

Cybersecurity

Cybersecurity Safety for Individuals

CSUSM Cybersecurity Education Hub

Cybersecurity Safety

- Social Engineering
- Phishing/Fraud
- Malware
- Staying safe out there

Social Engineering

- Definition: use psychological manipulation to trick people into performing some action
- Examples:
- Phishing
- Getting access to information assets
- Delivering malware



Phishing

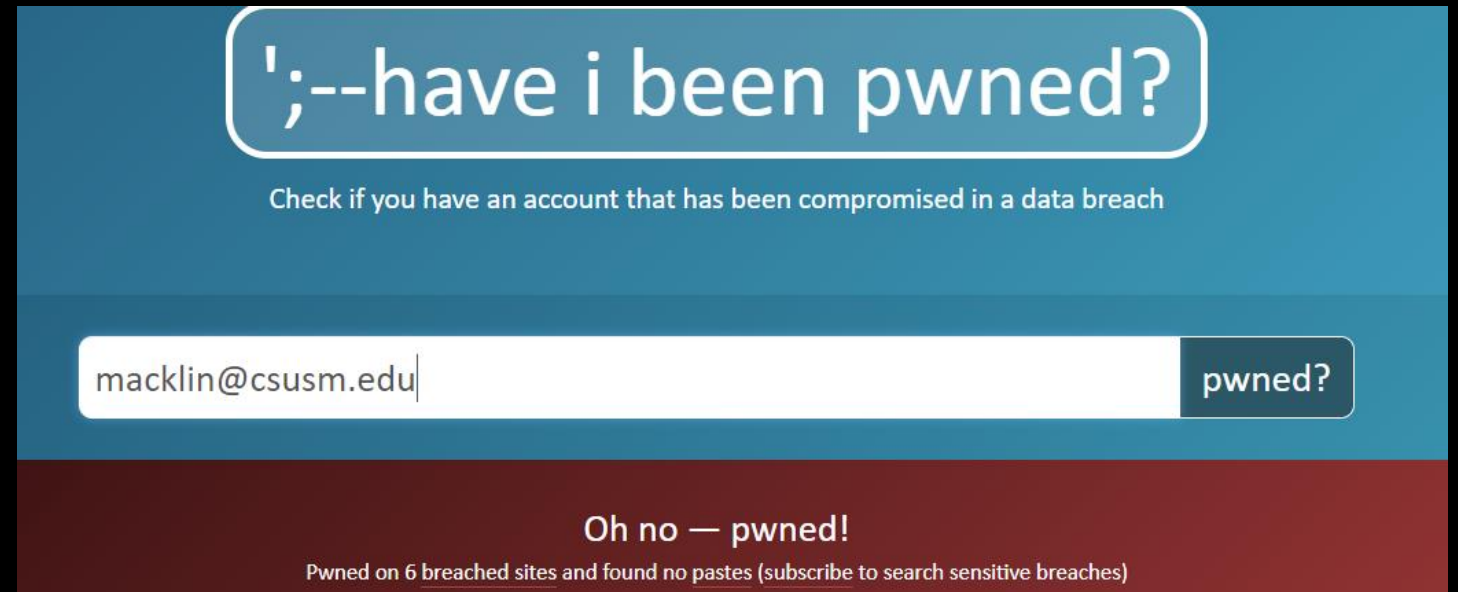
- Phishing – the practice of sending fraudulent email to get the victim to reveal information or take some action
- Historically - reveal personal info – account info, password, etc
- Now – click fake link to get payment or password

Phishing Message Characteristics

- Phishing: Attempts to induce people to reveal confidential information.
 - Characteristics:
 - Urgent – “Your account will be deactivated!”
 - “Look-alike” – email will appear to come from a known sender. It will use their logo, graphics, etc.
 - Scam – the “Nigerian Prince” scenario
 - Threat – the “IRS Notice” or similar
 - Tech Support – “Your computer is infected!”

Phishing for Credentials – Why?

- With your username and password:
 - Access to current system
 - Will it work on google? Amazon? E-bay?
- Can your system be used for fraud?
 - Send millions of phishing messages from your account?
- <https://haveibeenpwned.com/>



';--have i been pwned?

Check if you have an account that has been compromised in a data breach

macklin@csusm.edu | pwned?

Oh no — pwned!

Pwned on 6 breached sites and found no pastes (subscribe to search sensitive breaches)

Phishing for Dollars – Fraud (Phraud?)

- Common among students – the “work part time” scam
 - Criminals “hire” student to do admin work
 - Send student check to be deposited in students account
 - Asks student to disburse funds in various ways
 - Deposited check is canceled, student is out the money

----- Forwarded message -----

From: Dr Glenn Washman <almufty84@gmail.com>

Date: Tue, Mar 26, 2019 at 11:31 AM

Subject: University recruiting department Internship fixed-term II

To:

Dear Student,

I trust you are doing fine and i hope this finds you in a good frame of mind.i'm Dr Glenn Bushman and I'm very pleased discussing this WORK- STUDY opening since you were referred by the university chamber of commerce. I am very busy that is why i have asked for your help as my temporary personal assistant. I provide individual,group therapy and assessment for many of the university students with academic difficulties because of one disabilities or the other.

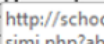
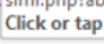
You have received this email because you have been selected from among several university students to work with me while we help Students with disabilities but as my temporary personal assistant.

Phishing – Urgent Problem

You Have 23 Undelivered/Pending Messages

Hi  @csusm.edu

Outlook Mail Service Server On 10th of February 2018 UTC 12:00AM, Detected
About (23) clustered messages Undelivered/Pending to your MailBox, They are awaiting your aproval to be delivered.

Below are list of approved ac  or
messages back to your mail  <http://school-of-teacher-training.co.uk/simi.php?abuja=mmagana@csusm.edu>
Click or tap to follow link.

*[View/Authorize Delivery for pending mails](#) From "Outlook Cloud Sever"

*[Report Error To Office Helpdesk](#) Microsoft Administrators at "Outlook IT Help Desk"

Further messages might be prevented if any of the above actions are not performed.

From: Microsoft365 Office Secured service <hcroteau@vicwest.com>

Date: Tuesday, February 20, 2018 at 12:04 PM

Subject: Your password will expire in two days

 Office 365

Microsoft

Thank you for submitting an automated request to delist your email address from suspension list.

<https://goo.gl/y721i>
Click or tap to follow

To complete the process, please confirm your email address by clicking the following link: [Confirm your email address](#)

*NOTE - Please do not respond to this email. It's sent from an unmonitored address.**

Malware – Why?

- “Pwn” your computer systems to
 - Harvest your data
 - Make your computer part of a “botnet”
 - Use your computer to mine bitcoin
- Ransomware
 - May threaten to publish your data or
 - May encrypt your data and require you to pay to receive the encryption key



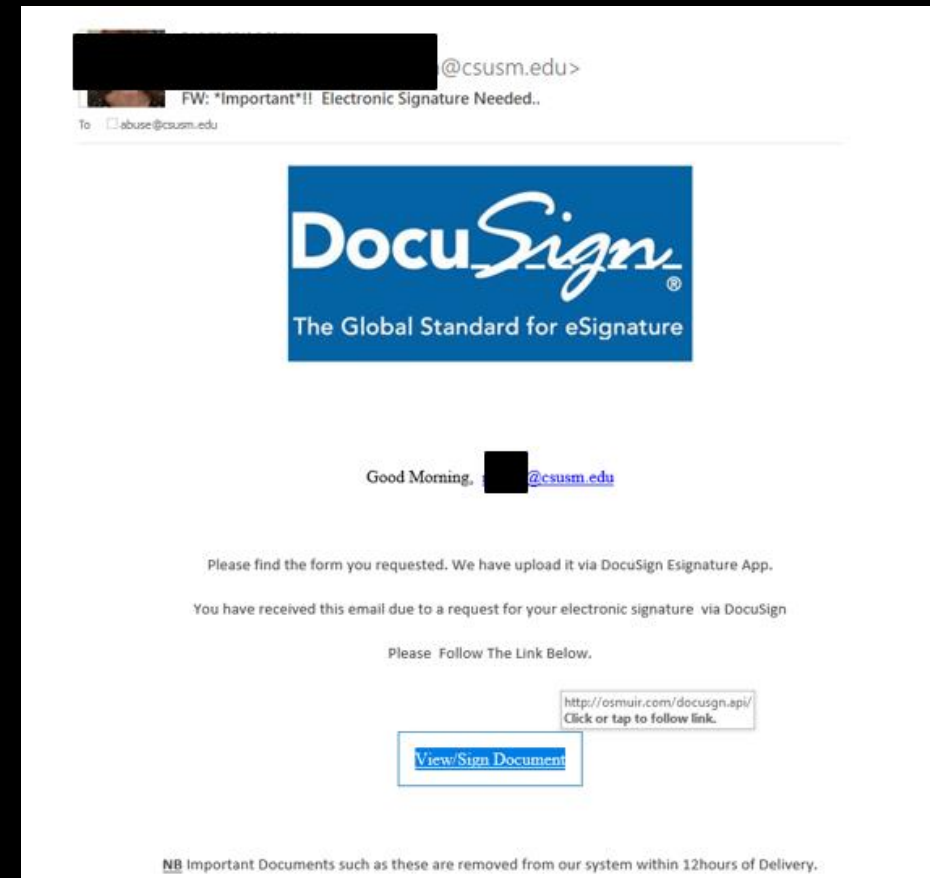
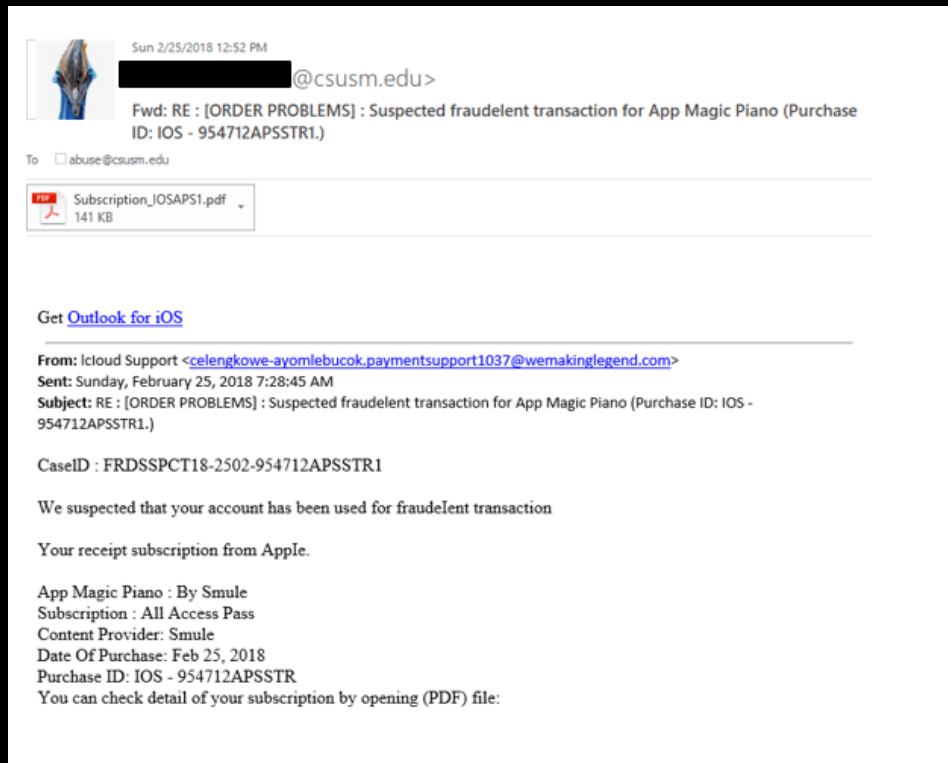
NEWS

Ransomware damage costs predicted to hit \$11.5B by 2019

Cyber crime rises sharply amidst a decline in the percentage of victims willing to pay ransoms.



Malware by Email



Protecting Yourself: Interacting via Email, Voice

- Phishing and Fraud:
 - Don't open attachments from strangers
 - Don't click links from strangers
 - Use your browser to "hover" over links before you click them. If they look weird, treat them as bad.
 - Don't write back to the sender to see if it was a real message!
 - Golden rule: If you didn't expect it, it could be phishing or fraud
 - Strangers on the internet are not going to offer you jobs, prizes or other good stuff

Protecting Yourself: Your Personal Computer

- Install and maintain an anti-virus program
- Install every security update – java, adobe, operating system... all of them. Every time.
- Look for and avoid those phishing messages (and phone calls!)
- Use a unique password everywhere
 - Use a password manager program
- Enable multi-factor authentication everywhere
- Don't give out your password!
- Be careful about connecting to unknown wireless networks