Cybersecurity Tips and Tricks

October 2016

Presenters:
Julie Goldstein & Jon Good
UC Cyber-Risk Coordination Center (C3)
UCOP Information Security Director

Email #1 – Legit or Scam?

Sent to a campus payroll director:

From: Janet Napolitano [mailto:President@ucop.edu]
Sent: Monday, February 22, 2016 8:18 AM
Subject: 2015 W-2 statement

I need all our employee's reference copies of 2015 W-2 wages and tax statement, i am working on a review and if you can work on the W2's and have it sent to me as an attachment this morning that will be splendid. Via email would be appropriate.

Regards.

Janet Napolitano.

Email #2 – Legit or Scam?

Sent to a manager in Cash Management:

From: Janet Napolitano [President@ucop.edu]
Sent: Tuesday, February 24, 2015 7:38 AM
Subject: Request

Hi Francis,

Hope you are having a splendid day. I want you to quickly email me the details you will need to help me process an outgoing wire transfer to another bank.

I will appreciate a swift email response.

Regards,
Janet Napolitano

Email #3 – Legit or Scam?

You receive the following email from the UCOP IT Service Desk:

Dear Outlook User,

Beginning next week, we will be deleting all inactive email accounts in order to create space for more users. You are required to send the following information in order to continue using your email account. If we do not receive this information from you by the end of the week, your email account will be closed.

*Name (first and last):
*Email Login:
*Password:
*Date of birth:
*Alternate email:

Please contact the IT Service Desk with any questions. Thank you for your immediate attention.

Email #4 – Legit or Scam?

Dear Julie Goldstein,

Elaine Goldstein (email address omitted) has sent you a Jacquie Lawson e-card. If you haven't heard of us, you'll be pleasantly surprised! Our e-cards are known for their artistry and gentle humour.

You can view your card here.

If you'd like to reply to the sender, simply click "Send a Reply" at the bottom of the card. And if you enjoy this e-card, you can learn more about us here.

With best wishes from us all,
Jacquie Lawson and team.

Jacquie Lawson

Phishing

Phishing

Phishing *= any attempt to trick people into*

- *revealing passwords,*
- *revealing confidential, personal or financial information,*
- *clicking on malicious links,*
- *opening harmful attachments,*
- *sending money,*

in person, over the phone, via email, instant message (IM), text, Facebook, Twitter, etc.

Phishing

Premise: Tricking people is easier than trying to break into systems.

Quick Fact: Most of the breaches the Sacramento FBI investigated last year started with a spear phish
(a sophisticated, targeted phish)

Phishing

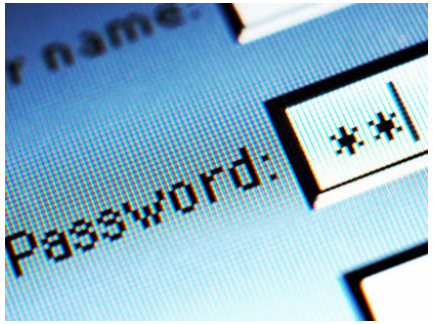
How to protect yourself:

- Be aware that phishing can come from anywhere: in person, over the phone, via e-mail, IM, text, Facebook, Twitter, etc.
- Be suspicious of unknown links and attachments, regardless of who they appear to come from.
- Never share your password with anyone.
- Never give private information (yours or other people's) to anyone you don't know or who doesn't have a legitimate business need for it.
- If you can't verify the legitimacy of a message, DELETE IT!
- If you're not sure about a message, forward it to the IT Service Desk (ServiceDesk@ucop.edu) for assistance.

Phishing

Extra Important:

- Use different passwords for different accounts
- Use different passwords for work and non-work



What's Wrong With This Picture?

Image from csoonline.com

Ransomware

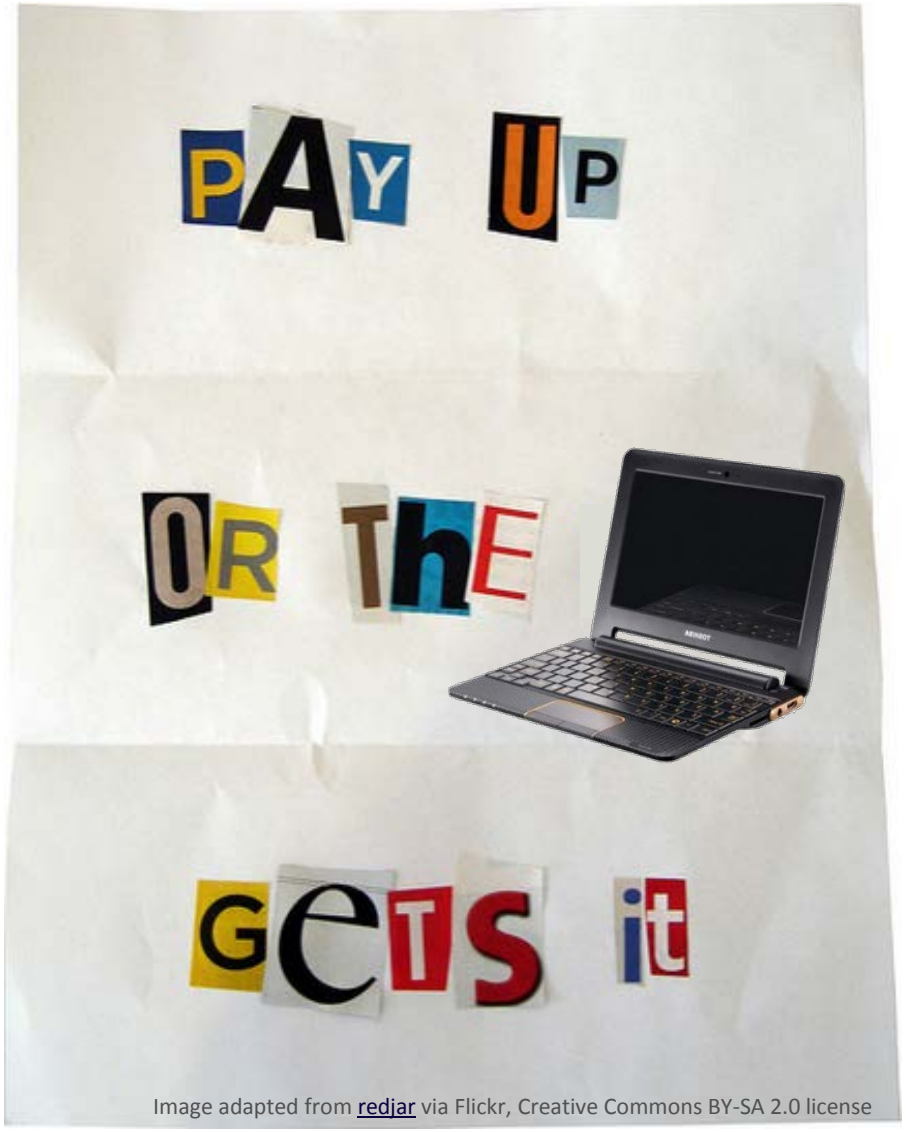


Image adapted from redjar via Flickr, Creative Commons BY-SA 2.0 license

Ransomware

Ransomware *= a type of malicious software (malware) that encrypts or locks you out of your computer, device or files until a ransom is paid.*

Quick Fact: 40% of all reported security incidents at UC involving compromised computers in the last year were ransomware.

Ransomware

How to protect yourself:

- Don't open files or click links in unsolicited emails, text messages, IMs, Facebook postings, tweets, etc.
- Don’t click on links in pop-up ads/windows; don’t respond to them in any way.
- Don’t fall for “Your computer is compromised – ACT NOW!” scams.
- DO store copies of all critical files on a drive that gets backed up regularly, or make your own backups.
- If you’re not sure about a message, don’t click on it. Forward it to the IT Service Desk (ServiceDesk@ucop.edu) for assistance.

Protect Mobile Devices!

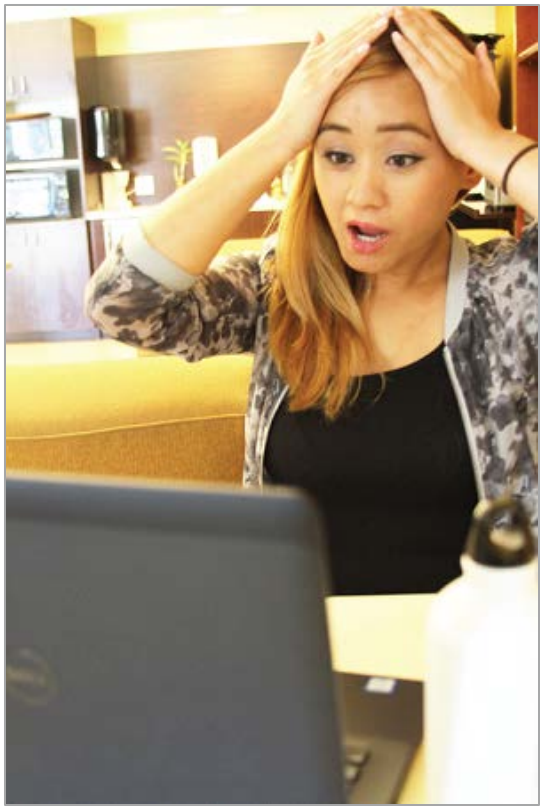
Tips for Protecting Your Phone and Other Portable Devices:

- Don't store anything too sensitive to be stolen.
- Back it up.
- Use complex passwords.
- Enable automatic screen locking.
- Don’t leave it lying around where someone could take it.
- Don't jailbreak or hack your phone or tablet.
- Be wary of public wireless.

Protect Your Online Privacy

Once You Share It Online, You Can't Take It Back.

- Don't reveal personal details or confidential info online.
- Never share your password.
- Check your privacy settings regularly.
- Be aware of apps that track your location.
- Don't advertise that you're out of town. Post your pictures when you get back.



Questions?

Presenters:

Julie Goldstein & Jon Good

UC Cyber-Risk Coordination Center (C3)

UCOP Information Security Director