Everyday Security

University at Buffalo
Information Security Office

What Are They After?

Yes, Universities are Targets, Too!

"In early 2014, malicious cyber actors successfully executed an e-mail phishing attack against 166 employees at an identified US university. The phishing message was embedded with a malicious link to a fraudulent university website that, when accessed, prompted employees to provide PII associated with their financial accounts. The actors successfully compromised the financial accounts of two employees, changing their direct deposit information so that money was delivered to an unspecified US bank, resulting in financial losses for the employees, according to an FBI contact…"

https://info.publicintelligence.net/DHS-UniversityCyberThreats.pdf

What? Money? How?

- Spamming from your account
- Click fraud from your computer
- Purchasing refundable air travel
- Redirecting your paycheck
- Extortion

Why is security important?

- NYS Information Security Breach Notification Act
- FERPA (Student Records)
- HIPAA (Health Information)
- GLBA (Financial)
- PCI (Credit Card Transactions)
- Personal risk

Consequences

- Fines
  - HIPAA - $1.5M per incident
  - NYS (SSN) – $10-$200 per SSN lost
  - PCI – Loss of ability to conduct transactions
- Lawsuits
  - Lose someone's SSN, they may sue for damages
- Overhead
  - Setup of call centers to answer questions, buying credit protection, etc

Consequences

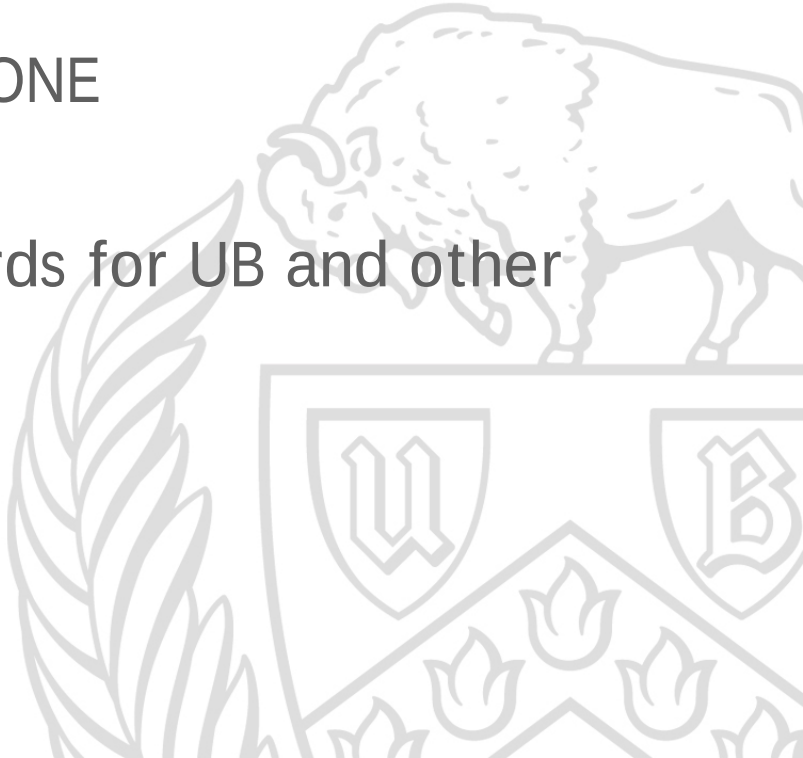
- Reputational concerns – faculty, students, parents, staff, granting agencies
- Growing social expectations due to wide-spread media coverage of identity theft

Risk To You

- Identity Theft
  - Thieves aren't just after the data you have access to, they're happy to take yours too!
- Financial Loss
  - Use the same password everywhere? Bad idea!

Basic Best Practices

- Passwords
  - Should be long/strong
  - Don't share them with ANYONE
  - Don't write them down
  - Don't use the same passwords for UB and other accounts



Basic Best Practices (cont.)

- Lock workstation/shut down when not in use
- Make sure software is up to date
  - Both OS and Applications
  - Secunia PSI for home
- Make sure AV software is up to date
- Firewall software should be enabled
- Recognize that email is NOT secure

Technology Implemented!
So now, are we safe?

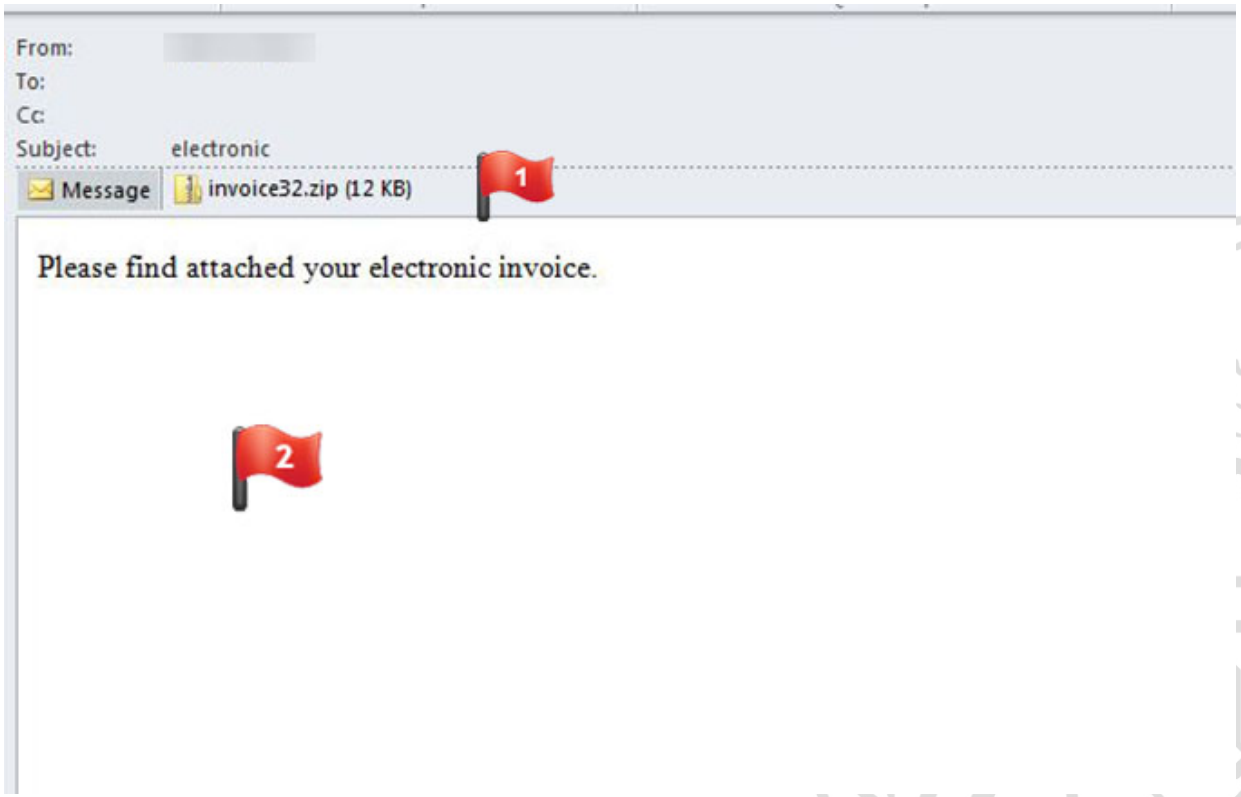
NO!!!

Huh…why not?

Physical Security – a parallel example

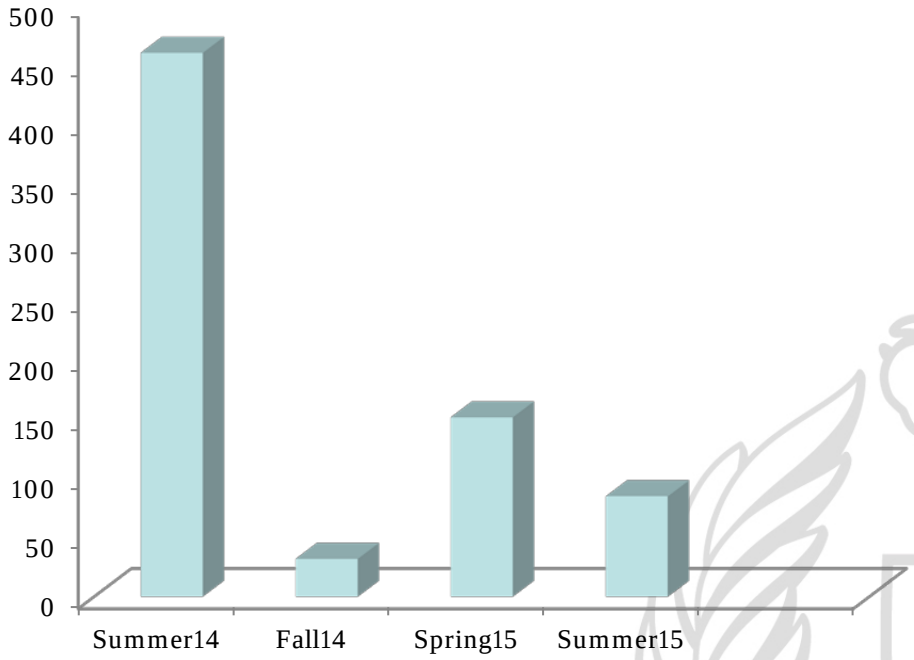
https://www.simpsonsworld.com/video/316046915870/episode/357630019692

Email: Infected Attachments

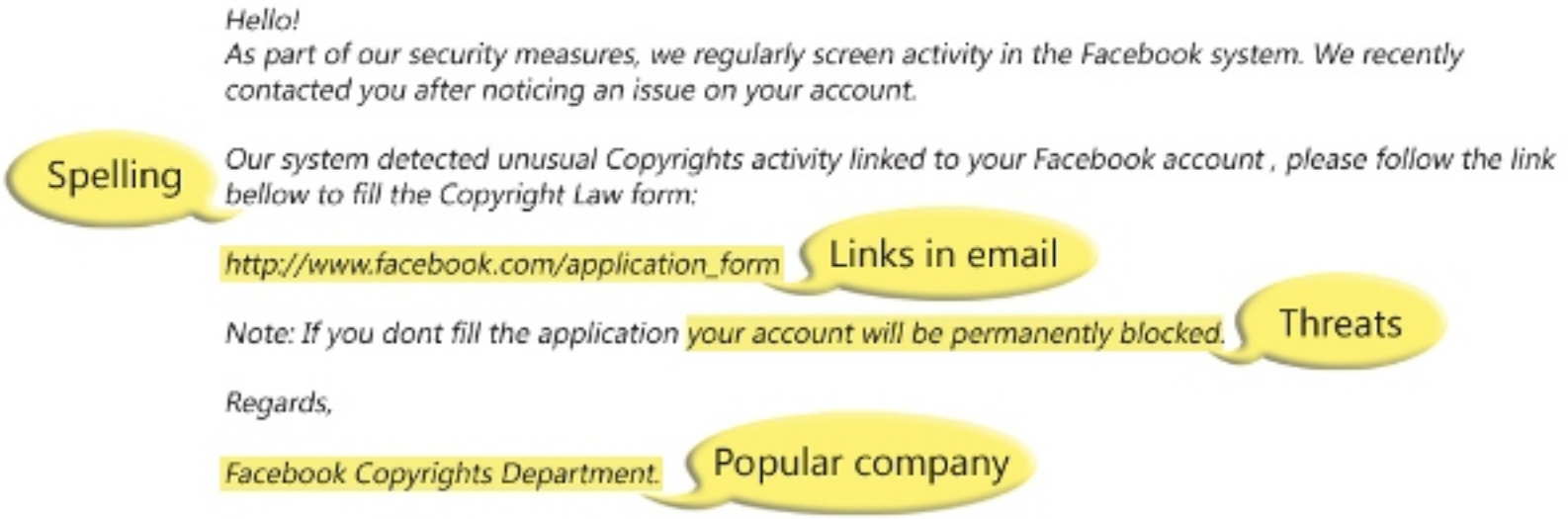


Email: Phishing!

UBIT Account Compromises



What does a phishing email message look like?



http://www.microsoft.com/security/online-privacy/phishing-symptoms.aspx

HINT: email does not come from official "@buffalo.edu" address

From: UB Technical Support <supportmessaging@abusemessage.buffalo.edu>
Date: May 23, 2013, 6:30:27 AM EDT
To: [redacted]@buffalo.edu
Subject: Urgent Message, Please Read

HINT: hovering on images/URLs shows you they do not link to "buffalo.edu"

ATTENTION UB,

Your email has been spammed too many times demanding for your email and password in other to protect your email account from been hacked further. The University board has decided to protect your account in a secured manner. This means helps in encrypting your password in our database to protect you from receiving spammed message.

ACTIVATE YOUR EMAIL PROTECTION LINK HERE

http://www.junewon.org/pm/images/Horde.htm

Admin Support

HINT: grammar

From: UBSupport Team [mailto:Support@teambuffalomail.edu]
Sent: Tuesday, May 14, 2013 11:18 AM
To: [redacted]@buffalo.edu
Subject: Important Mail: Virus Attack

HINT: email is not from "@buffalo.edu"

HINT: hovering on images/URLs shows you they do not take you to "buffalo.edu"

UB Email User,
We have detected a Trojan Horse Virus attack on your system which has compromised your email address. Kindly update your email address with us now to protect it from further damage.
PRESS HERE NOW

http://sims-it.net/wp-includes/js/jcrop/Web_Access.htm

Email Supp
University of Buffalo

NB: If you receive this message in your Junk folder and the Link refuses to click, please move this message to your Inbox folder to allow you click on the link.

HINT: not @buffalo.edu

----- Original Message -----
From: @yahoo.com
To:
Sent: Wed 05/01/13 5:25 AM
Subject: Fwd: Emergency

Sorry to bother you about this
I am presently in London, UK and am facing some difficulties here because i misplaced my wallet where my money and credit card were kept. Presently my passport and belongings have been seized by the hotel management pending when i settle my bills.

I need you to lend me 2,000 GBP to settle my hotel bills and get myself back home. I have reported the incident to the police here but they are not responding to the matter effectively.

I will reimburse the money as soon as i return. Please let me know if you can be of help ASAP. I don't have a phone where i can be reached, i only have limited access to internet here.

, J.D., M.A., Ph.D.
ProfessorSUNY at Buffalo Law School
e-mail: @yahoo.com
(716) 645- (Office) (716) 645- (Fax)

HINT: very suspicious that they would not be given access to a phone to call someone

-------- Original Message --------
Subject: Annual Form - Authorization to Use Privately Owned Vehicle on State Business
Date: Tue, 8 Oct 2013 15:48:37 +0000
From: Lola Ferrell <Lola@buffalo.edu>
To: [redacted]@buffalo.edu

All employees need to have on file this form STD 261 (attached). The original is retained by supervisor and copy goes to Accounting. Accounting need this form to approve mileage reimbursement.

The form can be used for multiple years, however it needs to re-signed annually by employee and supervisor.

Please confirm all employees that may travel using their private car on state business (including training) has a current STD 261 on file. Not having a current copy of this form on file in Accounting may delay a travel reimbursement claim.

Form_buffal...u.zip (10 KB)

What Can You Do To Help?

- Be diligent
  - Don't open unknown emails/attachments
  - Don't click on unknown links ANYWHERE
  - Be skeptical and suspicious!
- Report unusual activity to your IT support staff immediately

Additional Important Contact Information

- UBIT Security Alert Page:
  - http://www.buffalo.edu/ubit/news/alerts/ubit-security.html
- Phishing reporting:
  - abuse@buffalo.edu
- Questions/Request department presentation:
  - sec-office@buffalo.edu

Questions?