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

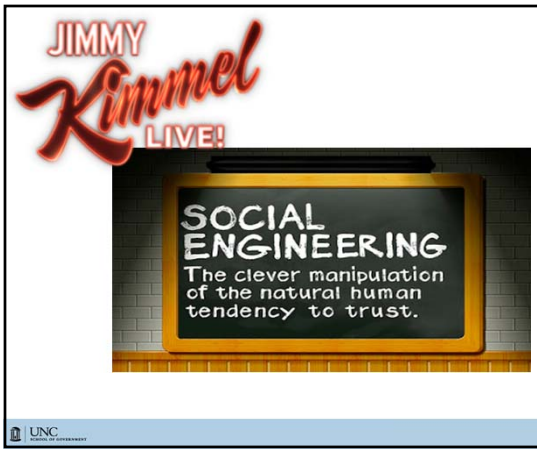
UNC SCHOOL OF GOVERNMENT www.sog.unc.edu

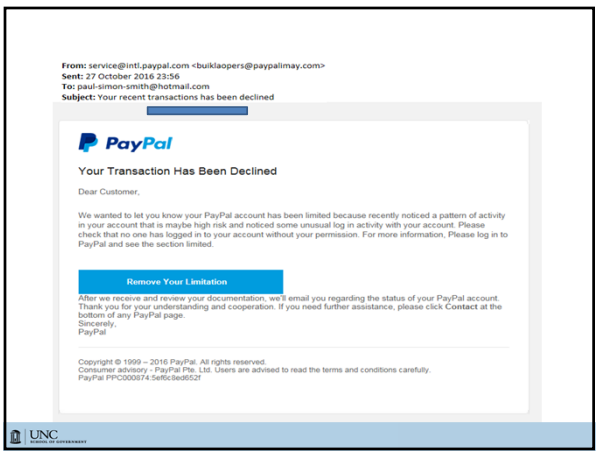
Shannon Tufts, PhD
Associate Professor of Public Law and Government
919.962.5438
tufts@unc.edu

AGENDA

- Cybersecurity – Why It Matters
- Social Engineering
- Types/Strategies of Attacks
  - Ransomware/Malware
  - Phishing
  - Business Email Compromise
- What to Look For: Protect Yourself & Your Clients
- Q&A

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





Shannon H Tufts, PhD
Associate Professor of Public Law & Government
tufts@sog.unc.edu; 919.962.5438

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

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

UNC

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

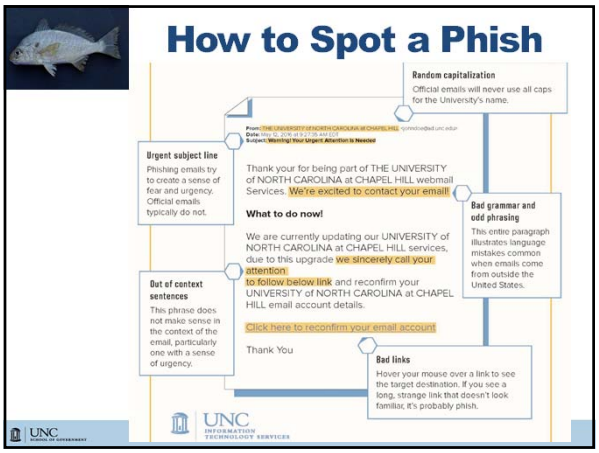
Jack,

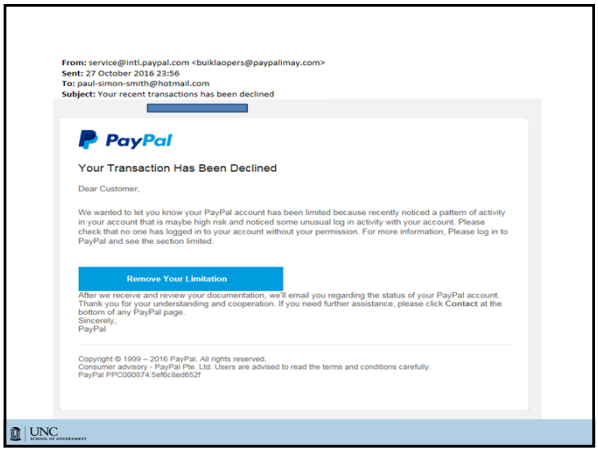
Thank you for your patience.
Attached is the file I need you to review.

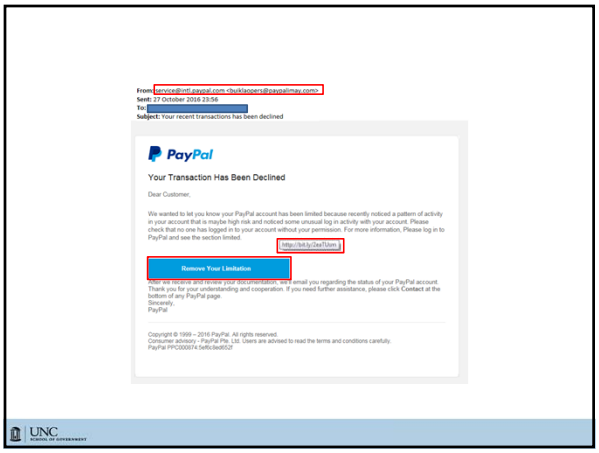
Thanks for your help.
-Lena

UNC

Shannon H Tufts, PhD
Associate Professor of Public Law & Government
tufts@sog.unc.edu; 919.962.5438



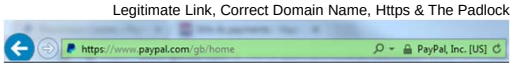




Shannon H Tufts, PhD
Associate Professor of Public Law & Government
tufts@sog.unc.edu; 919.962.5438

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

Legitimate Link, Correct Domain Name, Https & The Padlock



UNC

Voice Phishing Example

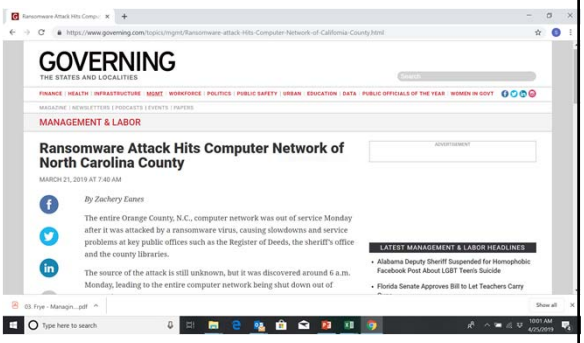
UNC

UNC

Shannon H Tufts, PhD
Associate Professor of Public Law & Government
tufts@sog.unc.edu; 919.962.5438

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.



Your Backups Aren't Enough

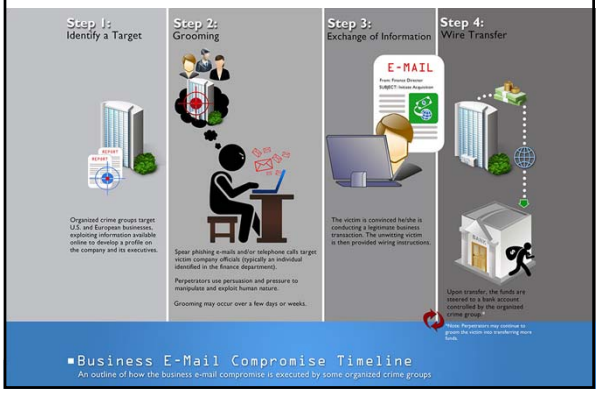
Stage 1. Phishing attempt or brute force attack is successful & a dropper virus is released (Emotet, Trickbot, etc)

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

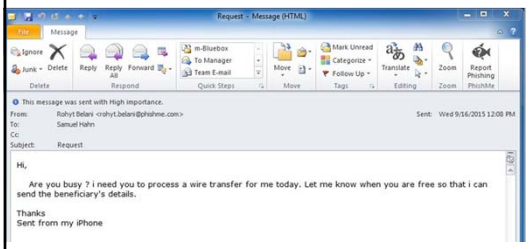
Stage 3. Ransomware is the big red flag alerting you that you have been hacked

Shannon H Tufts, PhD
Associate Professor of Public Law & Government
tufts@sog.unc.edu; 919.962.5438

Business Email Compromise Scams



What Does it Look Like?



Type #1: CEO Fraud

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

Shannon H Tufts, PhD
Associate Professor of Public Law & Government
tufts@sog.unc.edu; 919.962.5438

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

Type #2: Bogus Invoice Schemes

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

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

Shannon H Tufts, PhD
Associate Professor of Public Law & Government
tufts@sog.unc.edu; 919.962.5438

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.

UNC

Avoiding BEC Scams

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

UNC

Random Bait to Chew On

1 **Top phishing disguises:**
- Bills / Invoices (15.9%)
- Email delivery failures (15.3%)
- Legal / Law enforcement (13.2%)
- Scanned documents (11.5%)
- Package delivery (3.9%)

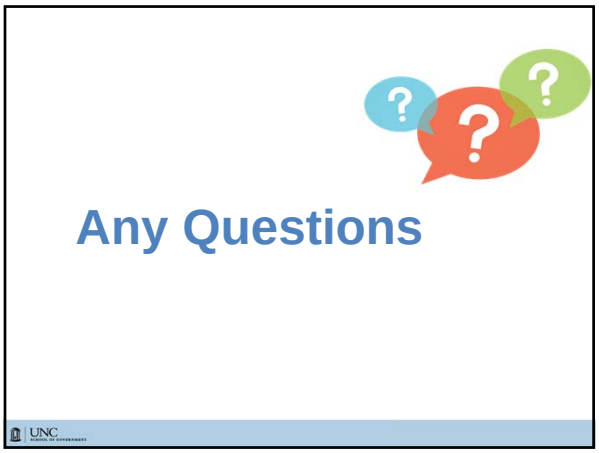
2 **Top malicious attachments:**
- Office files (38%)
- Archive files [.zip/etc.] (37%)
- PDF files (14%)

3 **Top Phishing Lures:**
- Dropbox Accounts
- Financial Institutions
- Generic Email Credential Harvesting

4 **Highest Click Rates:**
- Docusign (7%)
- Dropbox (2%)
- IRS (1%)

UNC 27

Shannon H Tufts, PhD
Associate Professor of Public Law & Government
tufts@sog.unc.edu; 919.962.5438



Shannon H Tufts, PhD
Associate Professor of Public Law & Government
tufts@sog.unc.edu; 919.962.5438