# Anatomy of a "Phishing" Email

Cybersecurity Awareness Month 2018

James Pardonek

# A Little About Jim P

Loyola's Information Security Officer

Manage the Information Security Team

Over 15 Years in Information Security

Certified Information Systems Security Professional (CISSP)

Certified Ethical Hacker (CE-H)

BS/MS (Technology) Purdue University

Rock Legend (in my own mind)

# A Little About Jim S

AVP – Enterprise Systems Services

Responsibilities
- IT Governance
- Admin/ERP/Student Systems
- Database Administration
- PMO
- Enterprise Architecture
- Information Security

Over 30 Years in Information Technology
- 20+ years of Applications, project Mgmt & Enterprise Architecture
- 10 Years in Information Security

BSCS – Aurora University

I'm no Jack Nicklaus or Tiger Woods!!
(even in my dream world)

# Let's Talk About Phishing

(fish´ing)

The act of sending an e-mail to a user **falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft.** The e-mail directs the user to visit a Web site where they are asked to update personal information, such as passwords and credit card, social security, and bank account numbers, that the legitimate organization already has. The Web site, however, is bogus and set up only to steal the user's information.

# Phishing Statistics

- There were at least 1,185,000 reported phishing attacks worldwide in 2017
- 76% of companies stated that they were victim of a phishing attack
- The attacks occurred using 174,600 unique domain names
- 3600 Loyola student victims

# Top 5 Types of Phishing Scams*

1. Deceptive Phishing – impersonating legitimate companies to steal information
2. Spear Phishing – targeted attack on a victim, crafted specifically to the individual
3. Social Media Phishing - harmful links through Facebook, Twitter, etc.
4. Malware-Based Phishing – downloadable files within phishing emails
5. File Sharing Scams – targets users of Google Docs, DropBox, etc.

*MetaCompliance

# Why Hackers Want Your Info

- The key for hackers is getting your password and login ID
- Even the simplest cell phone call is a miniature data gold mine.
- Two people talking on their mobiles think they are having a simple conversation, but as they chat, data is being collected about their location, the time and length of their call, and possibly the way that information interfaces with their other digital activity.
- Everywhere we turn we are leaving behind "digital breadcrumbs,"
- Facebook
  - 1.4 Billion Users
  - 4 Million Posts Per Minute
  - Over 500 Terabytes of information per day
    - TeraByte = 17,000 Hours Music, 40 Days Video, 310,000 Photos, 500 Hours Movies

# How Much Is Stolen Data Worth?

- Average estimated price for stolen credit and debit cards: $5 to $30 in the US
- Bank login credentials for a $2,200 balance bank account: $190
- Bank login credentials plus stealth funds transfers to US banks: from $500 for a $6,000 account balance, to $1,200 for a $20,000 account balance
- Login credentials for online payment services such as PayPal: between $20 and $50 for account balances from $400 to $1,000; between $200 and $300 for balances from $5,000 to $8,000
- Login credentials to hotel loyalty programs and online auction accounts: $20 to $1,400

# What are the Thieves looking for?

- Don't think that it's just your banking details that are important
- Some emails attempt to gain control over your account login
- Most people use the same login information on various other accounts.
- If they compromise your email account, they can reset all your other passwords.

# How can I help to stop them?

- Keeping strong and varying passwords
- Always be on the lookout for bogus emails masquerading as the real thing.
- Learn to spot a phishing expedition
  - While most phishing attempts are amateurish, some are quite convincing so it is important to understand how to recognize them at surface level as well as how they work under the hood.

# Examining What is in Plain Sight

- Most phishing attempts, "notify" you of activity on an account which is intended to alarm you into reacting.
  - Problems with your Email, the bank, even someone in your address book
  - So the call to action is to verify/restore your account by submitting just about every piece of personal information you can think of.
  - Fairly formulaic.
- While there certainly are exceptions, pretty much every phishing and scam email is loaded with red flags directly in the message themselves.
- Even if the text is convincing, you can usually find many mistakes littered throughout the message body which indicate the message is not legit.

# Email Account Phish

**From:** Baum, Laura Van Metre <laura.baum@vumc.org>
**Sent:** Monday, October 15, 2018 12:06 PM
**Subject:** Help Desk

**Dear: **** **@luc.edu,**

**Thank you for choosing Loyola University!**

**You are just one step away from our new email account upgrade portal.**

**Click below to verify your account:**

**Verify**

**Sincerely,**

**Help Desk University Chicago.**

# Email Account Phish

**From:** Baum, Laura Van Metre <laura.baum@vumc.org>
**Sent:** Monday, October 15, 2018 12:06 PM
**Subject:** Help Desk

**From:** Baum, Laura Van Metre <laura.baur
**Sent:** Monday, October 15, 2018 12:06 PM
**Subject:** Help Desk

**Dear: **** **@luc.edu,**

**Thank you for choosing Loyola University!**

**You are just one step away from our new email account upgrade portal.**

**Click below to verify your account:**

**Verify**

**Sincerely,**

**Help Desk University Chicago.**

# Email Account Phish

**From:** Baum, Laura Van Metre <laura.baum@vumc.org>
**Sent:** Monday, October 15, 2018 12:06 PM
**Subject:** Help Desk

**Dear: **** **@luc.edu,**

**Thank you for choosing Loyola Unive**

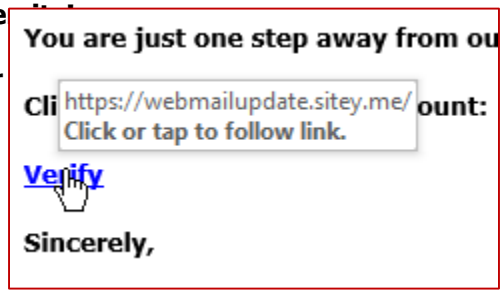
**You are just one step away from our**

**Click below to verify your account:**

**Verify**

**Sincerely,**

**Help Desk University Chicago.**



# Email Account Phish

**From:** Baum, Laura Van Metre <laura.baum@vumc.org>
**Sent:** Monday, October 15, 2018 12:06 PM
**Subject:** Help Desk

**Dear: **** **@luc.edu,**

**Thank you for choosing Loyola University!**

**You are just one step away from our new email account upgrade portal.**

**Click below to verify your account:**

**Verify**

**Sincerely,**

**Help Desk University Ch**

**Sincerely,**

**Help Desk University Chicago.**

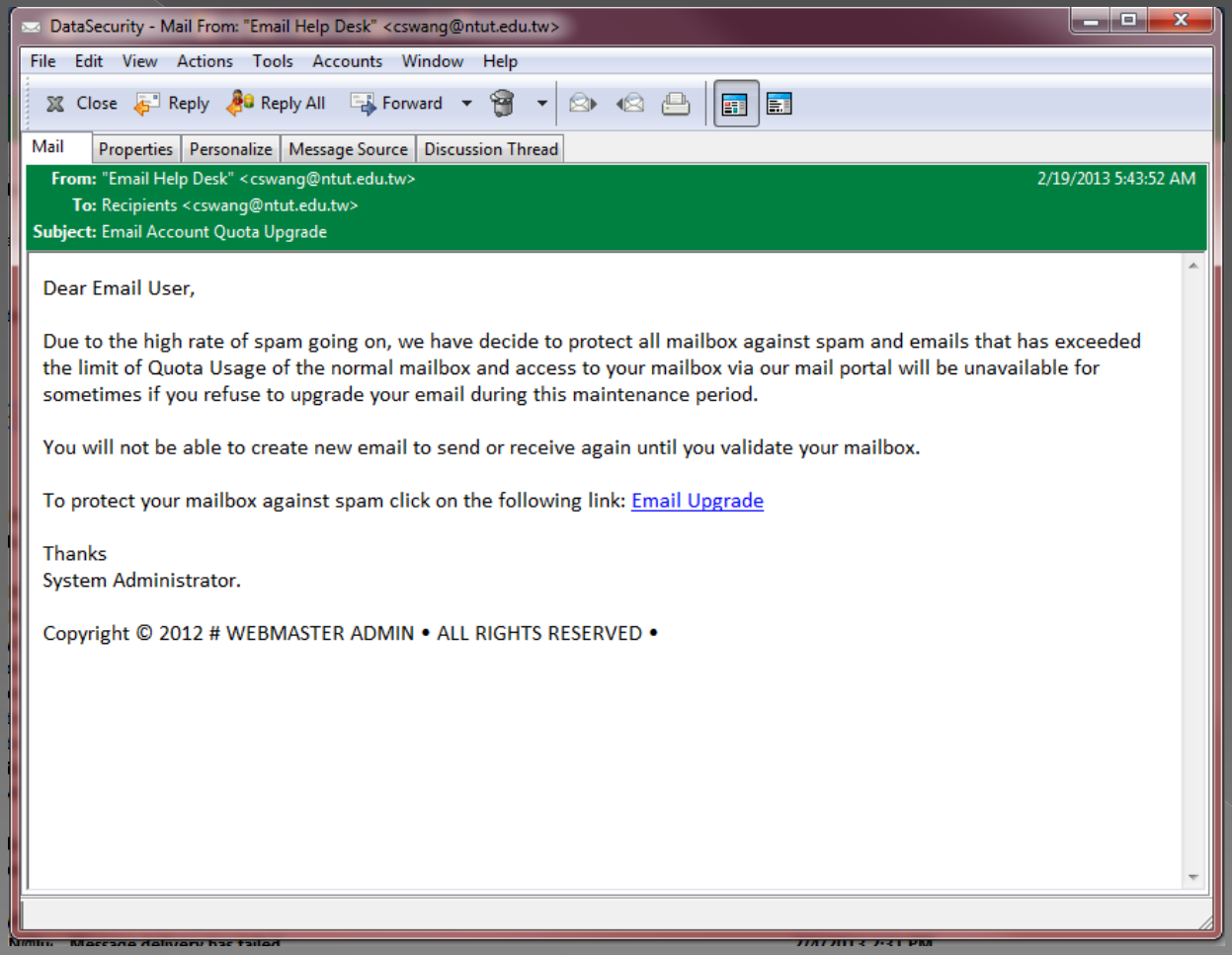
# Making You Panic?

**From:** [redacted]
**Sent:** Wednesday, October 05, 2011 11:34 AM
**To:** [redacted]
**Subject:** Regards

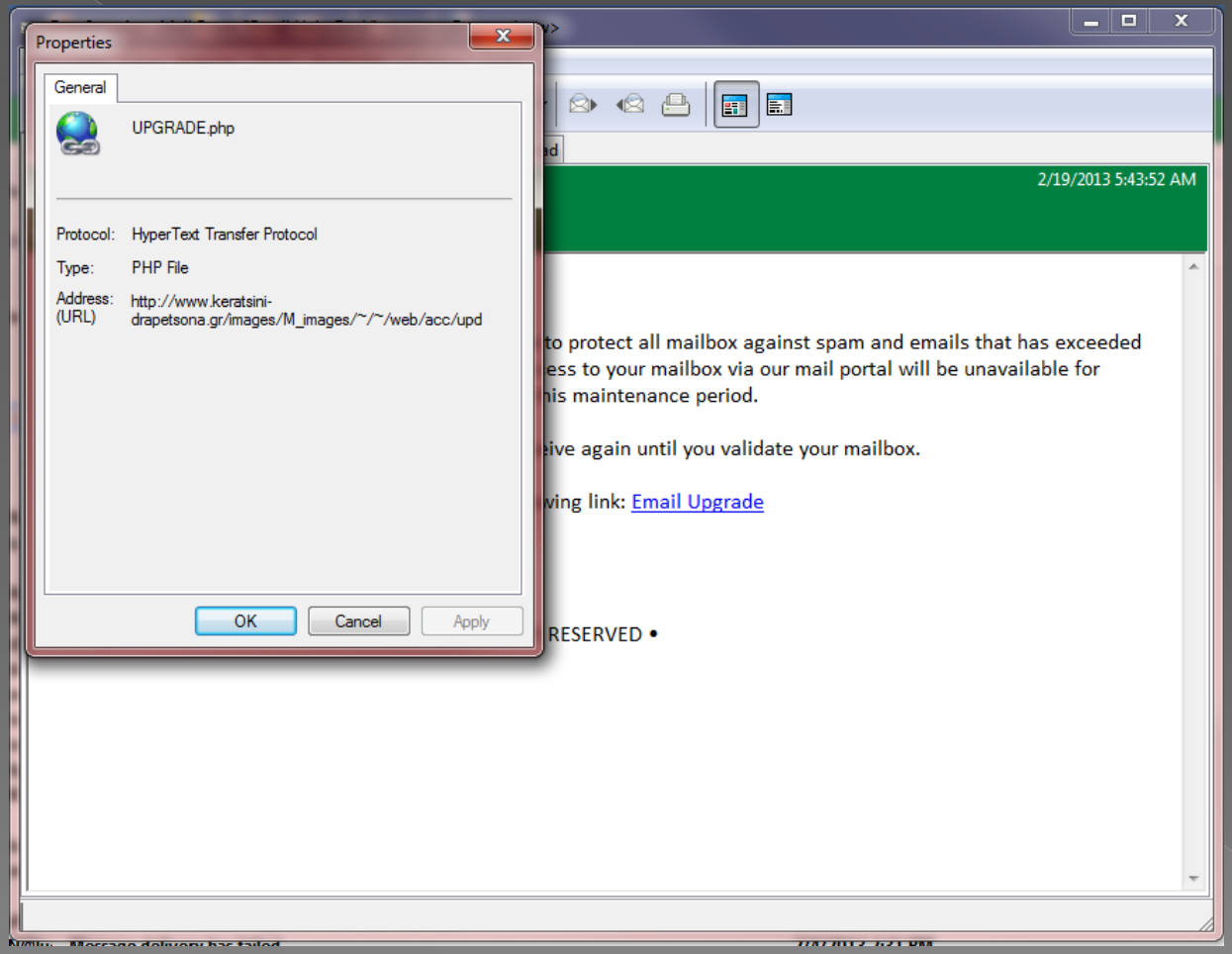
I Hope you get this on time ?I left on a trip to Spain,and I'm having some difficulties.
Unfortunately for me I got robbed on my way to the hotel where i lodged along with my Cell phone and my luggage and since then i have been without money.At the moment my passport has been seized by the hotel management pending the time payment is made. So i have limited access to emails for now.I urgently need your financial assistance. The total amount of money that i need is 2450Euros or any amount you can lend me to sort-out the bills, so i can make arrangements and return back. I'm in a panic now, I will refund you as soon as i get back, I am so confused right now. Thou i wasn't hurt because I complied immediately, waiting for your reply please.

Regards,
Love, Chris

# Login Credential Phish



# Login Credential Phish



# Can You Spot What's Wrong?

**From:** IT Helpdesk [mailto:cll32@duke.edu]
**Sent:** Thursday, October 06, 2011 6:03 AM
**To:** Jane Doe
**Subject:** Quota/storage upgrade option

To ensure quick, responsive e-mail services in the school webmail system, it is important to establish limits on the volume of data each user may store on our email system. The volume of e-mail you are storing on the Central e-mail server system has almost exceed your normal space allocation. In order to avoid imminent data loss you need to request for more storage space on your webmail account, simply click here to submit request.

IT Helpdesk

# Cynicism is a Good Defense

- When it comes to staying safe online, it never hurts to have a good bit of cynicism.

# 10 Tips for Identifying a "Phishy" Email

- Don't trust the display name.
- Look but don't click.
- Check for spelling mistakes.
- Beware of vague salutations.
- Don't give up personal information.
- Watch for urgent subject lines.
- Review the signature.
- Never click attachments.
- Don't trust the header.
- Don't believe everything you see!

# So They Got Your Email (Video)

# Passwords

- EU study of "office workers"
  - 16% used their name as password
  - 11% used favorite football team
  - 12% used the word "password"

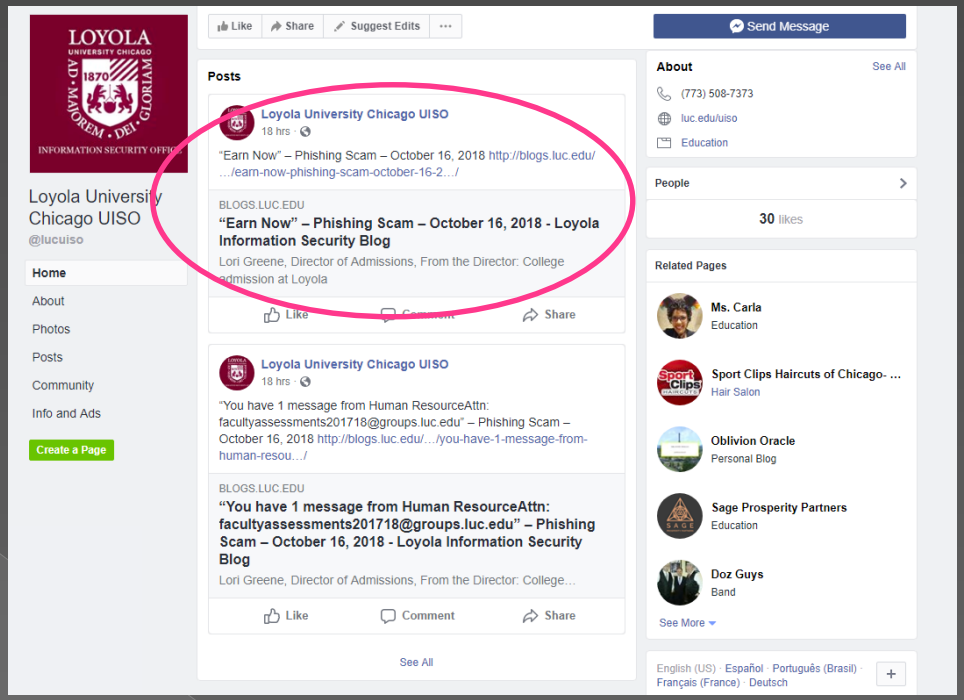
- Never use a word that could be in any dictionary, names of places, or any proper nouns
- Never use any of the above spelled backwards
- Never use any of the above simply followed by a digit
- Include upper and lower case, numbers, special characters

| RANK | PASSWORD |
|---|---|
| 1 | 123456 |
| 2 | password |
| 3 | 12345678 |
| 4 | qwerty |
| 5 | 12345 |
| 6 | 123456789 |
| 7 | football |
| 8 | 1234 |
| 9 | 1234567 |
| 10 | baseball |

# Resources

- Check UISO's pages for the latest security and phishing notices

**Facebook:**
https://www.facebook.com/lucuiso/




**Our Blog:**
http://blogs.luc.edu/uiso/


- www.luc.edu/its/uiso
- Twitter: @LUCUISO

# Escalation

- If you *do* fall victim to a phishing scam, here's how to escalate…
- Forward the email to datasecurity@luc.edu
- **Call the LUC Help Desk at ext. 84487 (773-508-4ITS)**
- After hours? Call the Help Desk and use the Emergency option for assistance

# Summary

- Unprofessional email title
- The sender address does not match the title
- The images look a bit amateurish: They don't match the background or look formatted to fit the style of the email
- A generic greeting is used: A company you've done business with or contacted before you likely use your name instead of a vague greeting
- Reply by email is requested: Because scammers are not the legitimate company, they are likely to request an email response
- Secure information is requested: Legitimate companies would never request such sensitive information via email
- Typos and poor grammar are a big hint that the email is fraudulent

# Thank You!


- **James Pardonek, MS, CISSP, CEH, GSNA**
- **Information Security Officer**

**(773) 508-6086**


- www.luc.edu/its/uiso
- Facebook: https://www.facebook.com/lucuiso/
- Our Blog: http://blogs.luc.edu/uiso
- Twitter: @LUCUISO
- Data Security Hotline (773) 508-7373