Computer Network Security

COMP 178 | Spring 2025 | University of the Pacific | Jeff Shafer

Penetration Testing: Social Engineering

"Humans are incapable of securely storing high-quality cryptographic keys, and they have unacceptable speed and accuracy… They are also large, expensive to maintain, difficult to manage, and they pollute the environment. It is astonishing that these devices continue to be manufactured and deployed. But they are sufficiently pervasive that we must design our protocols around their limitations."

Charlie Kaufman, Radia Perlman and Mike Speciner

Network Security: Private Communication in a Public World (1995)

Trick the Humans

- **Goal: Trick the human!**
  - Divulging password?
  - Running malicious program allowing remote access?
  - Allowing physical access to restricted spaces?
  - …
  - …
- Can be effective even if systems are 100% impervious from a technology standpoint

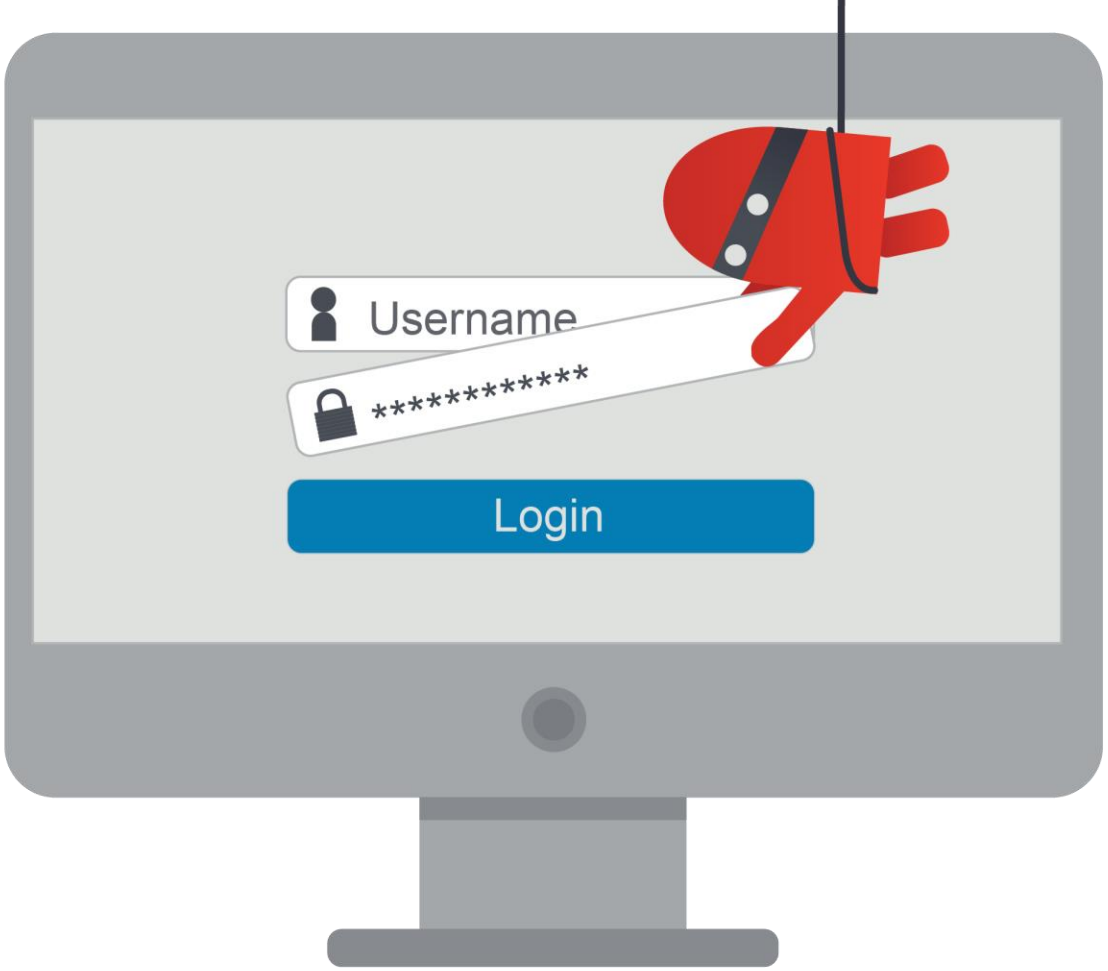
Trick the Humans

- More **detailed reconnaissance** at the start of the pentest (*OSINT*) leads to…
- More knowledge about what is "normal" for ~~targets~~ "client employees", which leads to…
- More effective (*less suspicious*) social engineering attacks, which leads to…
- More wins! (more user credentials, more software running on target computers), which leads to…
- **More comprehensive pentest**
  (justify the $$ they're paying you)

Penetration Testing

Penetration testers restricts their activities to only systems, machines, facilities, etc. which they have **explicit written permission** to test!

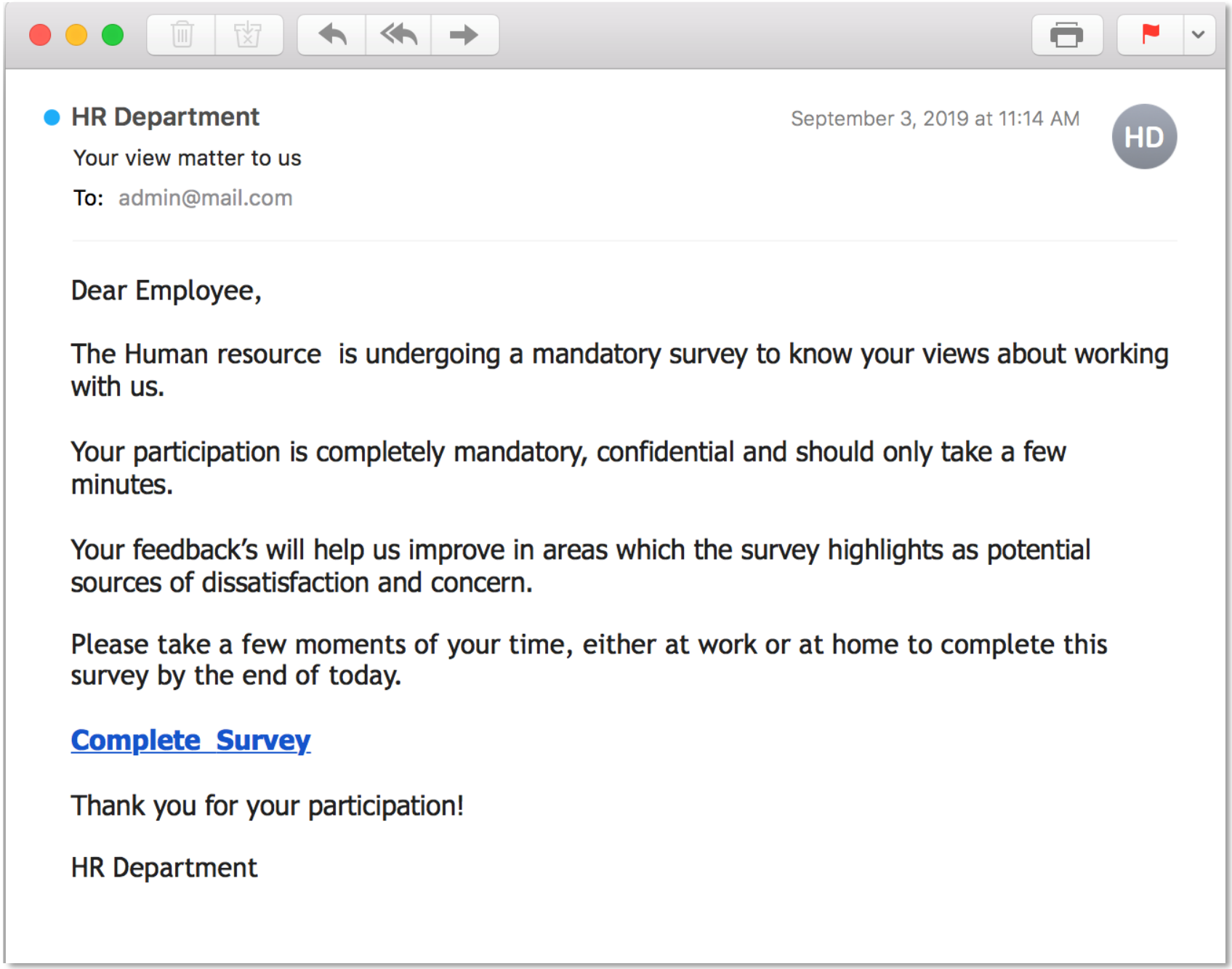
Do you have permission to test the humans?



Social Engineering Attacks

Phishing

- Goal: Trick the user into providing confidential information
  - For pen testing: **passwords**
  - For criminals: Social security numbers? Credit cards? Wide scope of PII
- Method: Impersonate some legitimate system and convince user to enter information there



HR Department September 3, 2019 at 11:14 AM

HD

Your view matter to us

To: admin@mail.com

Dear Employee,

The Human resource is undergoing a mandatory survey to know your views about working with us.

Your participation is completely mandatory, confidential and should only take a few minutes.

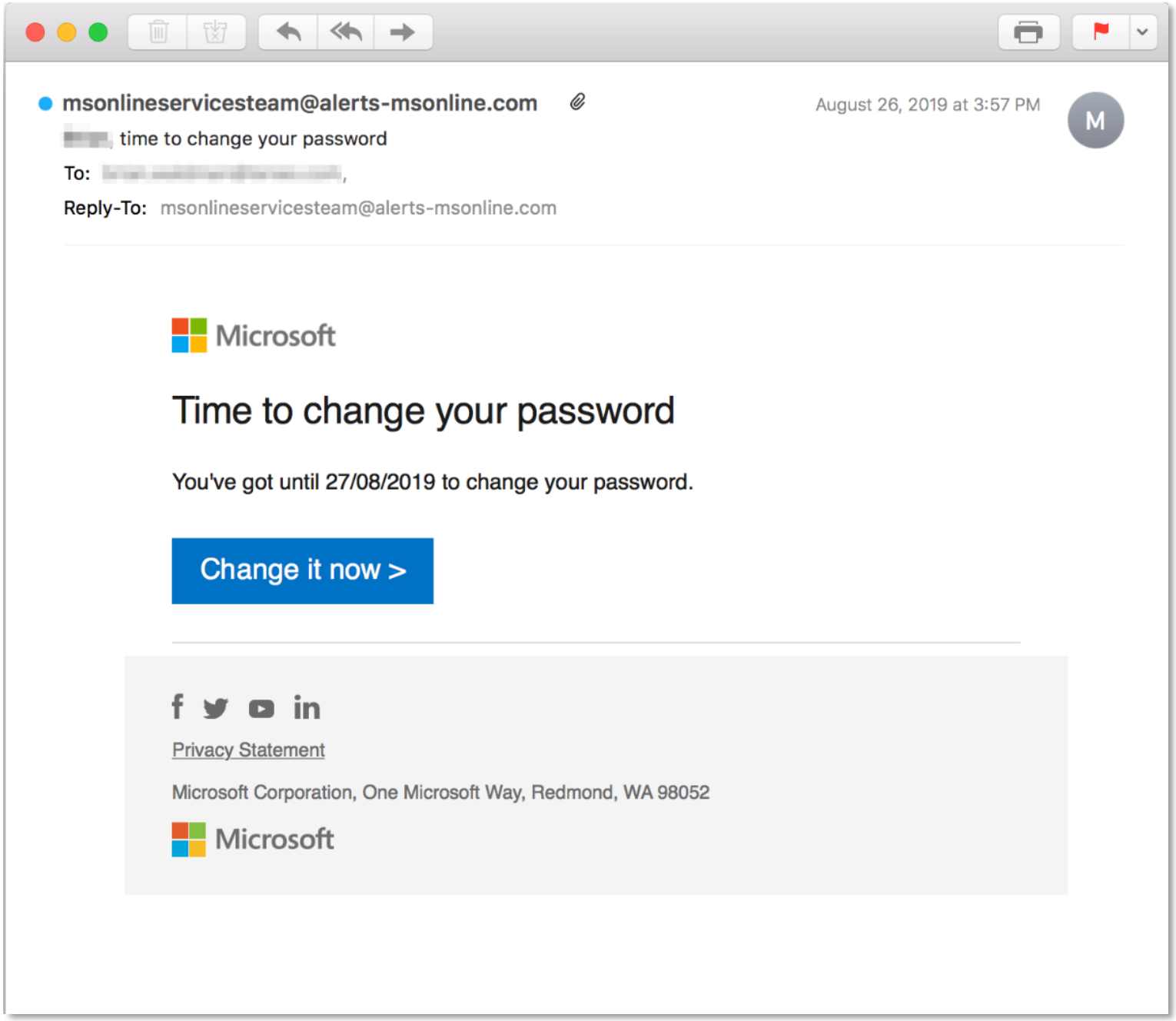
Your feedback's will help us improve in areas which the survey highlights as potential sources of dissatisfaction and concern.

Please take a few moments of your time, either at work or at home to complete this survey by the end of today.

Complete Survey

Thank you for your participation!

HR Department



msonlineservicesteam@alerts-msonline.com

August 26, 2019 at 3:57 PM

M

[redacted] time to change your password

To: [redacted],

Reply-To: msonlineservicesteam@alerts-msonline.com

Microsoft

Time to change your password

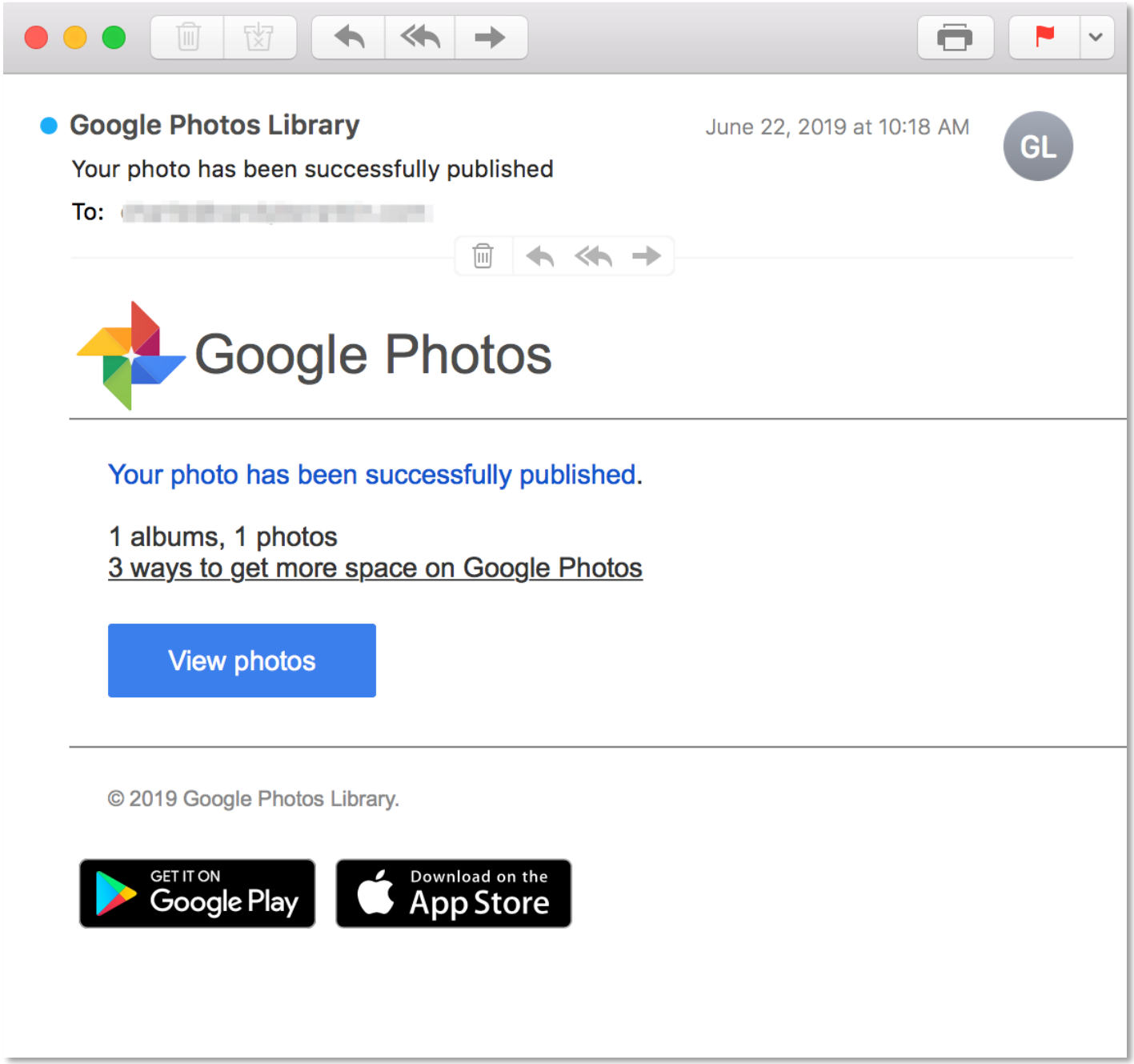
You've got until 27/08/2019 to change your password.

Change it now >

Privacy Statement

Microsoft Corporation, One Microsoft Way, Redmond, WA 98052

Microsoft



Google Photos Library

June 22, 2019 at 10:18 AM

GL

Your photo has been successfully published

To: [redacted]

Google Photos

Your photo has been successfully published.

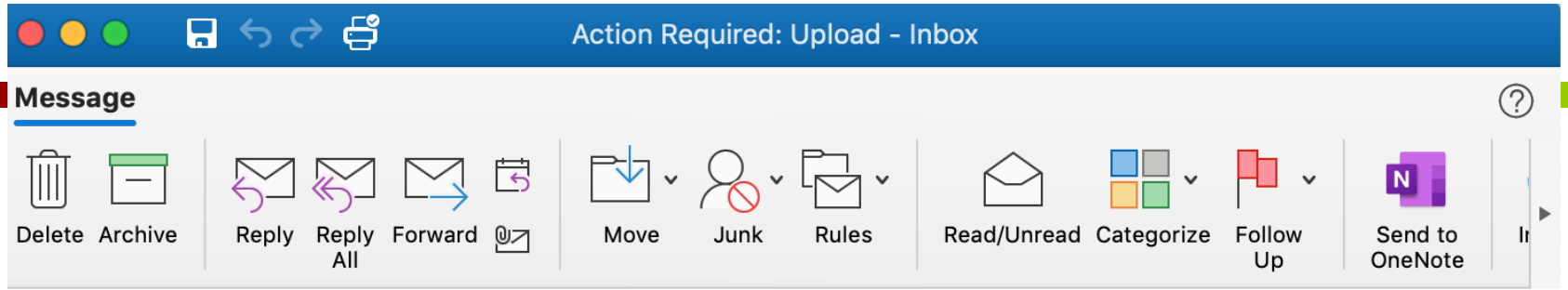
1 albums, 1 photos

3 ways to get more space on Google Photos

View photos

GET IT ON Google Play

Download on the App Store



Action Required: Upload

Today at 5:49 AM

To: Office365 Alerts

Dear Pacific Community,
Hello ,

This is a courtesy notice from Human Resources, you will be needed to Upload a few documents, via the button below. These documents will aid us in completing your California Covid-19 Relief Fund and Vaccine Distribution Update and Next Steps for Our University. For information will be relayed to you after completion.

Upload

No further action will be required, we apologize for any inconvenience and appreciate your understanding.

Thanks,

University of the Pacific

3601 Pacific Avenue
Stockton, CA 95211

lSacramento Campusl

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 94107 © 2017 Dropbox

File download link *actually* went to a malicious site to capture Berkeley single-signon login credentials

Could have also downloaded a malicious file (PDF? MS Office?) and attempted to exploit vulnerable client applications

https://security.berkeley.edu/news/phishing-example-your-dropbox-file

From: <NAME REMOVED>
Date: Sat, Apr 1, 2017 at 2:09 PM
Subject: Library Account
To: xxxxx@berkeley.edu

Dear Student,

Your access to your library account is expiring soon due to inactivity. To continue to have access to the library services, you must reactivate your account. For this purpose, click the web address below or copy and paste it into your web browser. A successful login will activate your account and you will be redirected to your library profile.

https://auth.berkeley.edu/cas/login?service=https%3a%2f%

If you are not able to login, please contact <Name Removed> at xxxxx@berkeley.edu for immediate assistance.

Sincerely,
<Name Removed>
University Library
University of California Berkeley

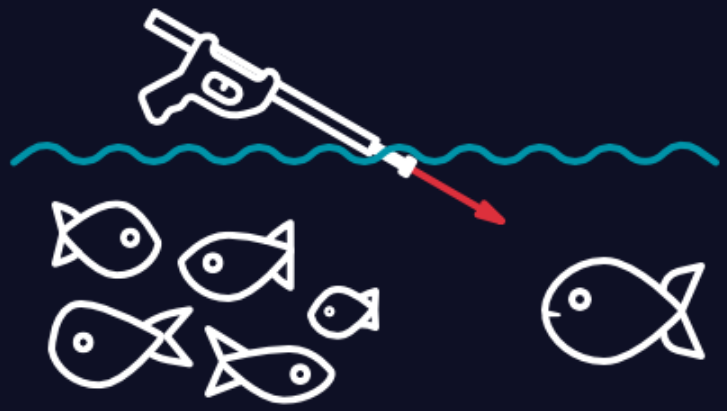
Link *actually* went to a malicious site to capture Berkeley single-signon login credentials

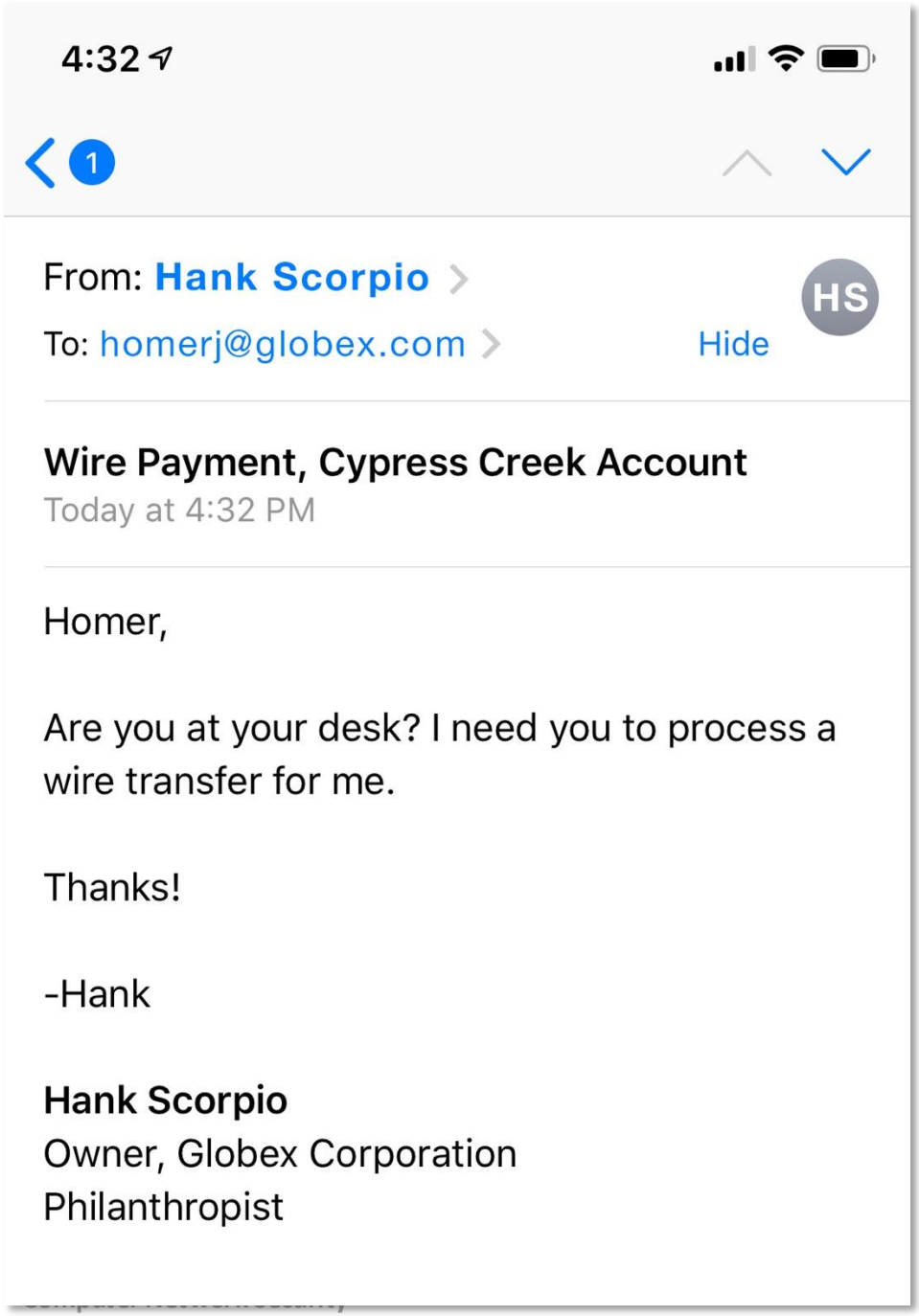
https://security.berkeley.edu/news/phishing-example-library-account-0

Spear Phishing

- Same idea as phishing, **but narrowly targeted**
  - Single target or small group of targets
  - Highly researched (reconnaissance), carefully written

Spear phishing is a targeted attack where an attacker creates a fake narrative or impersonates a trusted person, in order steal credentials or information that they can then use to infiltrate your networks.




4:32
1
From: Hank Scorpio
To: homerj@globex.com
Hide
HS
Wire Payment, Cypress Creek Account
Today at 4:32 PM
Homer,
Are you at your desk? I need you to process a wire transfer for me.
Thanks!
-Hank
Hank Scorpio
Owner, Globex Corporation
Philanthropist

Wire fraud!

Demo of cloning LinkedIn.com and capturing passwords when users attempt to log in

https://www.youtube.com/watch?v=u9dBGWVwMMA

PRESENTED BY INFINITELOGINS

BROWSER IN THE BROWSER

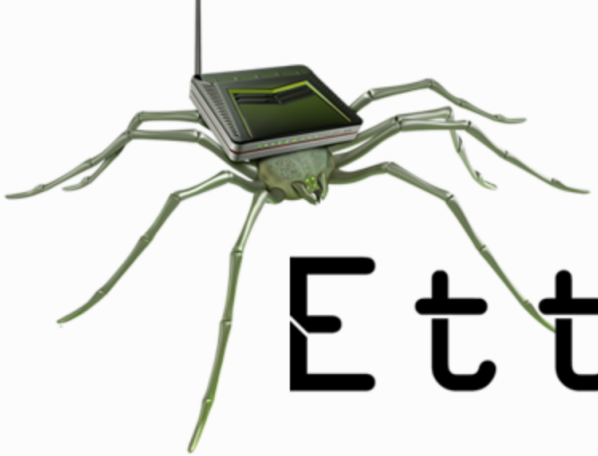
mr.d0x's PHISHING TECHNIQUE

Demo of Browser in the Browser (BITB) Phishing Technique
Attack info: https://mrd0x.com/browser-in-the-browser-phishing-attack/

https://www.youtube.com/watch?v=ntS7WHaznjI

Site Cloning

- If you have a man-in-the-middle position and can intercept/inject network traffic, you could use a more advanced attack
- Instead of tricking user into following a bogus link, spoof the DNS request for `facebook.com` to go to an IP address you control



ETTERCAP HOME PAGE

HOME ABOUT DOWNLOADS GET INVOLVED BUG SUBMISSION USERS MAILING LIST

WELCOME TO THE ETTERCAP PROJECT

Ettercap is a comprehensive suite for man in the middle attacks. It features sniffing of live connections, content filtering on the fly and many other interesting tricks. It supports active and passive dissection of many protocols and includes many features for network and host analysis.

https://www.ettercap-project.org/

Penetration Testing Tips for Email-based Social Engineering

- Suggestion: Split your email-based social engineering into two parts
  - Part 1 - Email everyone with a **benign** link and track who clicks it (producing statistics for client)
  - Part 2 - With company staff, click on a **malicious** link and record the results (i.e. would the exploit have been successful on all of those client systems?)
- Eliminates the risk of accidentally exploiting systems *outside* the scope of your pentest

Baiting

- Leave ~~malware~~ *pentest*-infected physical media (USB keys, …) in locations where potential victims will find it
- Victim connects drive to their computer
- Contents?
  - Macro enabled documents and spreadsheets
  - PowerShell scripts


8 GB

"Users Really Do Plug in USB Drives They Find"

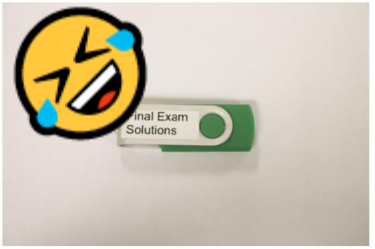
Dropped 297 USB drives on campus of University of Illinois, Urbana-Champaign. 30 unique locations on campus, varied time of day. Non-malicious HTML payload.

(a) Unlabeled drive

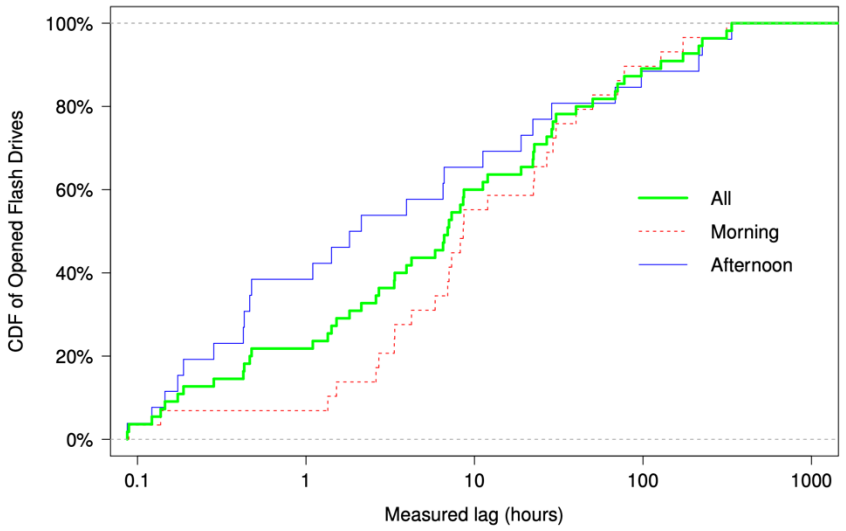
(b) Drive with keys

(c) Drive with return label

(d) Confidential drive



(e) Exam solutions drive



Effective: 45-98% of drives connected to a computer

Fast: Median time of 6.9 hours

Users Really Do Plug in USB Drives They Find, Matthew Tischer, et. al. IEEE Security and Privacy, 2016
https://elie.net/static/files/users-really-do-plug-in-usb-drives-they-find/users-really-do-plug-in-usb-drives-they-find-paper.pdf

The Dark Arts of Social Engineering – SANS Security Awareness Summit 2018
Jen Fox, Senior Cyber Security Consultant, All Covered

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