


**Cybersecurity:
Protecting Yourself, Your
Organization, and Your Client Data**



UNC
SCHOOL OF GOVERNMENT

www.sog.unc.edu

Shannon Tufts, PhD
Associate Professor of Public Law
and Government
919.962.5438
tufts@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>

UNC
SCHOOL OF GOVERNMENT

2

Cyber Security Knowledge  **QUIZ**

Q1. What does the https:// at the beginning of a URL mean?

UNC
SCHOOL OF GOVERNMENT

Pro Tip

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

UNC
SCHOOL OF GOVERNMENT

4

Cyber Security Knowledge QUIZ

Q2. 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?

UNC
SCHOOL OF GOVERNMENT

5

Pro Tip

Never Pay!

UNC
SCHOOL OF GOVERNMENT

Cyber Security Knowledge QUIZ

Q3. Which of the following passwords is most secure?

UNC
SCHOOL OF GOVERNMENT

7

Pro Tip

Password

- ❖ 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)

UNC
SCHOOL OF GOVERNMENT

8

Cyber Security Knowledge QUIZ

Q4. Which of these options is a form of two-factor authentication?

UNC
SCHOOL OF GOVERNMENT

Pro Tip

- ❖ 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.

UNC
SCHOOL OF GOVERNMENT

10

Cyber Security Knowledge

Q5. 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?

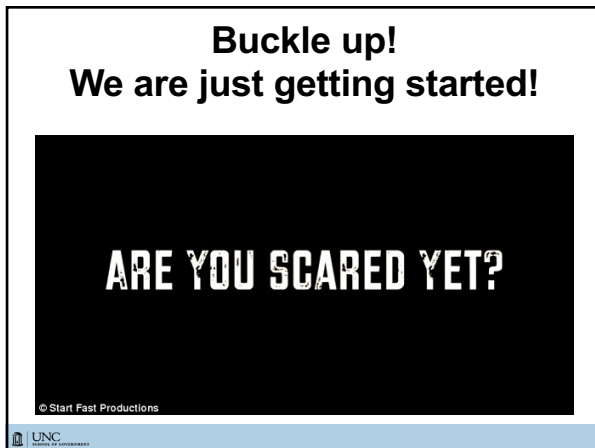
UNC
SCHOOL OF GOVERNMENT

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.

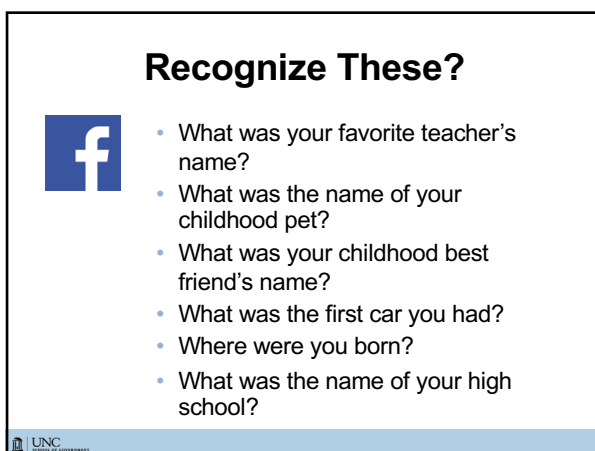
UNC
SCHOOL OF GOVERNMENT



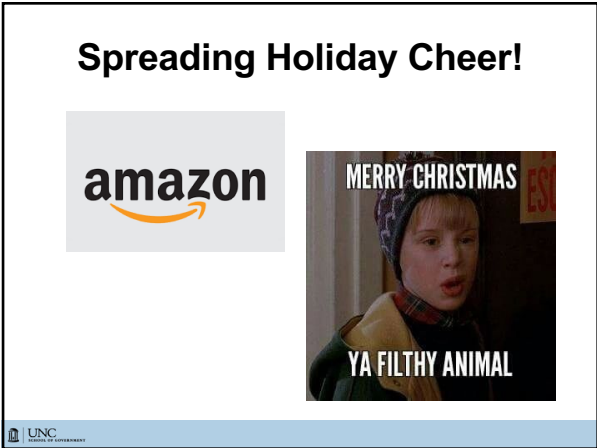
13



14



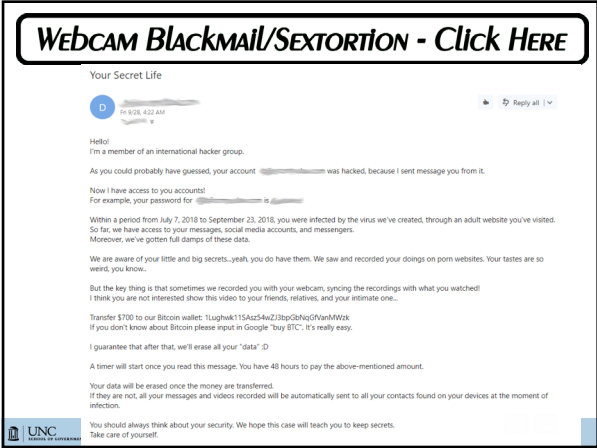
15



16



17







19

Hacker 101: Build Trust

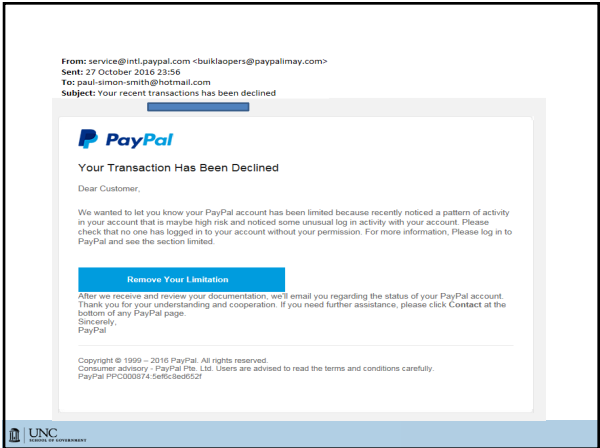
- Spear phishers personalize emails to try to gain your trust
 - Full name
 - Mailing address
 - Name of your employer
 - Personal Data (SSN, Banking Account Number, etc)

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

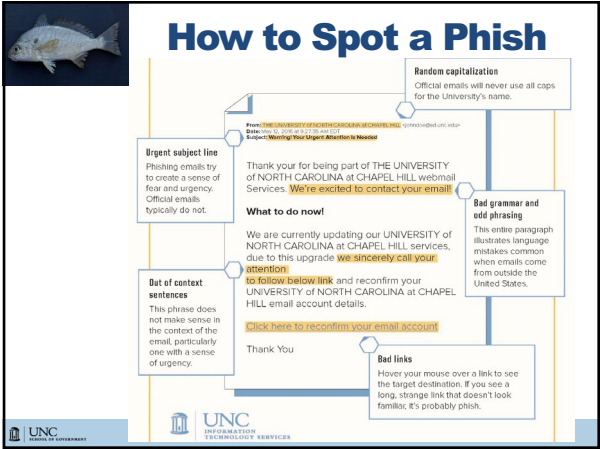


20

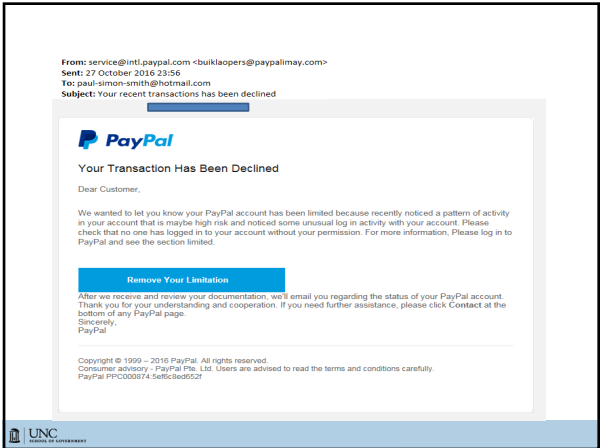


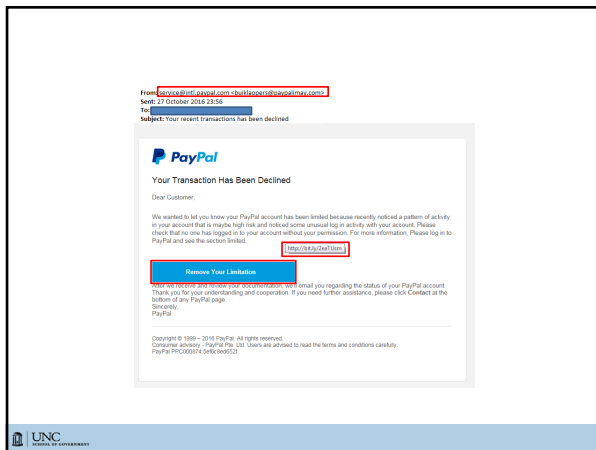


22

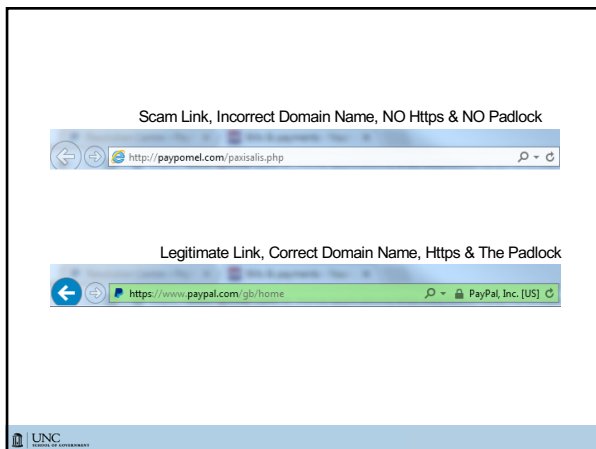


23






25



26



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

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






28

Voice Phishing Example





29





What Is It?

pay up OR ELSE!

- Ransomware is a type of malware that attempts to extort money from a computer user by infecting or taking control of the victim's computer, or files, or documents stored on it.
- Ransomware will either lock or prevent normal usage, or encrypt the documents and files on it to prevent access to the saved data.

UNC
SCHOOL OF GOVERNMENT

31

GOVERNING
THE STATES AND LOCALITIES

FRANCE | HEALTH | INFRASTRUCTURE | MISDE | WORKFORCE | POLITICS | PUBLIC SAFETY | URBAN | EDUCATION | DATA | PUBLIC OFFICIALS OF THE YEAR | WOMEN IN GOV

MAGAZINE | NEWSLETTERS | PRODUCTS | EVENTS | PAPERS

MANAGEMENT & LABOR

Ransomware Attack Hits Computer Network of North Carolina County

MARCH 21, 2019 AT 7:40 AM

By Zachery Eames

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

UNC
SCHOOL OF GOVERNMENT

32

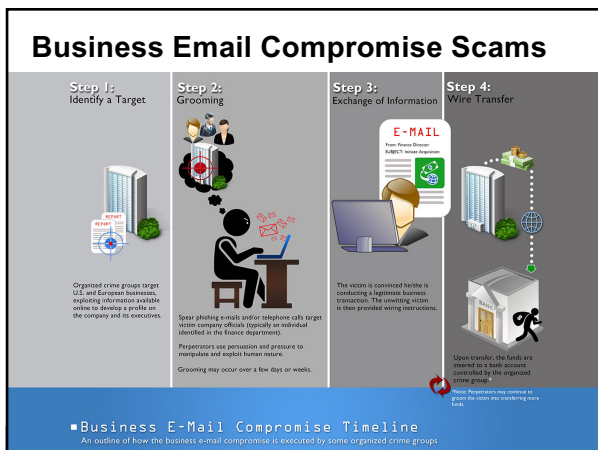
Your Backups Aren't Enough

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


UNC
SCHOOL OF GOVERNMENT



34

Type #1: CEO Fraud

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



UNC
SCHOOL OF GOVERNMENT

35

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


UNC
SCHOOL OF GOVERNMENT

Type #2: Bogus Invoice Schemes

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

INVOICE

FALSE



37

Bogus Invoices

From: Brandon Wood

To: Brandon Wood


Subject: APPROVAL DOCUMENT

Date: Monday, July 30, 2018 8:17:34 AM

Attachments: Invoice(1).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



38

App State fleeced for almost \$2 million by scam; feds get most of the money back

- In 2016, Appalachian State hired Charlotte-based Rodgers Construction to build its new health science college facility. That October, the company filed a form with the school to establish wire transfers and direct deposits.
- Two months later, a staff member in the App State's controller's office received an email purported to be from Doug McDowell, the controller for Rodgers Construction.
- The email included a new direct deposit form along with instructions that the school should reroute company payments to a bank account at JPMorgan Chase. About a week later, some \$1.96 million was sent to the new location.
- On Dec. 20, the *real* Doug McDowell contacted App State to ask why the company had not received its money.



39

Avoiding BEC Scams

- Always check the sender and verify it is legitimate
- Check reply-to addresses as well
- Check links before clicking

40

Direct Deposit Scams

PHISHING SCAM

DIRECT DEPOSIT CONFIRMATION

Current \$659.16 Year to Date \$3,004.96

ment has be

Description TAXABLE

41

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

Hi Mary,

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.

John Smith
Director of Operations
ABC Company

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

Odd-looking, computerized 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.

Implied sense of urgency.

North Carolina Stats



UNC
SCHOOL OF GOVERNMENT

43

North Carolina Government Cyber Statistics

180+ counties, cities, K-12s, and state government systems attacked since 2013

- North Carolina had 10 (reported) ransomware attacks in 2019 and another 10 in 2020 (as of May 30).

TOP 10 STATES BY VICTIM LOSS¹⁰



- FBI's 2018 Internet Crime Repc
 - Top 10 for victim loss
 - 7,7523 Victims
 - \$137,230,988 total loss
 - 1,997 complaints

UNC
SCHOOL OF GOVERNMENT

44

Legislative Updates

House Bill 217

"§ 143B-1379. State agency cooperation and training; liaisons; county and municipal government reporting.

- ✓ Updates the definition of what is reportable and adds the term and definition of "Significant cybersecurity incidents"
- ✓ Adds to the liaisons tasks to provide corrective action plans
- ✓ Includes Privacy as a requirement and not just Security
- ✓ Excludes military personnel identified as security liaisons from requiring background investigations in lieu of security clearances
- ✓ Legislatively mandates cyber awareness training and reporting (includes contractors)
- ✓ Requires that county and municipal government report cybersecurity incidents.
- ✓ Further clarify that cyber incident information shared to DIT will be protected under G.S. 132-6.1(c)
- ✓ Encourages private sector entities to report cyber incidents

Link to report incidents: <https://it.nc.gov/resources/cybersecurity-risk-management/statewide-cybersecurity-incident-report-form>

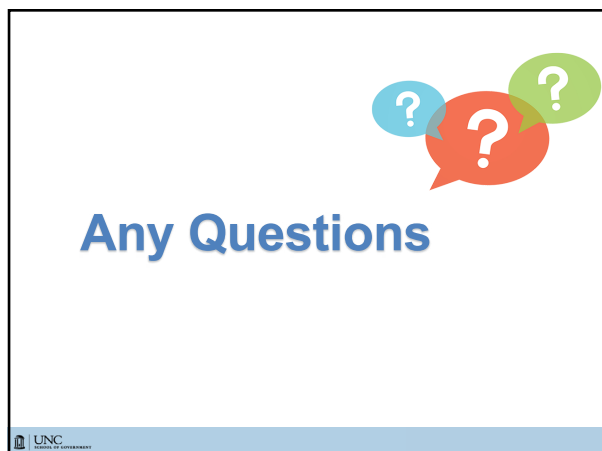
UNC
SCHOOL OF GOVERNMENT

Shann⁴⁵
Assoc
Government

tufts@sog.unc.edu; 919.962.5438



46



47
