Overview of Cybersecurity

Part Two

This research is supported by Award #1542465:
RET Site: Cyber Security Initiative for Nevada Teachers (CSINT)

Objectives

- Be able to identify malware, adware, etc
- Be able to identify a phishing scam
- Be able to discuss what makes a strong password/passphrase
- Be able to explain 2 factor authentication
- Be able to explain what an SSL certificate is
- Understand and know how to look for encryption

Threats and Attacks

Threat

- A possible danger in the system which an attacker could exploit to cause harm

Attack

- An attempt to cause some kind of damage to the system

Threats and Attacks

Examples

- **Threat:**

- **Attack:**

Malware

Malware is software intended to do some kind of damage

Examples:

Malware

Malware is software intended to do some kind of damage

- **Worm**: malware which spreads from computer to computer by replicating itself to nearby vulnerable devices
- **Trojan**: malware hidden inside a seemingly-innocuous file
- **Ransomware**: malware which encrypts a computer’s files and demands a fee for the decryption key

Adware

Software which makes its money through advertising

- More intrusive adware uses techniques such as pop-ups and autoplay audio
- If a service is free, it often makes money through selling ads or data
  - Be wary of what data you give away

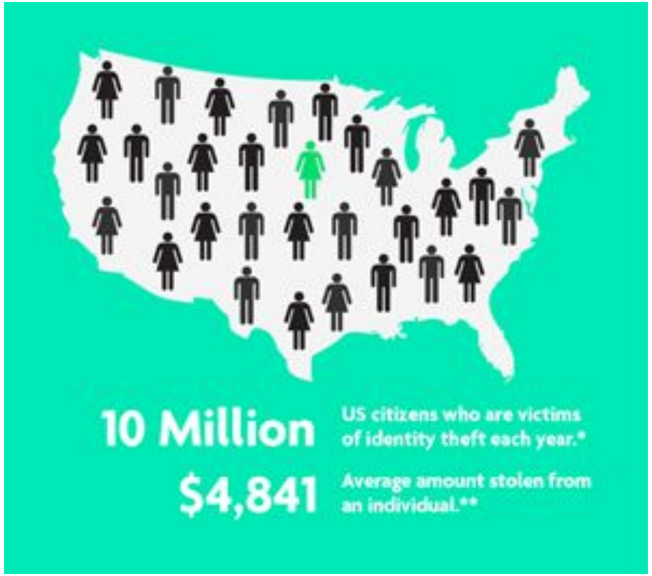
Question: What is your online identity?

- Personal information online about an individual
- Account credentials - usernames, emails, passwords
- Authentication - when you enter in your credentials, to prove that you are you
- Loss of credentials can lead to great harm

Identity theft

What is identity theft?

- Someone steals your account credentials and uses them
- Impersonates you, could order things in your name


10 Million
US citizens who are victims of identity theft each year.*
$4,841
Average amount stolen from an individual.**

Consequences of Identity Theft

- You could be harmed financially, socially, professionally
- Someone with your bank account credentials could steal all your money or rack up a massive debt on your credit card
- Someone with one of your social network credentials could post embarrassing things or harass the people on your contacts list
- Someone who steals your SSN could:
  - Open financial accounts in your name
  - Steal your health insurance coverage
  - File a fraudulent tax refund
  - Give your SSN to law enforcement if they are caught committing a crime, tangling you up in their criminal history and having a false criminal history show up on your background check.

Phishing

Q: What is phishing?

Individual with malicious intent impersonating a trustworthy entity to get a victim to give up personal information

Question: What are some ways we can identify common phishing schemes?

- An attempt to create a sense of urgency (i.e. “your account is going to be shut down”)
- Look for bad spelling, poor grammar
- Look for strange looking links included in email, or unlikely email addresses
- Watch for unexpected pop-ups, strange browser behavior

From: “Sass, Bradley” sass@tamhsc.edu

Subject: Your Dropbox File

Date: Mon, 30 Jan 2017

Hello,

You just received a file through Dropbox Share Application.

Please click below and log in to view file.

View file

Every time a friend installs Dropbox, we’ll give both of you 1 GB of Space for free! Need even more space? Upgrade your Dropbox and get 1 TB (1,000 GB) of space.

Happy Dropboxing.

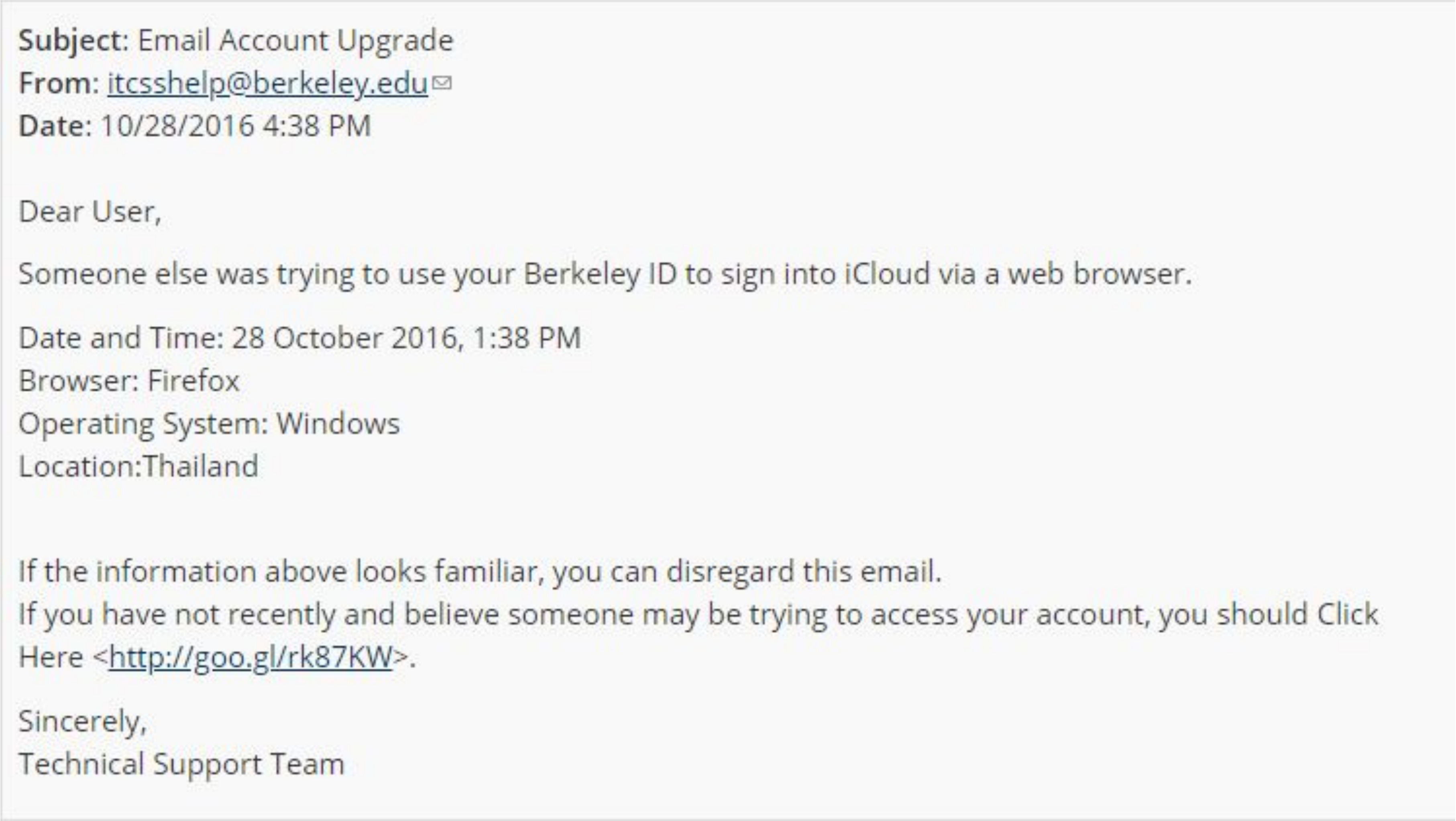
-The Dropbox Team

Dropbox, Inc., PO Box 77767, San Francisco, CA 94017 © 2017 Dropbox

What makes this a Phishing message?

The link in the email message to "View File" is a ruse to capture CalNet passphrase credentials.

1. The return address of the sender is from the network domain for Texas A&M Health Sciences Center (@tamhsc.edu), not Dropbox.
2. If you hold your cursor over the "View File" link, you will see that the URL address is a forgery of the real CalNet login address
3. Check “whois tamhsc.edu” to find out who the domain belongs to.



Subject: Email Account Upgrade
From: itcsshelp@berkeley.edu
Date: 10/28/2016 4:38 PM

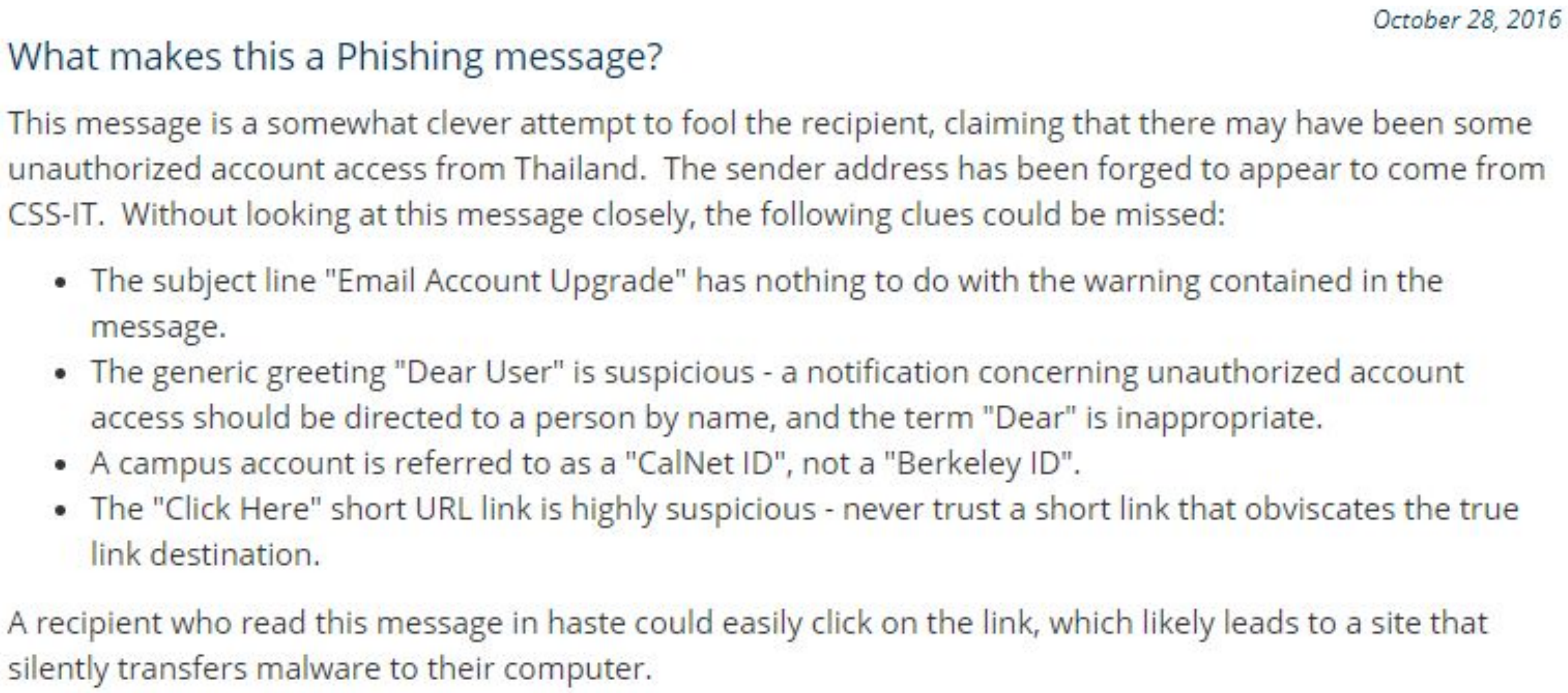
Dear User,

Someone else was trying to use your Berkeley ID to sign into iCloud via a web browser.

Date and Time: 28 October 2016, 1:38 PM
Browser: Firefox
Operating System: Windows
Location:Thailand

If the information above looks familiar, you can disregard this email.
If you have not recently and believe someone may be trying to access your account, you should Click Here <http://goo.gl/rk87KW>.

Sincerely,
Technical Support Team



October 28, 2016

What makes this a Phishing message?

This message is a somewhat clever attempt to fool the recipient, claiming that there may have been some unauthorized account access from Thailand. The sender address has been forged to appear to come from CSS-IT. Without looking at this message closely, the following clues could be missed:

- The subject line "Email Account Upgrade" has nothing to do with the warning contained in the message.
- The generic greeting "Dear User" is suspicious - a notification concerning unauthorized account access should be directed to a person by name, and the term "Dear" is inappropriate.
- A campus account is referred to as a "CalNet ID", not a "Berkeley ID".
- The "Click Here" short URL link is highly suspicious - never trust a short link that obviscates the true link destination.

A recipient who read this message in haste could easily click on the link, which likely leads to a site that silently transfers malware to their computer.

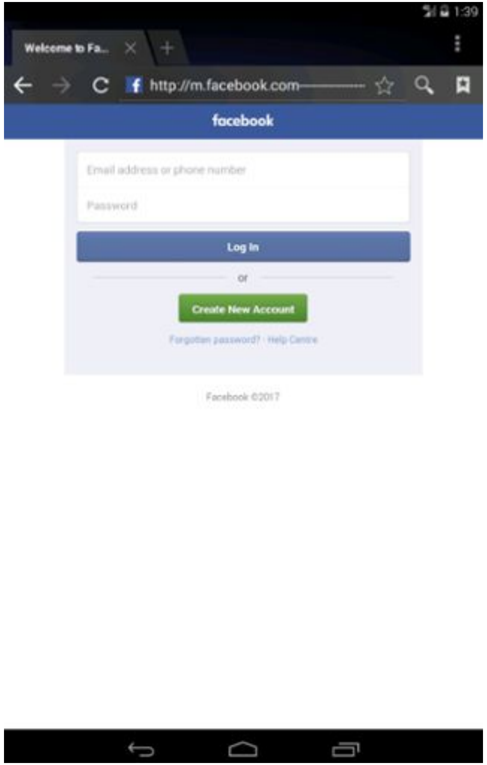
Bitly URL shortener (https://bitly.com/)

Before:
https://www.intel.com/content/www/us/en/homepage.html

After:
https://intel.ly/2ob5FDx

(the Google shortener shown in the previous slide is no longer available)

Mobile Phishing Scheme Example


1:39
Welcome to Fa...
http://m.facebook.com————
facebook
Email address or phone number
Password
Log In
or
Create New Account
Forgotten password? · Help Centre
Facebook ©2017

This is not Facebook.com, even though that's what the browser indicates (screen too small for URL)

The URL is actually:
http://m.facebook.com——————-validate—-step9.rickytaylk[dot]com/sign_in.html

Strong Passwords

Pick the best one:

- Pass123
- Tr0b@d0r$
- Qwerty
- GeeWhizThisSureIsAGoodPassword

#Abithiw2itb!
?

Question: why is the one you chose the best one?

Activity-*What makes a strong password?*

Length-the longer the password is, the stronger it is against attacks

Complexity- a different amount of symbols such as numbers, uppercase and lowercase letters, and special symbols.

Q: Both are important, but if you had to choose one, which one would you choose?

Test the previous slide's passwords on these websites

https://howsecureismypassword.net/

https://www.grc.com/haystack.htm

Passphrases

Difference between passwords and passphrases

- Password is one word, tends to be shorter
- Harder to remember
- Easier to crack

Passphrase

- Longer = stronger
- Easier to remember

2 Factor Authentication

- 1 layer of authentication = 1 failure point
- 2 layers = more redundancy, combination of authentication techniques
- 2nd layer = something you have

SOMETHING YOU KNOW
+
SOMETHING YOU HAVE

Password Managers

Password managers allow the security of having unique, strong passwords without the pain of remembering them

- With a strong master password and 2-factor authentication, a password vault can be kept very secure
- If a password manager is designed correctly, it is impossible to gain any passwords without the master password (even with all data stored on the computer)

Password Managers

Example password managers

- LastPass
- KeePass
- 1password

SSL(Secure Sockets Layer) Encryption

- *Encryption* scrambles data so it looks unintelligible
- SSL encrypts data transferred on the internet
- Green lock and “https” are confirmation of encryption from browser
- Be wary of transferring personal info on sites without SSL

Security Blogs

https://digitalguardian.com

https://thehackernews.com

http://blog.talosintelligence.com

https://www.globalsign.com/

https://www.scmagazine.com

https://krebsonsecurity.com/

References

Majority of the content

http://nevadacyberclub.com/cyber-clinics/guidance/

Passphrase generator

https://www.rempe.us/diceware/#eff

Password strength

https://howsecureismypassword.net/

https://www.grc.com/haystack.htm

SSL Encryption

https://www.youtube.com/watch?v=UNImBt5tTlg

Protecting your identity

https://programs.online.utica.edu/articles/TenWaysToProtectYourIdentity

References

Phishing Images:

- Facebook: https://fossbytes.com/facebook-phishing-technique-url-padding/
- Apple notifications: https://krausefx.com/blog/ios-privacy-stealpassword-easily-get-the-users-apple-id-password-just-by-asking

Helpful tips

- **Make sure your devices are locked whenever you’re not using them**
- An attacker can break into almost any account you have if they compromise your email account
- Staying logged into an account means an attacker doesn’t need to figure out the credentials for that account if they get into your computer

Helpful tips

- **Keep software up to date**
- Updating is a hassle, but it is critical in order to keep your computer secure
- Many major attacks are the result of long-out of date software