



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



Shannon Tufts, PhD  
Associate Professor of Public Law  
and Government  
919.962.5438  
[tufts@unc.edu](mailto:tufts@unc.edu)

 [www.sog.unc.edu](http://www.sog.unc.edu)

### Webcam Blackmail/SEXTORTION - Click HERE

Your Secret Life

Hi!

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 your accounts!  
For example, your password for [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 dumps 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: 1Ughmk115Acq4wz23pp2bNq9VnWw2k  
If you don't know about Bitcoin please type 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.

## AGENDA

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


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

## 93% of all breaches or incidents



**"PHISHING"**


- 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



### SOCIAL ENGINEERING

The clever manipulation of the natural human tendency to trust.

From: service@intl.paypal.com <bulkaopers@paypalimay.com>  
Sent: 27 October 2016 23:58  
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 PFC000074-6ef5c6e0c07


## 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.



## How to Spot a Phish



- Random capitalization**  
Official emails will never use all caps for the University's name.
- Urgent subject line**  
Phishing emails try to create a sense of fear and urgency. Official emails typically do not.
- Bad grammar and odd phrasing**  
This entire paragraph illustrates language mistakes common when emails come from outside the United States.
- But of content sentences**  
This phrase does not make sense in the context of the email, particularly one with a sense of urgency.
- What to do now!**  
We are currently updating our UNIVERSITY of NORTH CAROLINA at CHAPEL HILL webmail Services. **We're excited to contact your email!** **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.



## Approach

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



**Stage One: The Lure**

1<sup>st</sup> 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 wif.

-Lena

From: service@intl.paypal.com <bulksapers@paypal.com>  
Sent: 27 October 2016 23:56  
To: paul-simon-smth@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 Plus, Ltd. Users are advised to read the terms and conditions carefully.  
PayPal PFC000874-5e65c8e852f



## 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

From: service@intl.paypal.com <bulksapers@paypal.com>  
Sent: 27 October 2016 23:56  
To: paul-simon-smth@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.

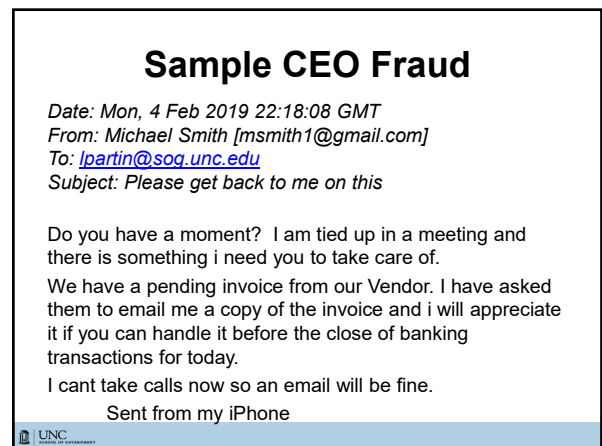
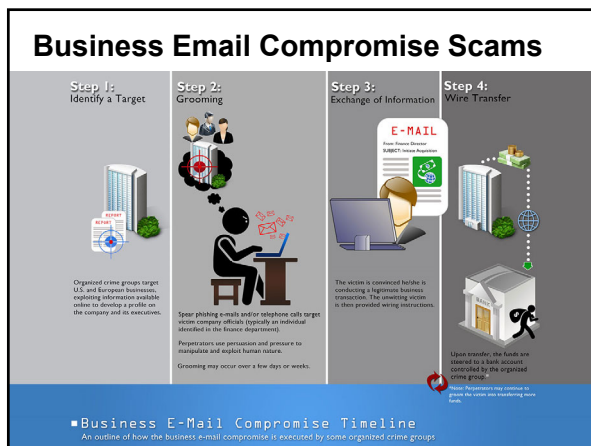
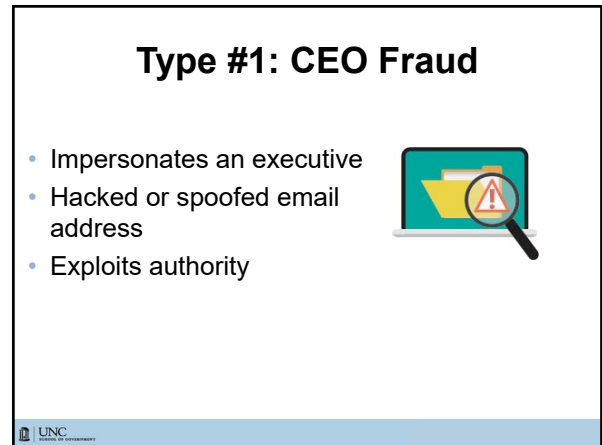
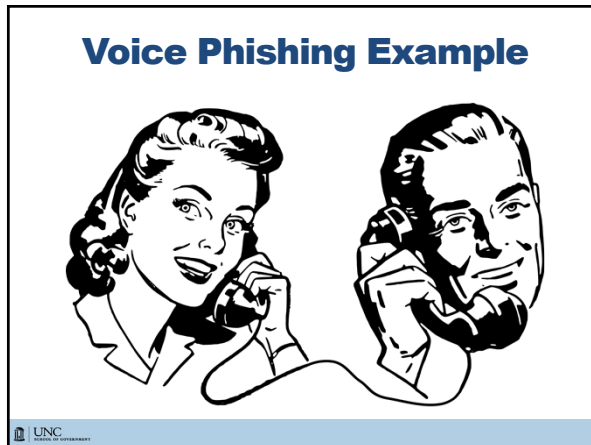
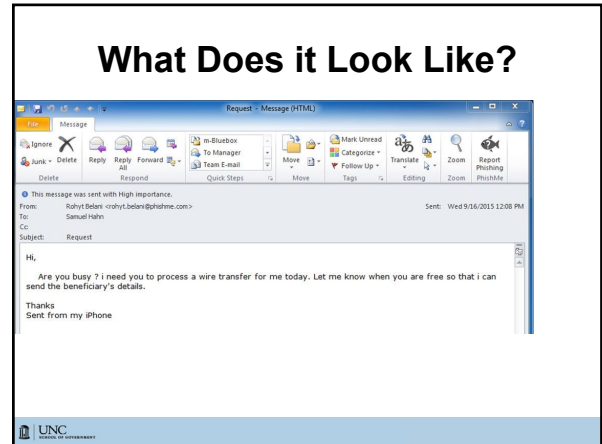
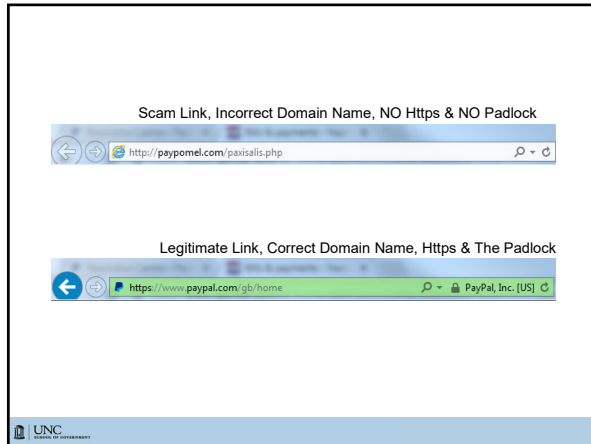
**Remove Your Limitation**

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 Plus, Ltd. Users are advised to read the terms and conditions carefully.  
PayPal PFC000874-5e65c8e852f





## Type #2: Bogus Invoice Schemes

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



## Avoiding BEC Scams

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

## 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@pctc.com](mailto:Brandon@pctc.com)

## Random Bait to Chew On

- |  |   |
|--|---|
| <p><b>1 Top phishing disguises:</b></p> <ul style="list-style-type: none"> <li>• Bills / Invoices (15.9%)</li> <li>• Email delivery failures (15.3%)</li> <li>• Legal / Law enforcement (13.2%)</li> <li>• Scanned documents (11.5%)</li> <li>• Package delivery (3.9%)</li> </ul> | <p><b>2 Top malicious attachments:</b></p> <ul style="list-style-type: none"> <li>• Office files (38%)</li> <li>• Archive files [.zip/etc.] (37%)</li> <li>• PDF files (14%)</li> </ul> |
| <p><b>3 Top Phishing Lures:</b></p> <ul style="list-style-type: none"> <li>• Dropbox Accounts</li> <li>• Financial Institutions</li> <li>• Generic Email Credential Harvesting</li> </ul>  | <p><b>4 Highest Click Rates:</b></p> <ul style="list-style-type: none"> <li>• DocuSign (7%)</li> <li>• Dropbox (2%)</li> <li>• IRS (1%)</li> </ul>                                      |

## 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.



## Any Questions