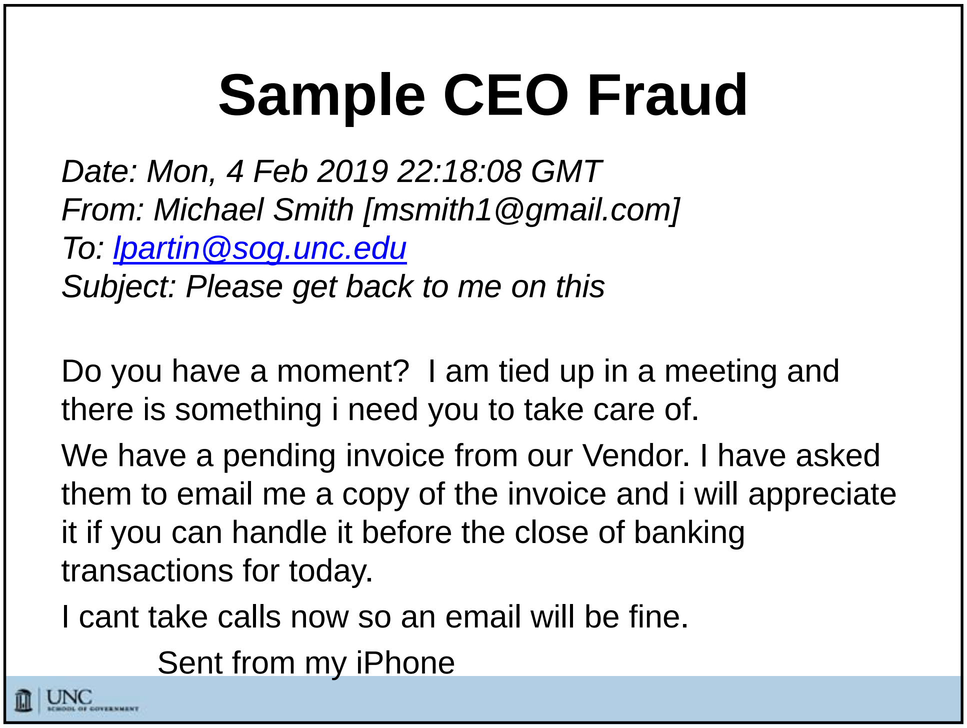
44



Type #1: CEO Fraud

- Impersonates an executive
- Hacked or spoofed email address
- Exploits authority

45



Sample CEO Fraud

Date: Mon, 4 Feb 2019 22:18:08 GMT
From: Michael Smith [msmith1@gmail.com]
To: lpartin@sog.unc.edu
Subject: Please get back to me on this

Do you have a moment? I am tied up in a meeting and there is something i need you to take care of.

We have a pending invoice from our Vendor. I have asked them to email me a copy of the invoice and i will appreciate it if you can handle it before the close of banking transactions for today.

I cant take calls now so an email will be fine.

Sent from my iPhone

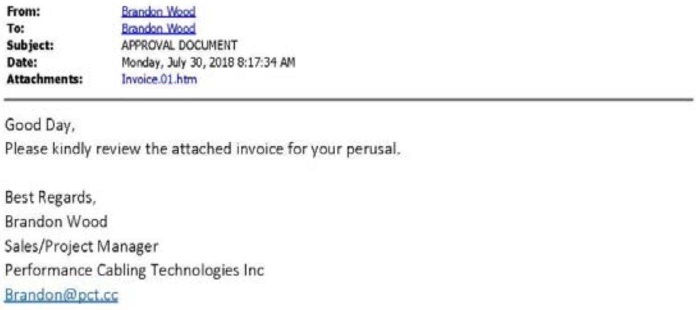
46

Type #2: Bogus Invoice Schemes

- Impersonate trusted vendor or supplier
- Use fake invoices
- Point you to new location for wire transfer

47

Bogus Invoices



From: Brandon Wood
To: Brandon Wood
Subject: APPROVAL DOCUMENT
Date: Monday, July 30, 2018 8:17:34 AM
Attachments: Invoice.01.htm

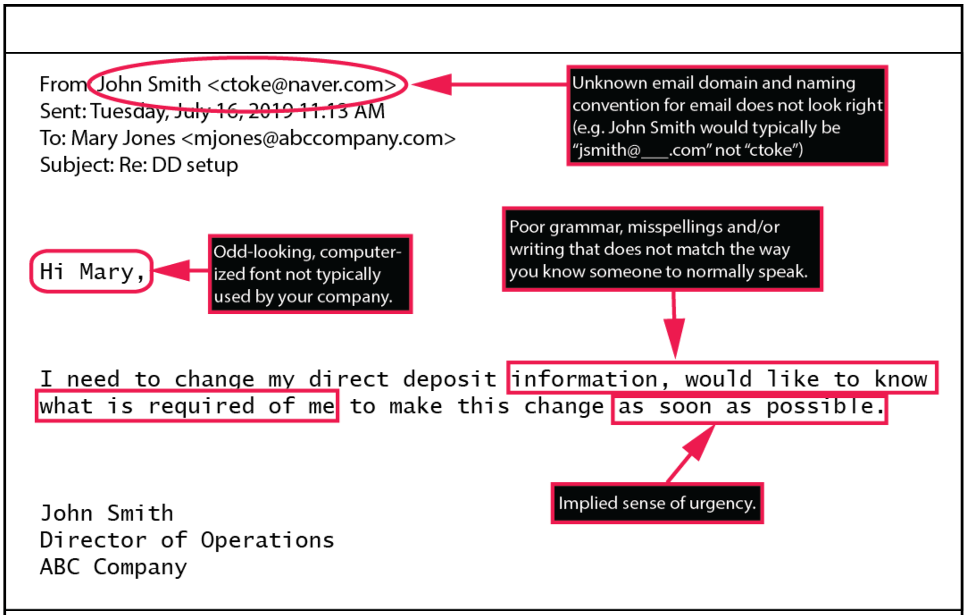
Good Day,
Please kindly review the attached invoice for your perusal.

Best Regards,
Brandon Wood
Sales/Project Manager
Performance Cabling Technologies Inc
Brandon@pct.cc

48

Direct Deposit Scams

49



From: John Smith <ctoke@naver.com>
Sent: Tuesday, July 16, 2019 11:13 AM
To: Mary Jones <mjones@abccompany.com>
Subject: Re: DD setup

Unknown email domain and naming convention for email does not look right (e.g. John Smith would typically be "jsmith@___.com" not "ctoke")

Hi Mary,

Odd-looking, computer-ized font not typically used by your company.

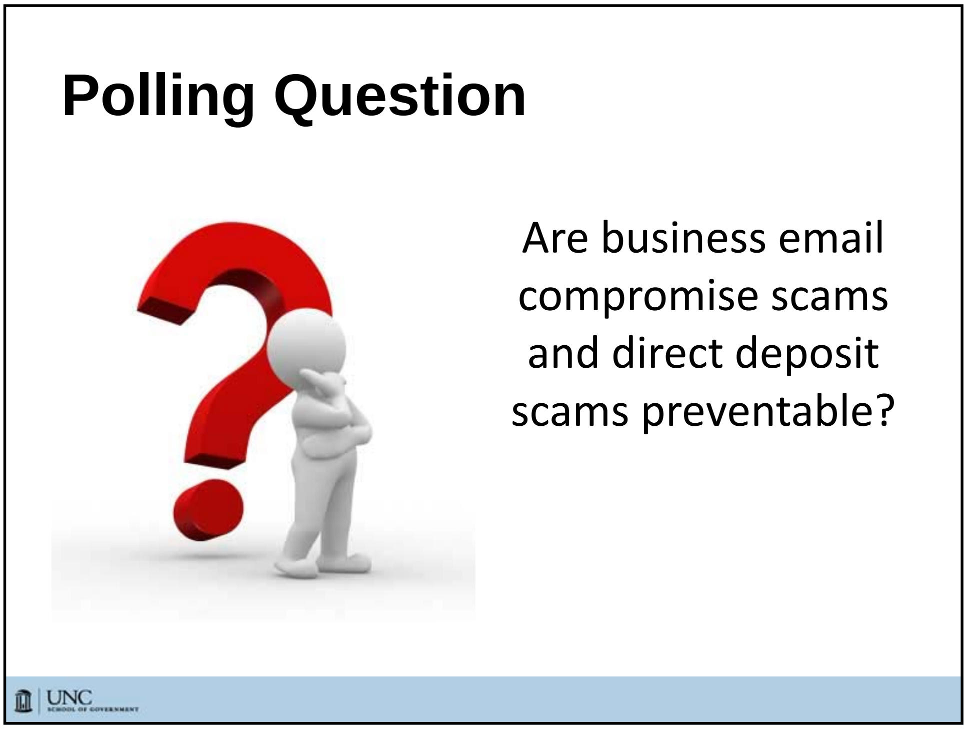
Poor grammar, misspellings and/or writing that does not match the way you know someone to normally speak.

I need to change my direct deposit information, would like to know what is required of me to make this change as soon as possible.

Implied sense of urgency.

John Smith
Director of Operations
ABC Company

50

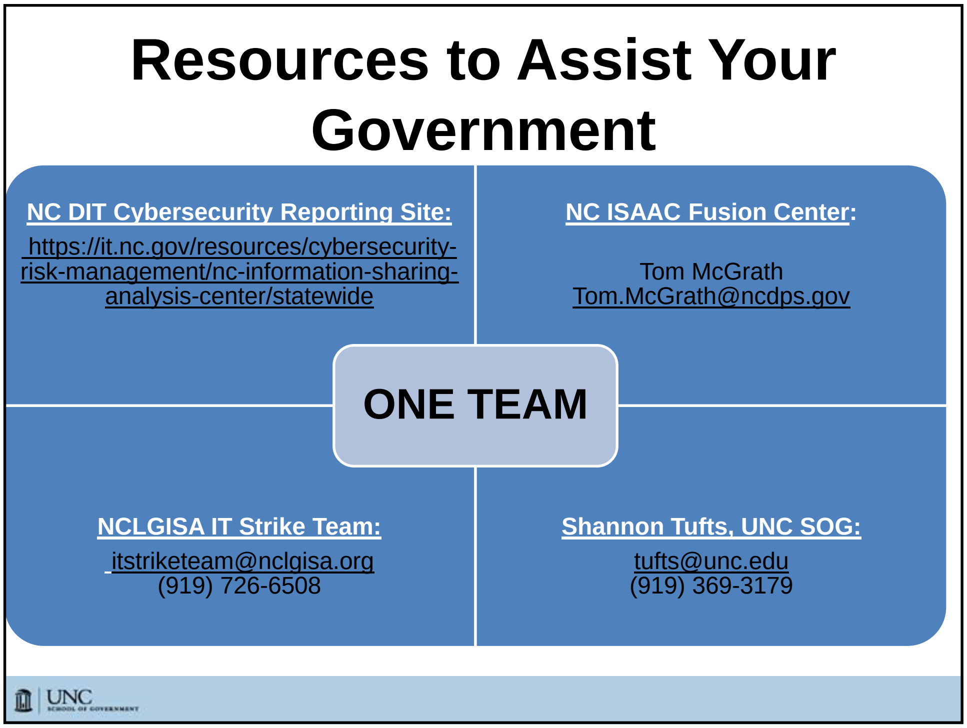


Polling Question

Are business email compromise scams and direct deposit scams preventable?

UNC
SCHOOL OF GOVERNMENT

51



Resources to Assist Your Government

NC DIT Cybersecurity Reporting Site:
https://it.nc.gov/resources/cybersecurity-risk-management/nc-information-sharing-analysis-center/statewide

NC ISAAC Fusion Center:
Tom McGrath
Tom.McGrath@ncdps.gov

ONE TEAM

NCLGISA IT Strike Team:
itstriketeam@nclgisa.org
(919) 726-6508

Shannon Tufts, UNC SOG:
tufts@unc.edu
(919) 369-3179

UNC
SCHOOL OF GOVERNMENT

52

NCLGISA IT Strike Team Recommendations for Non-IT Staff

1. If you suspect ransomware, contact your IT department immediately!
    1. They should start severing all Internet-based connections asap.

2. Don't turn off your computer/server, just disconnect it from the Internet (ethernet and wireless)

3. Do not try to stay up and "functional", as it will allow for rapid, catastrophic proliferation across your networks and into any interconnections you might have with neighboring entities.

** No, you cannot just turn on your computer really quickly and insert a flash drive for those files you really need.

53

6. Do not allow vendors to have open tunnels into your environment for remote support. Use a documented process for external access.

7. Do not use the same credentials for domain, system or software administration and your local accounts. Many of the recent breaches have involved compromised domain administrator credentials, which often are found to be the same as cached local administrator credentials.

8. Ask for immutable backups that are stored physically and virtually apart from the network for critical systems. After attacking the domain controller(s), most current variants go straight to encrypting your backups.

10. Determine what servers contain sensitive data (PHI, PII, financial data, CJIS data, etc) and keep this on file outside of the network.

54

16. Know your cyber-liability insurance policy well and have conversations with them prior to an event to determine their standard course of action (preferred vendors, etc).
17. Require user education for phishing messages and aggressive response to mitigate anyone who falls for phishing. Exposed credentials and malware downloads are part of the problem and can be limited with proper education.
18. Create a Continuity of Operations plan for your entity including defining who will serve as Incident Commander and drill it to make sure it works for your team!
19. Work with senior leadership to create a prioritization document for bringing departments/applications back online.

55

Questions

56