

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

UNC
SCHOOL OF GOVERNMENTwww.sog.unc.edu

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

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

Pro Tip



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!



5


Pro Tip

Never Pay!



ransomware victims who paid but never got their files back

20%




6

Cyber Security Knowledge

QUIZ

Which of the following passwords is most secure?


1. Boat123
2. WTh!5Z
3. into*48
4. 12345
5. I have no clue!




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)




8

Cyber Security Knowledge

QUIZ

Which of these options is a form of two-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

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.




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

UNC

SCHOOL OF GOVERNMENT

13

SOCIAL
ENGINEERING

The clever manipulation
of the natural human
tendency to trust.

JIMMY
Kimmel

LIVE!

UNC

SCHOOL OF GOVERNMENT

14

Recognize These?

f

- 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?

UNC

SCHOOL OF GOVERNMENT

15

Spreading Holiday Cheer!

amazon

MERRY CHRISTMAS

ES

YA FILTHY ANIMAL

UNC

SCHOOL OF GOVERNMENT

16

Shannon H Tufts, PhD

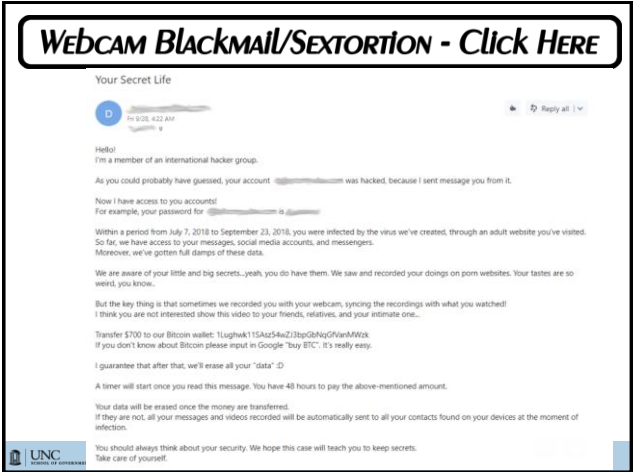
Associate Professor of Public Law & Government

tufts@sog.unc.edu; 919.962.5438

4



17



18



19

Cyber Security Knowledge

Examples of a “phishing attack” that you may have received:

1. Sending someone an email that contains a malicious link that is disguised to look like an email from someone they know/trust.
2. Creating a fake website that looks nearly identical to the real website in order to trick users to entering their login information.
3. Sending someone a text message that contains a malicious link that is disguised to look like a notification that the person won a contest.

20



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




21



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.




22

From: service@intl.paypal.com <bulkaop@paypalmay.com>

Sent: 27 October 2016 23:56

To: paul-simon-smith@hotmail.com

Subject: Your recent transactions has been declined



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.

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 PPC000874.5ef6cbed052f



23



How to Spot a Phish

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

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

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

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

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.

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.


Phishing email example:
From: THE UNIVERSITY OF NORTH CAROLINA AT CHAPEL HILL <communications@unc.edu>
Date: Wednesday, October 26, 2016 12:01 PM
Subject: **Urgent: Important! Your Urgent Attention is Needed**

Thank you 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



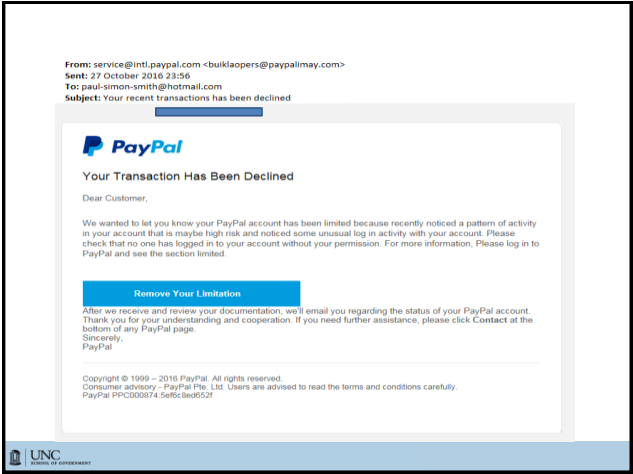
24

Shannon H Tufts, PhD

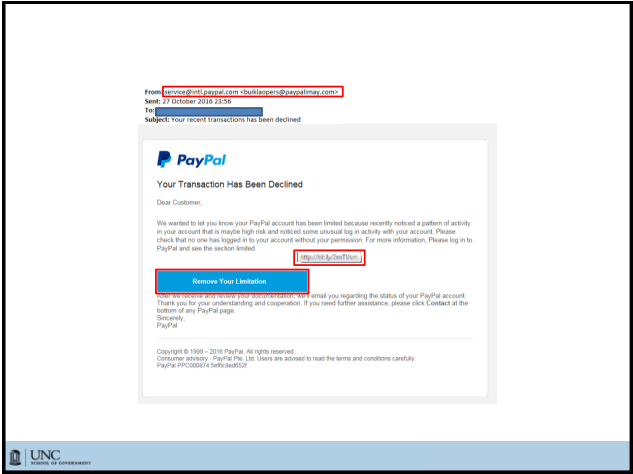
Associate Professor of Public Law & Government

tufts@sog.unc.edu; 919.962.5438

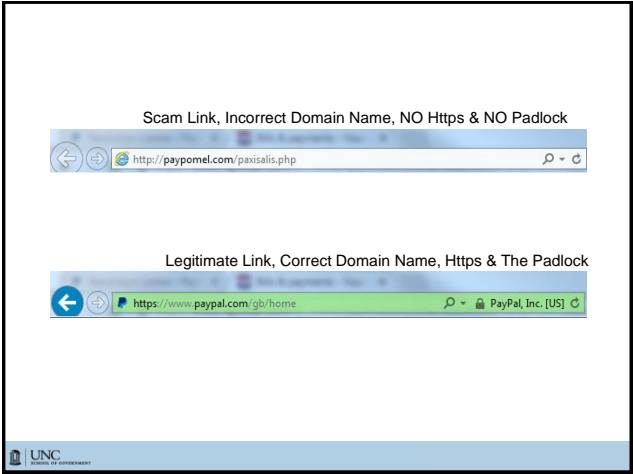
6



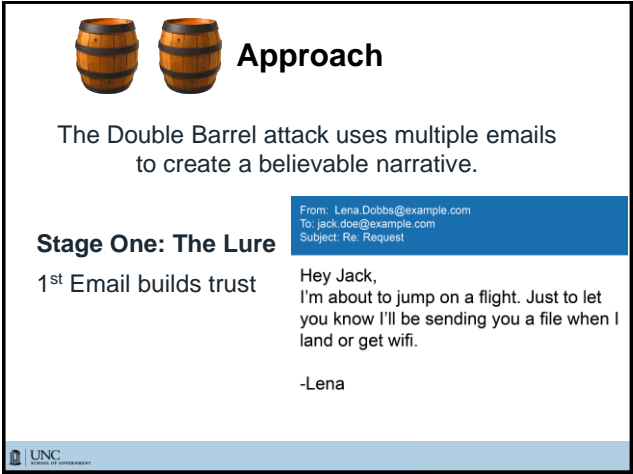
25



26



27



28

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






29

Voice Phishing Example






30






31

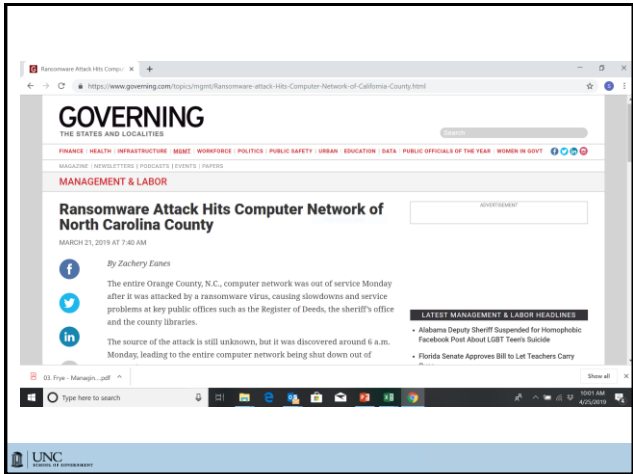
What Is It?



- 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.



32






33


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







34



Type #1: CEO Fraud

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





37

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




38

Type #2: Bogus Invoice Schemes

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






39

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



40

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.



41

Avoiding BEC Scams

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



42

Direct Deposit Scams





43

North Carolina Stats







44

NC Government Cyber 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 Oct 1, 2020, we have over 20 confirmed ransomware events in NC jurisdictions.
- Exponential growth in attacks and attack vectors
- Disturbing trend with data exfiltration





45


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>



46



Any Questions



47