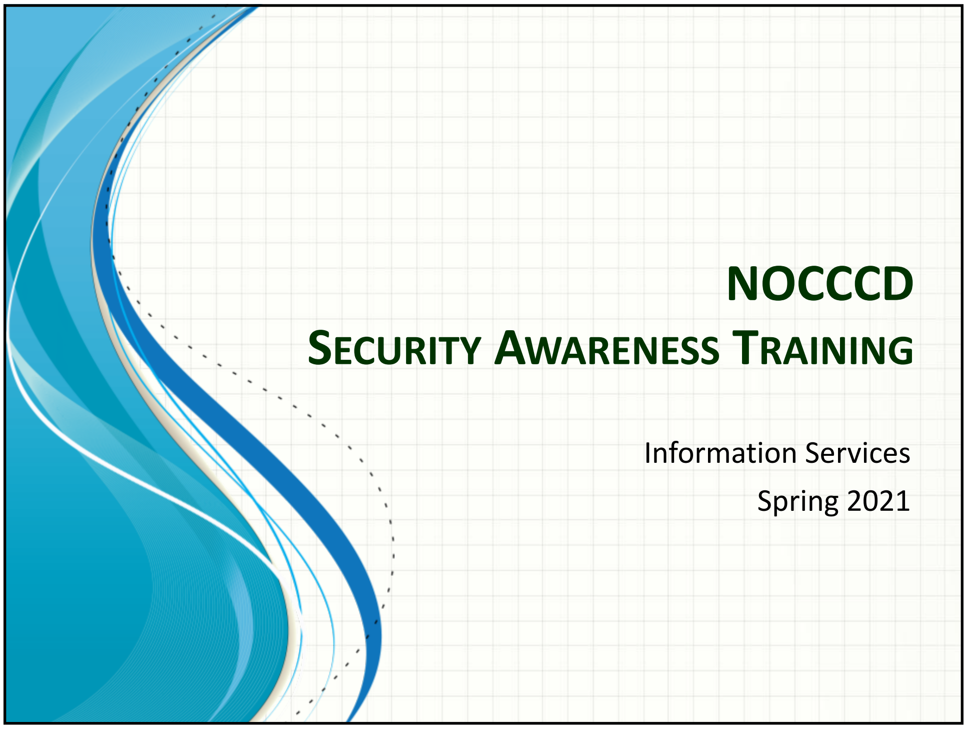
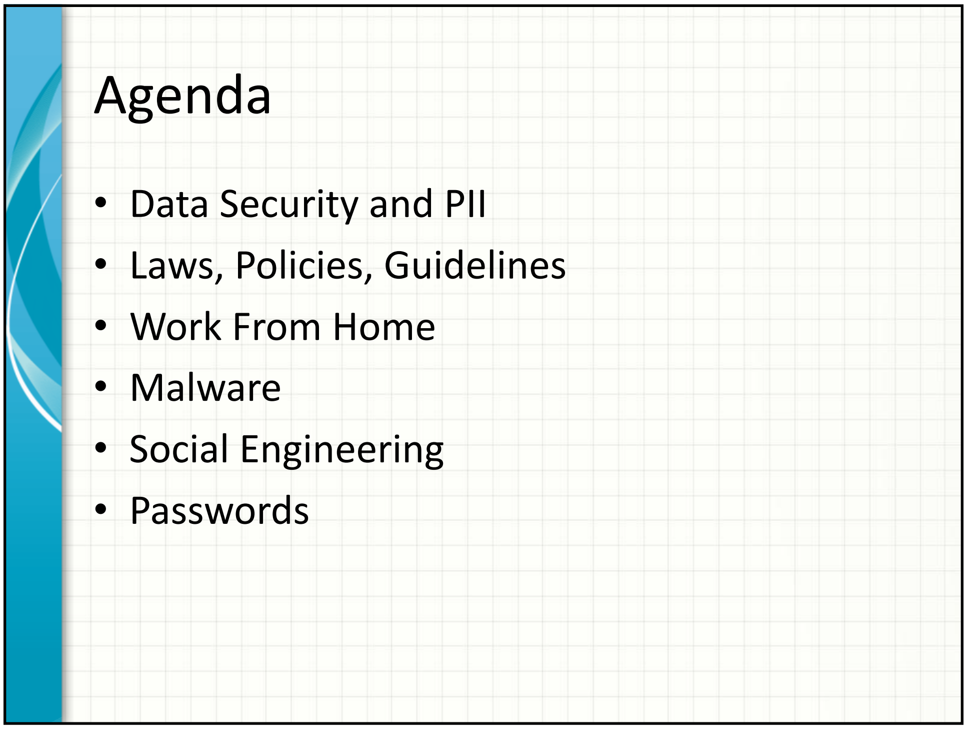


NOCCCD
SECURITY AWARENESS TRAINING

Information Services

Spring 2021

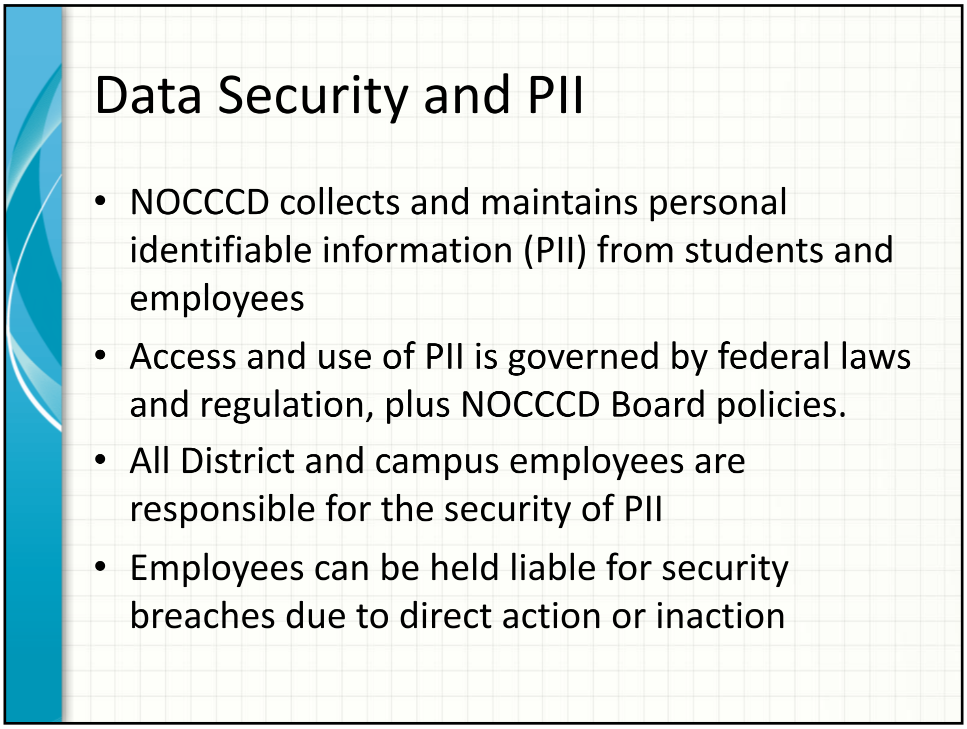
1



Agenda

- Data Security and PII
- Laws, Policies, Guidelines
- Work From Home
- Malware
- Social Engineering
- Passwords

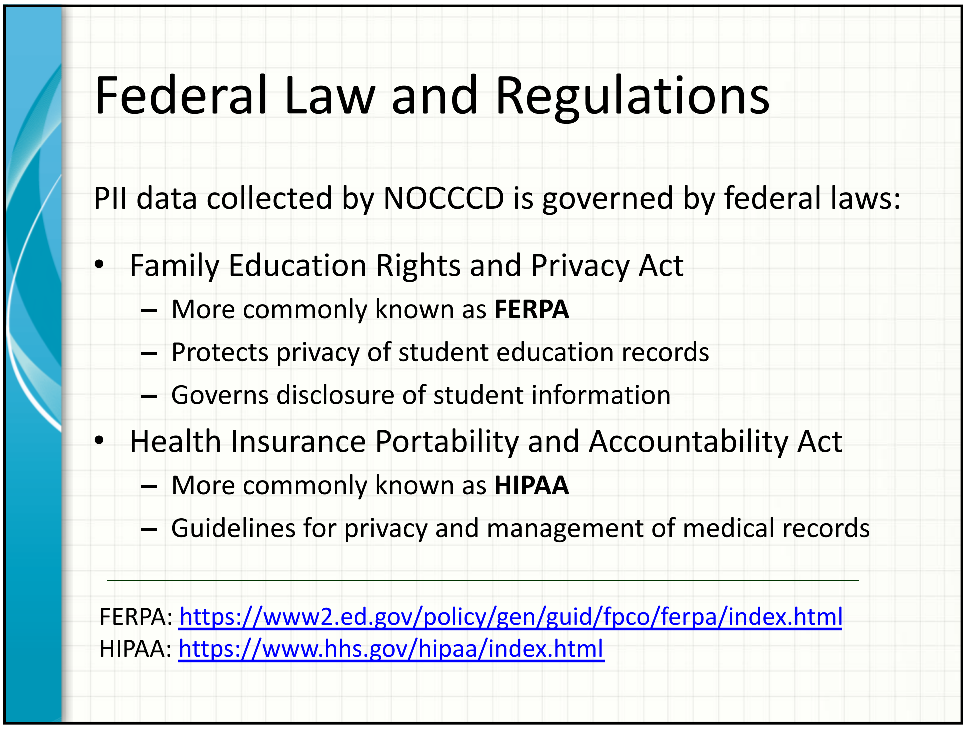
2



Data Security and PII

- NOCCCD collects and maintains personal identifiable information (PII) from students and employees
- Access and use of PII is governed by federal laws and regulation, plus NOCCCD Board policies.
- All District and campus employees are responsible for the security of PII
- Employees can be held liable for security breaches due to direct action or inaction

3



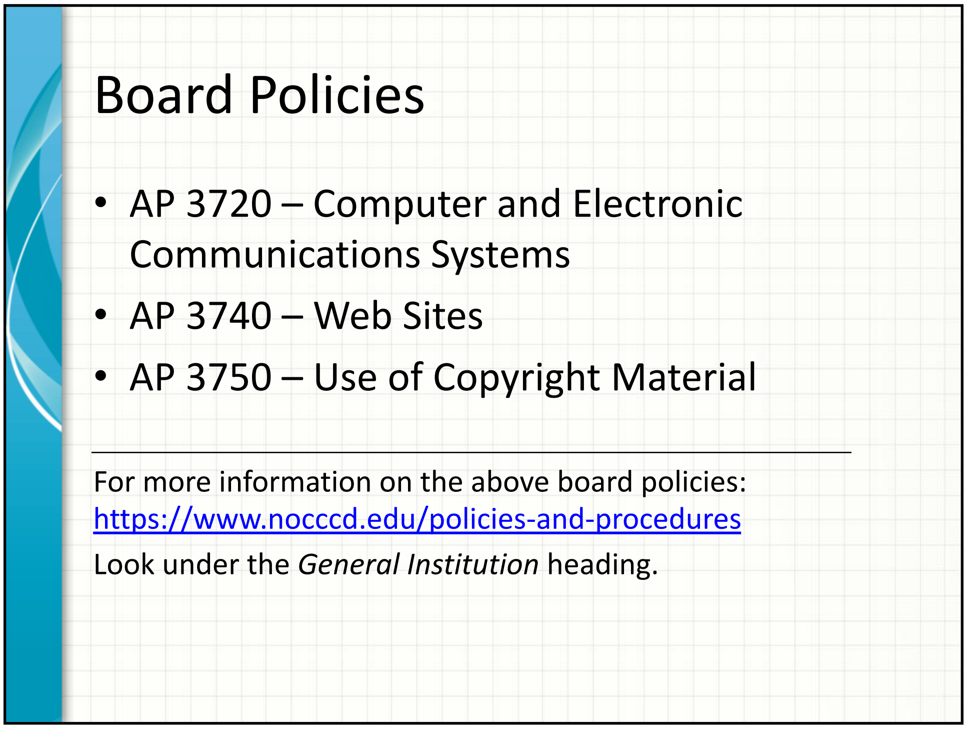
Federal Law and Regulations

PII data collected by NOCCCD is governed by federal laws:

- Family Education Rights and Privacy Act
  - More commonly known as **FERPA**
  - Protects privacy of student education records
  - Governs disclosure of student information
- Health Insurance Portability and Accountability Act
  - More commonly known as **HIPAA**
  - Guidelines for privacy and management of medical records

FERPA: https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html
HIPAA: https://www.hhs.gov/hipaa/index.html

4



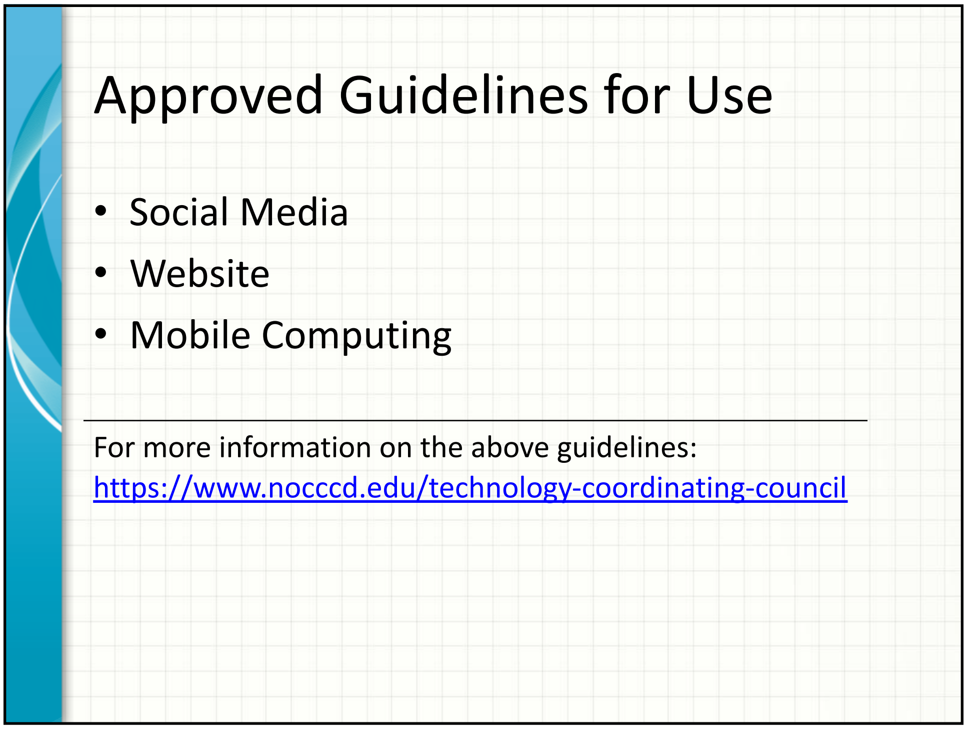
Board Policies

- AP 3720 – Computer and Electronic Communications Systems
- AP 3740 – Web Sites
- AP 3750 – Use of Copyright Material

For more information on the above board policies:
https://www.nocccd.edu/policies-and-procedures

Look under the *General Institution* heading.

5

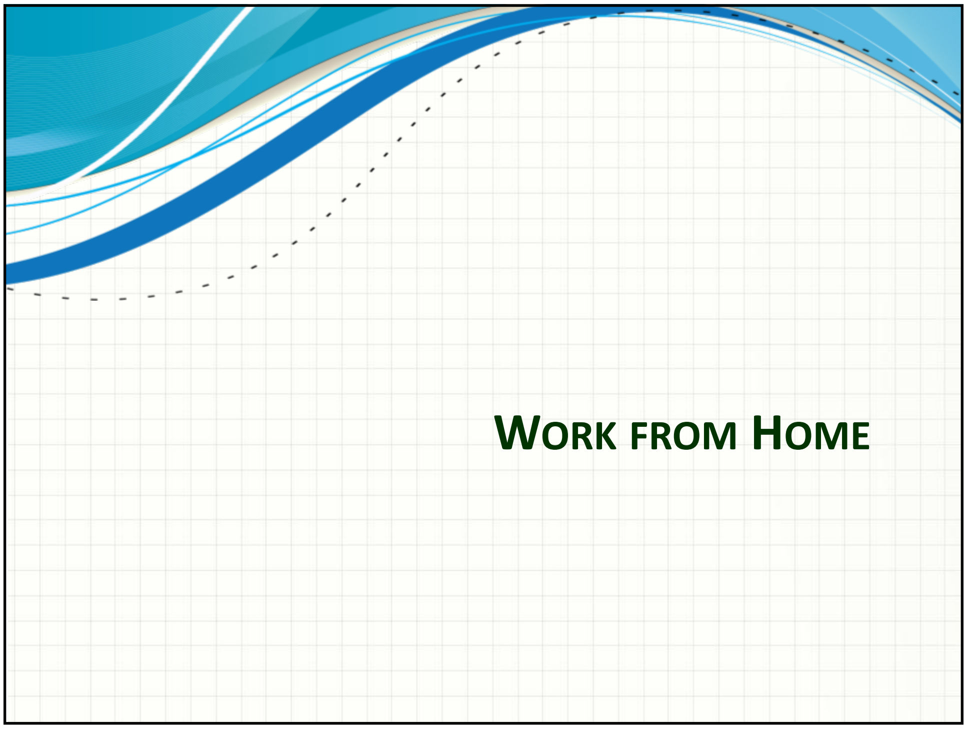


Approved Guidelines for Use

- Social Media
- Website
- Mobile Computing

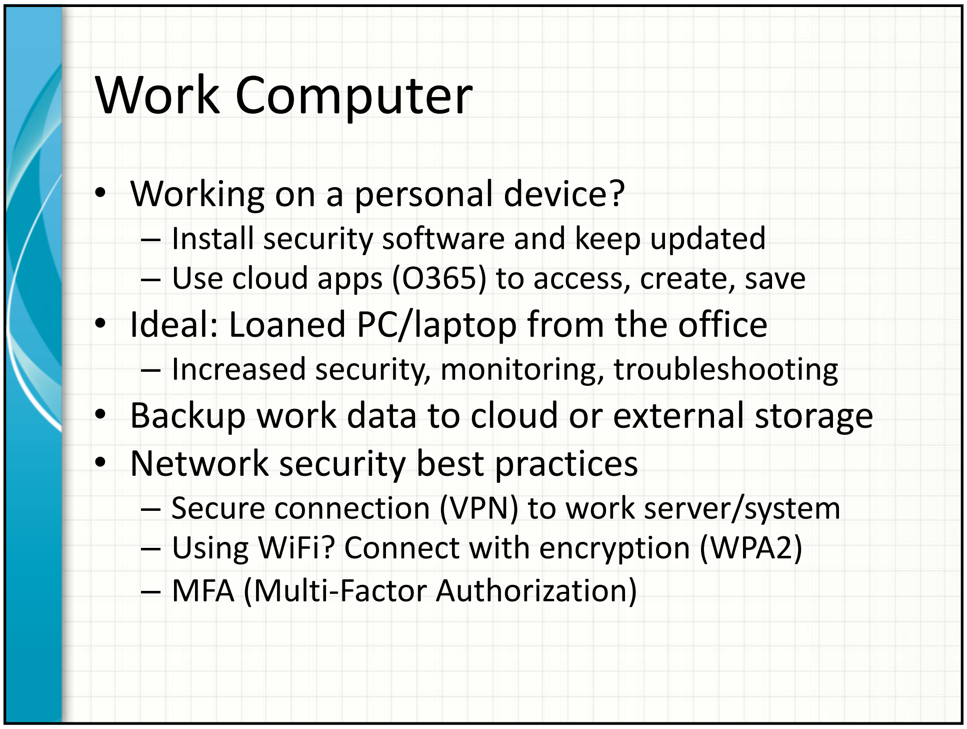
For more information on the above guidelines:
https://www.nocccd.edu/technology-coordinating-council

6



Work from Home

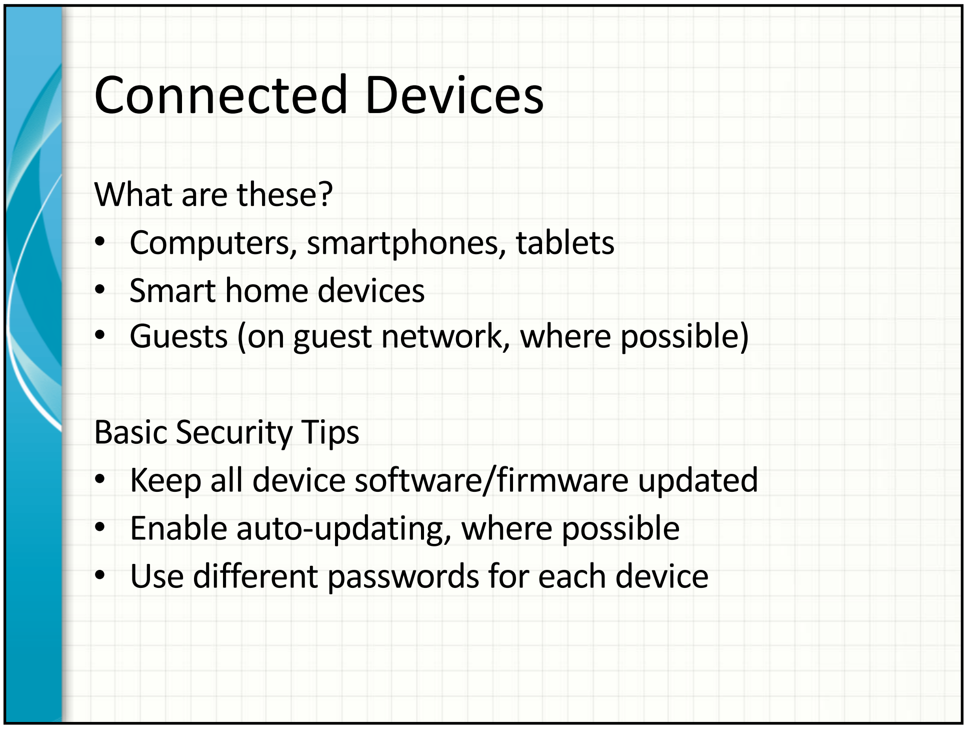
7



Work Computer

- Working on a personal device?
  - – Install security software and keep updated
  - – Use cloud apps (O365) to access, create, save
- Ideal: Loaned PC/laptop from the office
  - – Increased security, monitoring, troubleshooting
- Backup work data to cloud or external storage
- Network security best practices
  - – Secure connection (VPN) to work server/system
  - – Using WiFi? Connect with encryption (WPA2)
  - – MFA (Multi-Factor Authorization)

8



Connected Devices

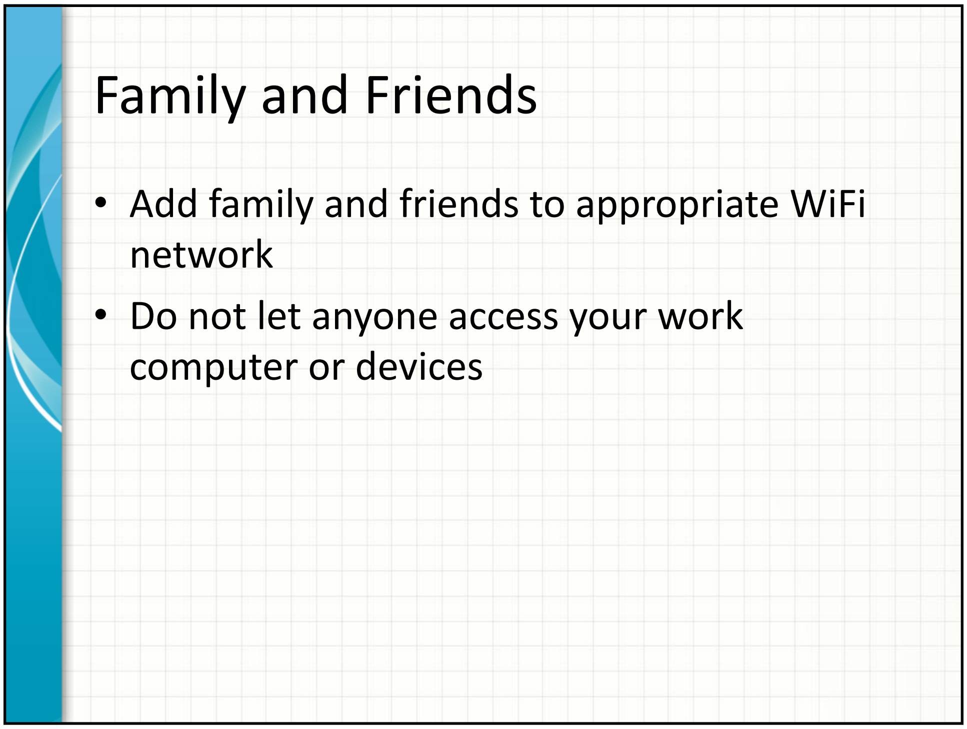
What are these?

- Computers, smartphones, tablets
- Smart home devices
- Guests (on guest network, where possible)

Basic Security Tips

- Keep all device software/firmware updated
- Enable auto-updating, where possible
- Use different passwords for each device

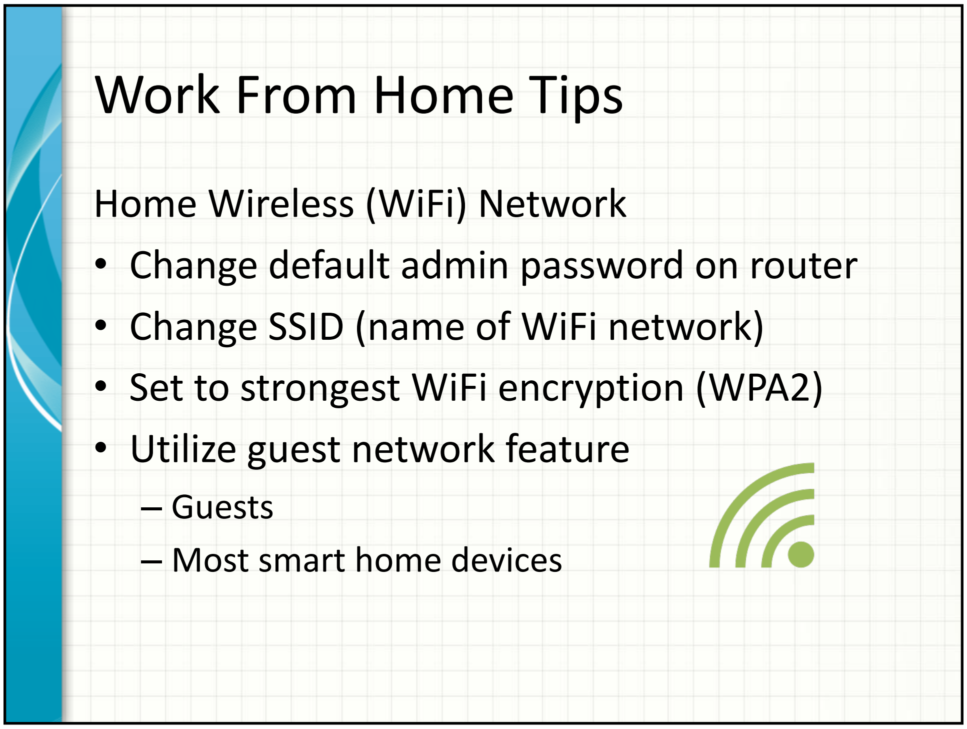
9



Family and Friends

- Add family and friends to appropriate WiFi network
- Do not let anyone access your work computer or devices

10

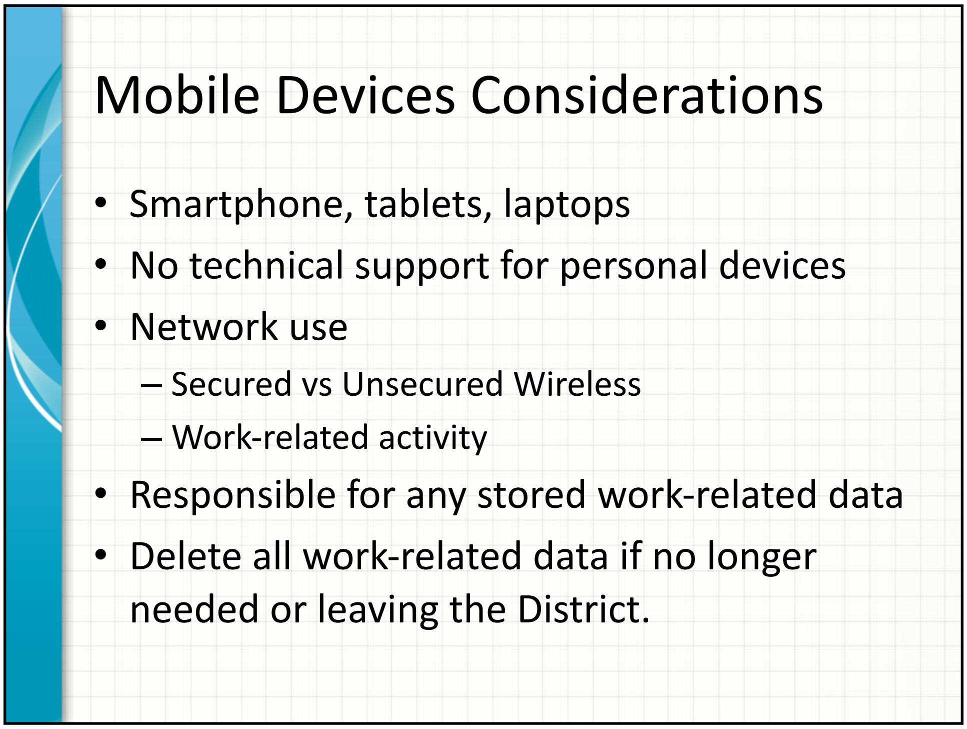


Work From Home Tips

Home Wireless (WiFi) Network

- Change default admin password on router
- Change SSID (name of WiFi network)
- Set to strongest WiFi encryption (WPA2)
- Utilize guest network feature
  - Guests
  - Most smart home devices

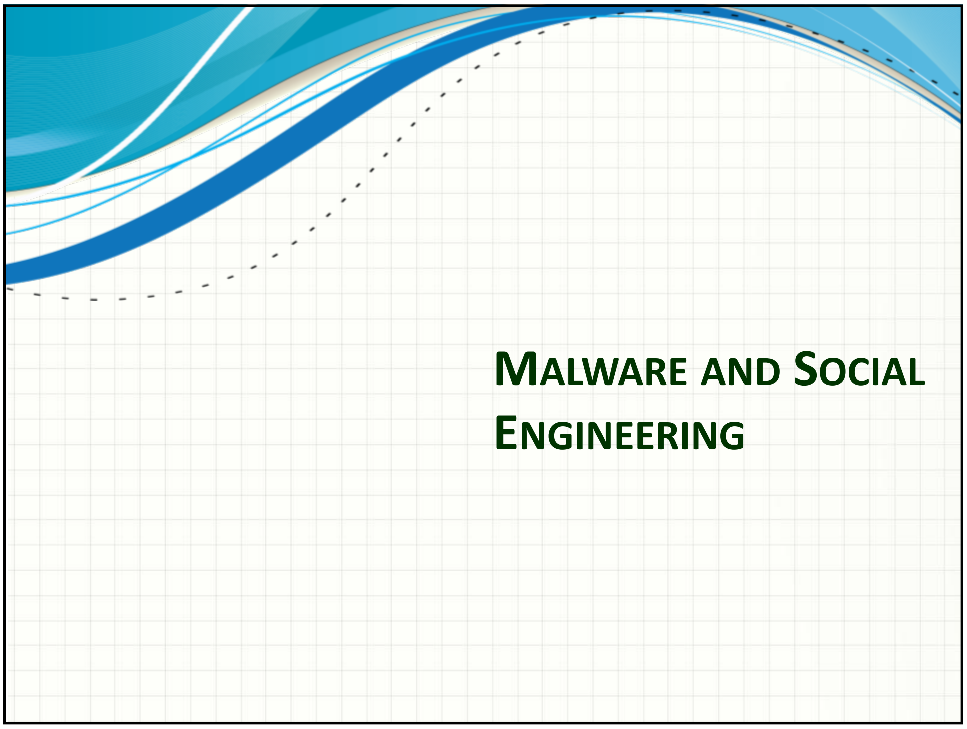
11



Mobile Devices Considerations

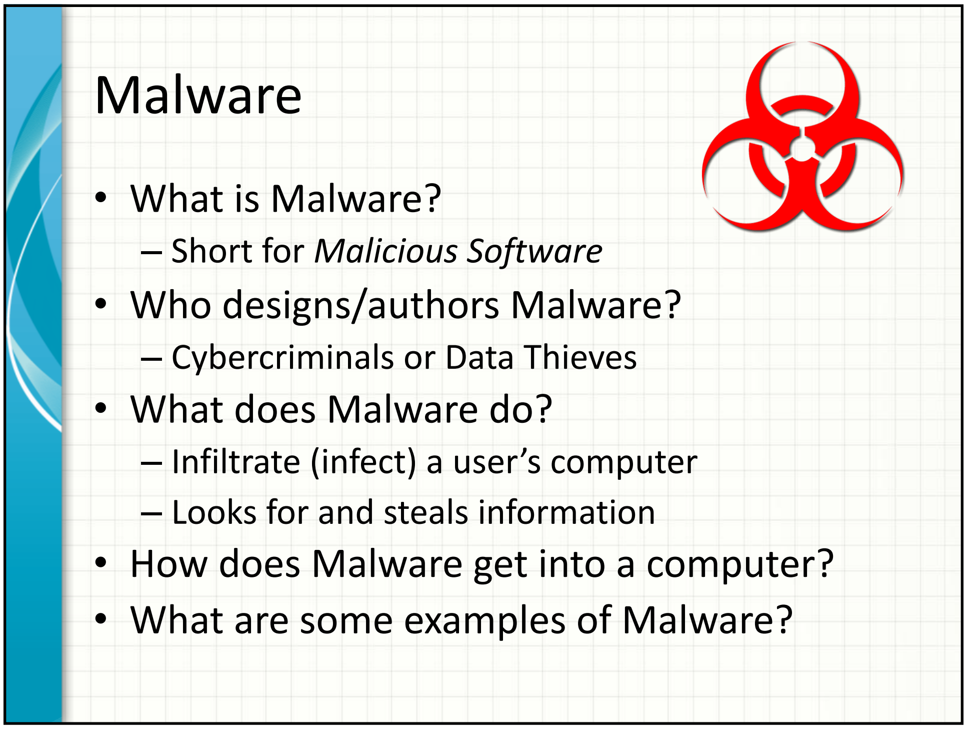
- Smartphone, tablets, laptops
- No technical support for personal devices
- Network use
  - Secured vs Unsecured Wireless
  - Work-related activity
- Responsible for any stored work-related data
- Delete all work-related data if no longer needed or leaving the District.

12



MALWARE AND SOCIAL ENGINEERING

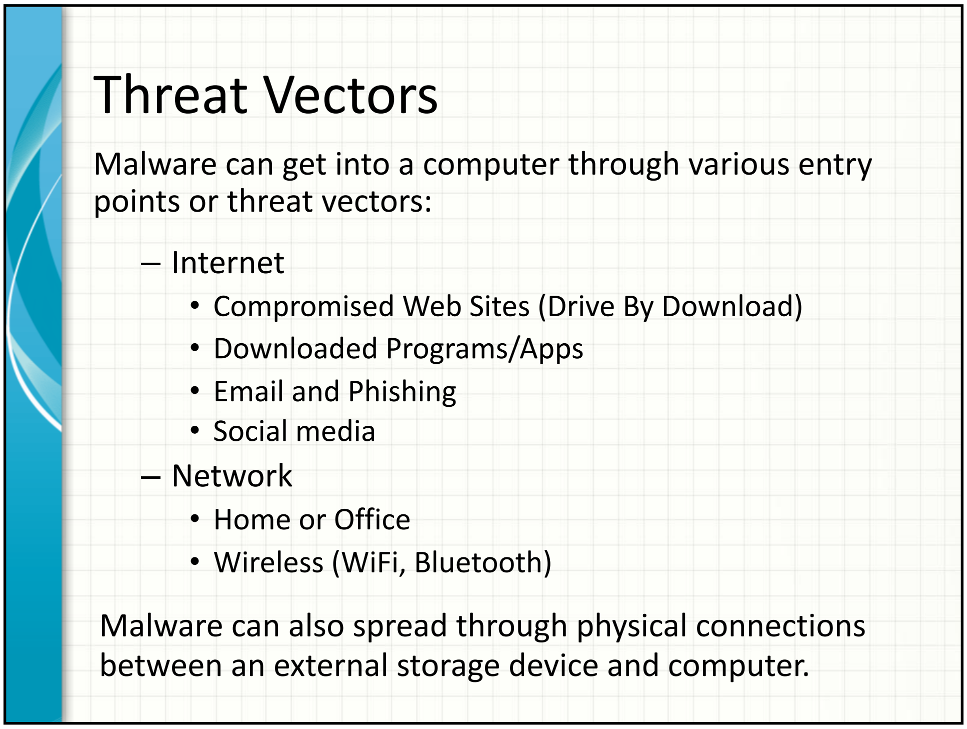
13



Malware

- What is Malware?
  - Short for *Malicious Software*
- Who designs/authors Malware?
  - Cybercriminals or Data Thieves
- What does Malware do?
  - Infiltrate (infect) a user’s computer
  - Looks for and steals information
- How does Malware get into a computer?
- What are some examples of Malware?

14



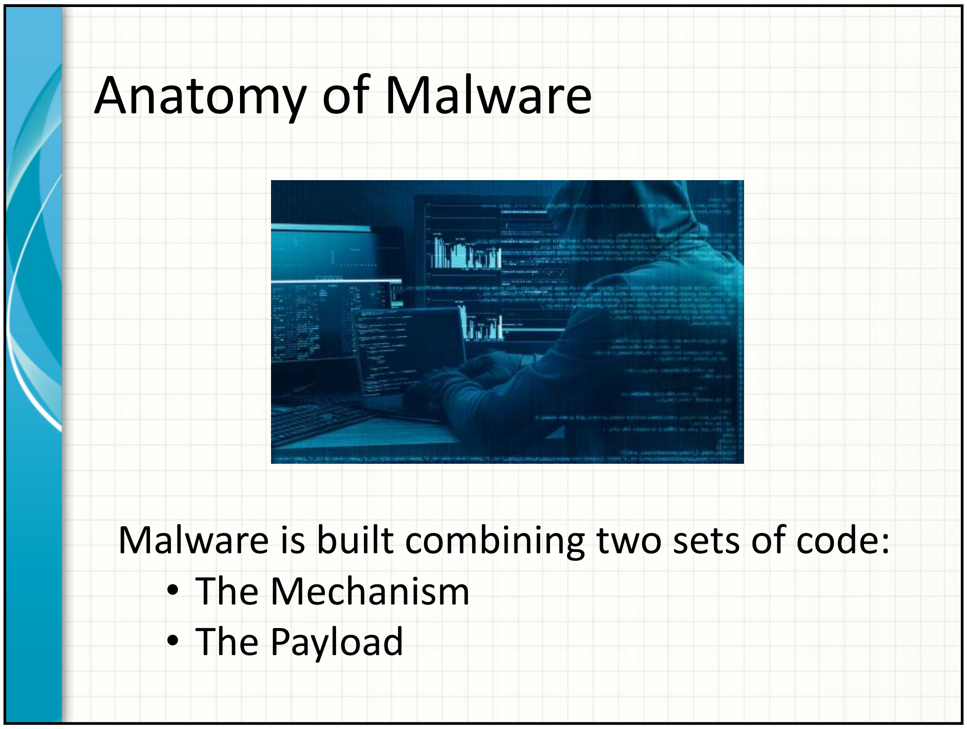
Threat Vectors

Malware can get into a computer through various entry points or threat vectors:

- Internet
  - Compromised Web Sites (Drive By Download)
  - Downloaded Programs/Apps
  - Email and Phishing
  - Social media
- Network
  - Home or Office
  - Wireless (WiFi, Bluetooth)

Malware can also spread through physical connections between an external storage device and computer.

15

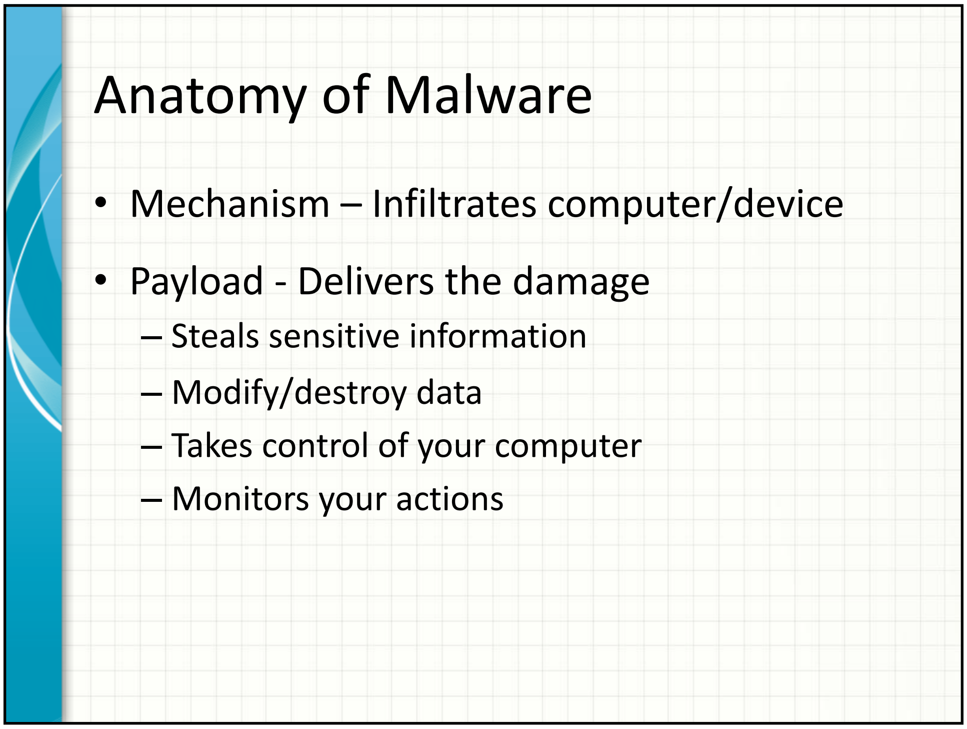


Anatomy of Malware

Malware is built combining two sets of code:

- The Mechanism
- The Payload

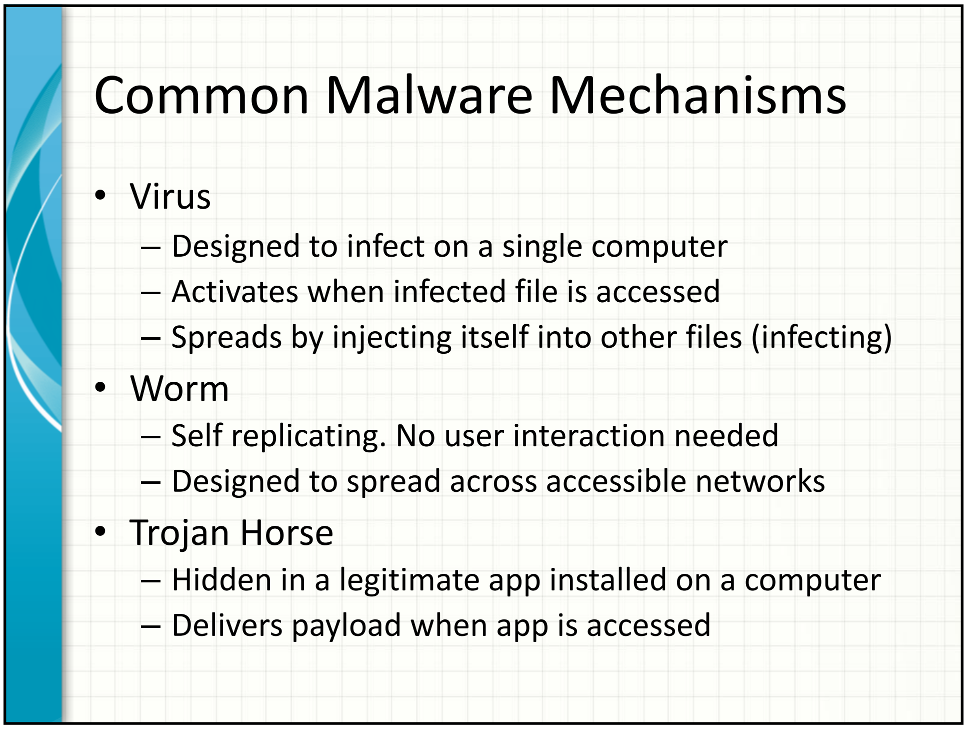
16



Anatomy of Malware

- Mechanism – Infiltrates computer/device
- Payload - Delivers the damage
  - Steals sensitive information
  - Modify/destroy data
  - Takes control of your computer
  - Monitors your actions

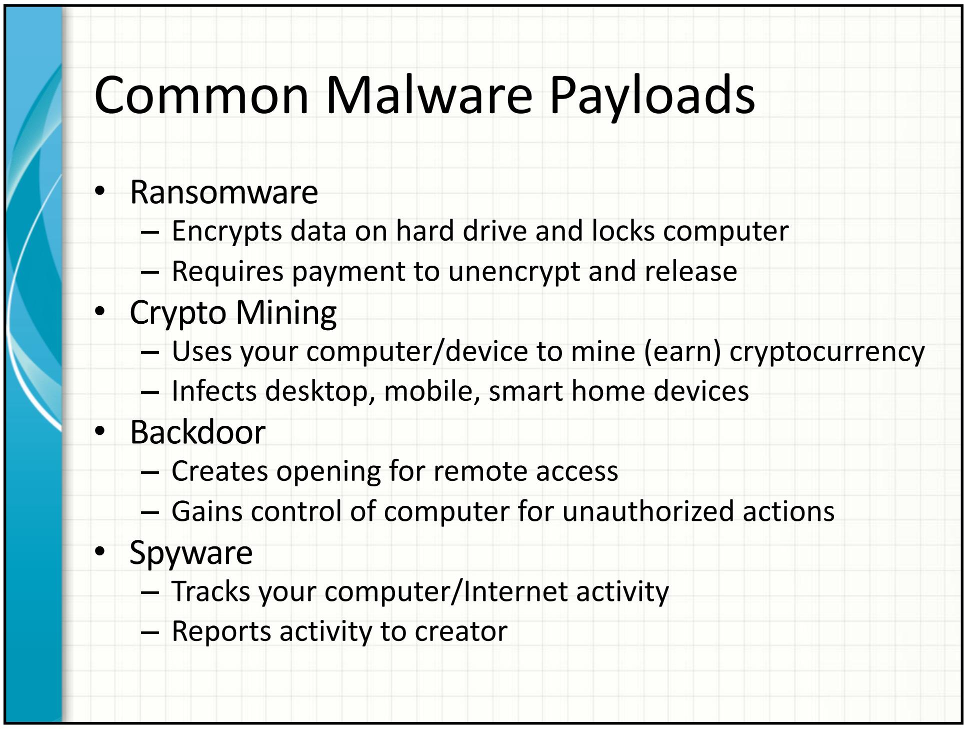
17



Common Malware Mechanisms

- Virus
  - Designed to infect on a single computer
  - Activates when infected file is accessed
  - Spreads by injecting itself into other files (infecting)
- Worm
  - Self replicating. No user interaction needed
  - Designed to spread across accessible networks
- Trojan Horse
  - Hidden in a legitimate app installed on a computer
  - Delivers payload when app is accessed

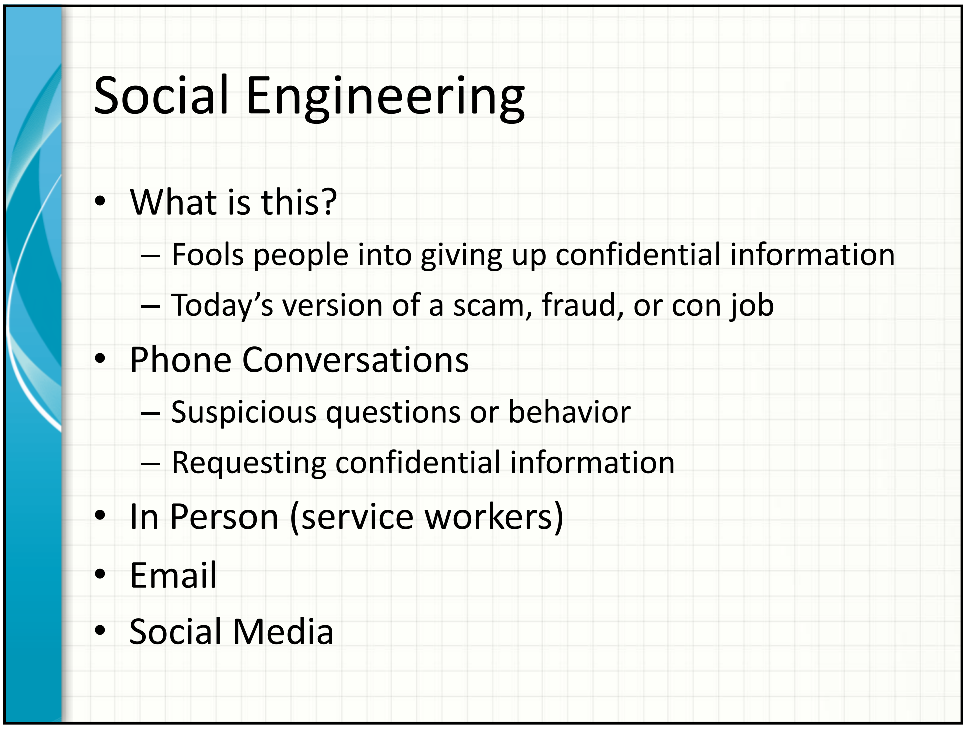
18



Common Malware Payloads

- Ransomware
  - Encrypts data on hard drive and locks computer
  - Requires payment to unencrypt and release
- Crypto Mining
  - Uses your computer/device to mine (earn) cryptocurrency
  - Infects desktop, mobile, smart home devices
- Backdoor
  - Creates opening for remote access
  - Gains control of computer for unauthorized actions
- Spyware
  - Tracks your computer/Internet activity
  - Reports activity to creator

19



Social Engineering

- What is this?
  - Fools people into giving up confidential information
  - Today’s version of a scam, fraud, or con job
- Phone Conversations
  - Suspicious questions or behavior
  - Requesting confidential information
- In Person (service workers)
- Email
- Social Media

20

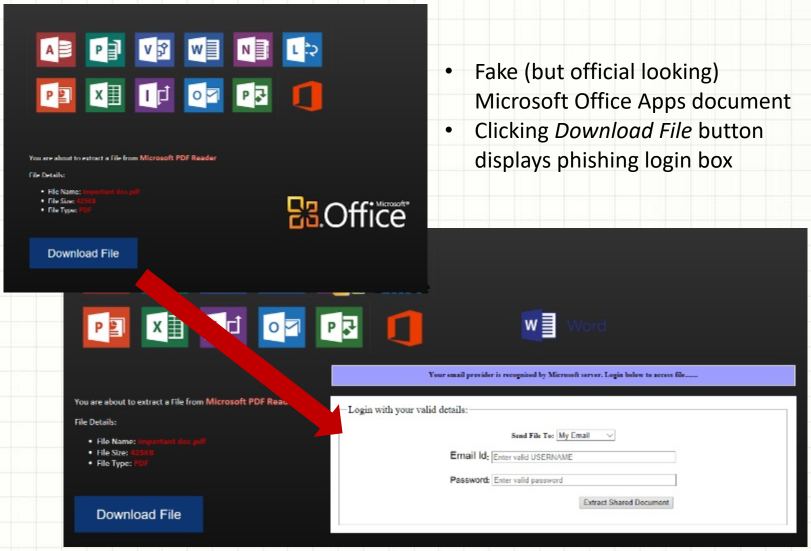
Email Threats

- Attachments
  - Confirm with sender if attachment not expected
  - Delete if sender is unknown
  - Malware can also hide in MS Office files and PDFs
  - Be careful if attached file requests access to run code
- Phishing Attacks
  - Know the classic signs (Review Handout)
  - Look before you click on links
  - Never provide personal, financial, login information
  - Can also trigger a malware attack

Important: Contact your campus ACT or our Help Desk if you are suspicious about an email you received.

21

Phishing Site Example (Chancellor)



You are about to extract a File from Microsoft PDF Reader

File Details:

- File Name: important doc.pdf
- File Size: 425KB
- File Type: PDF

Your email provider is recognized by Microsoft server. Login below to access file......

Login with your valid details:

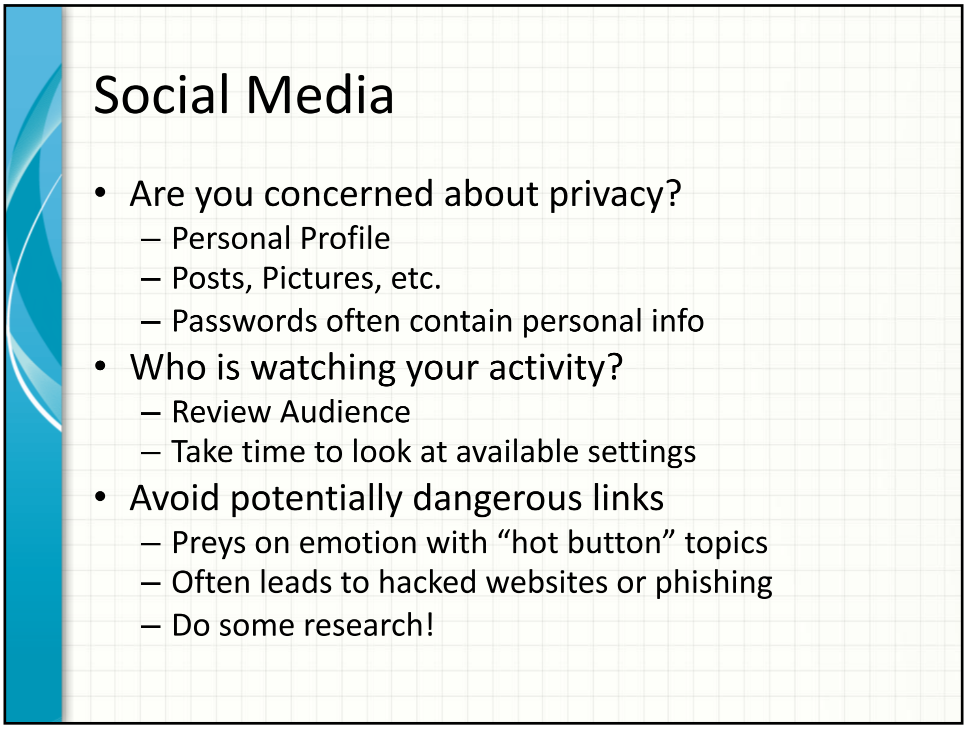
Send File To: My Email

Email Id: Enter valid USERNAME

Password: Enter valid password

- Fake (but official looking) Microsoft Office Apps document
- Clicking *Download File* button displays phishing login box

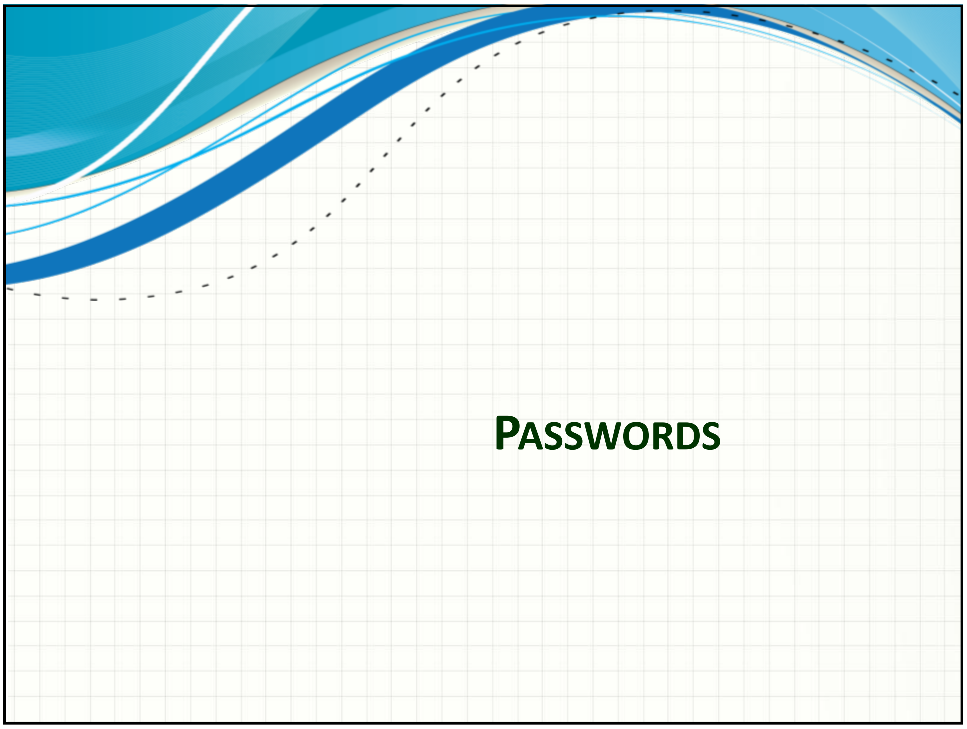
22



Social Media

- Are you concerned about privacy?
  - Personal Profile
  - Posts, Pictures, etc.
  - Passwords often contain personal info
- Who is watching your activity?
  - Review Audience
  - Take time to look at available settings
- Avoid potentially dangerous links
  - Preys on emotion with “hot button” topics
  - Often leads to hacked websites or phishing
  - Do some research!

23



PASSWORDS

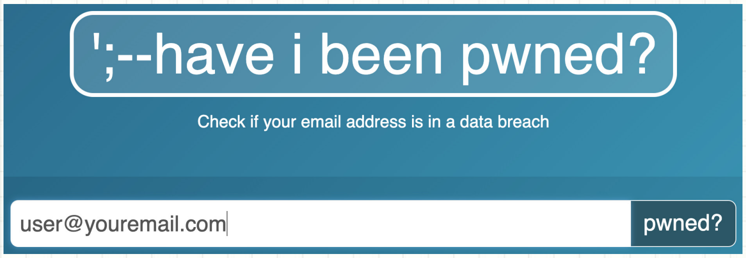
24

Passwords

- First and last line of defense to your data
- How passwords are stolen:
  - Phishing attacks
  - Repeating passwords from other logins
  - Guessed using personal information
  - Commonly used or weak password
  - Spyware (keyloggers)
  - Written down and stored in physical location
  - Unrelated data breach

25

Data Breach



';--have i been pwned?

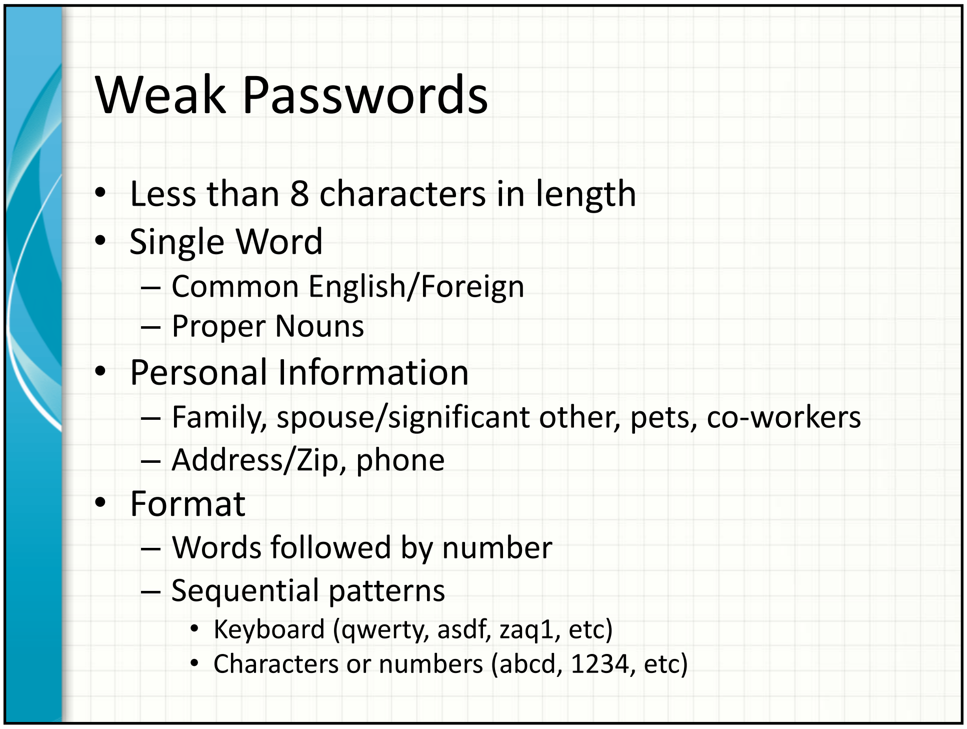
Check if your email address is in a data breach

user@youremail.com

https://haveibeenpwned.com/

- Personal data may have been stolen
- In most cases, you were not notified
- Check your email addresses
- Consider password changes based on results

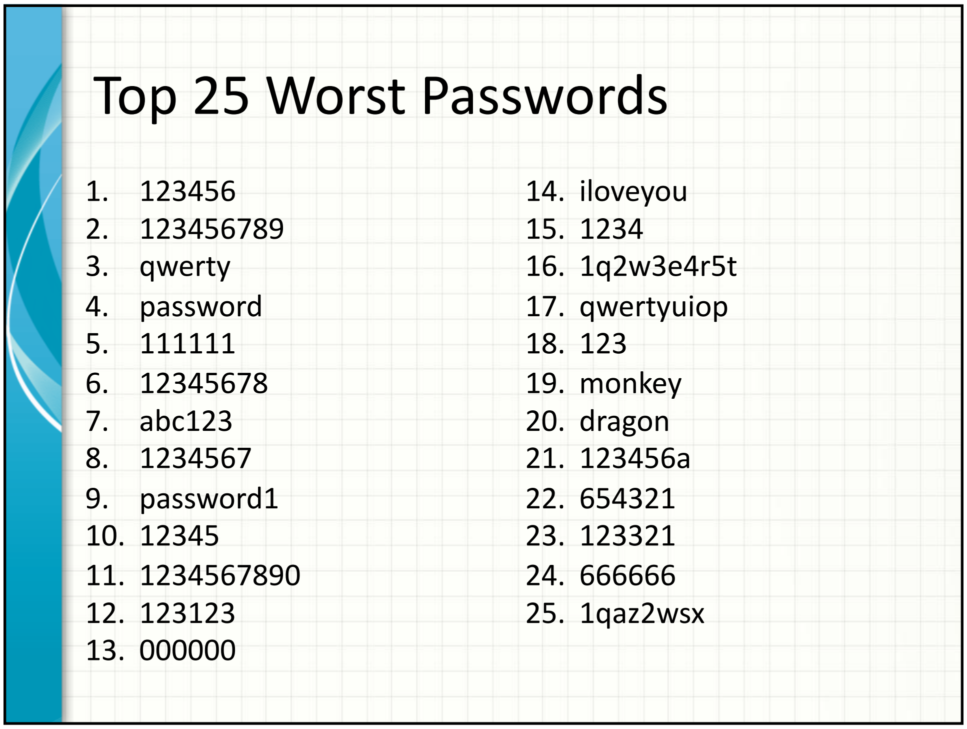
26



Weak Passwords

- Less than 8 characters in length
- Single Word
  - Common English/Foreign
  - Proper Nouns
- Personal Information
  - Family, spouse/significant other, pets, co-workers
  - Address/Zip, phone
- Format
  - Words followed by number
  - Sequential patterns
    - Keyboard (qwerty, asdf, zaq1, etc)
    - Characters or numbers (abcd, 1234, etc)

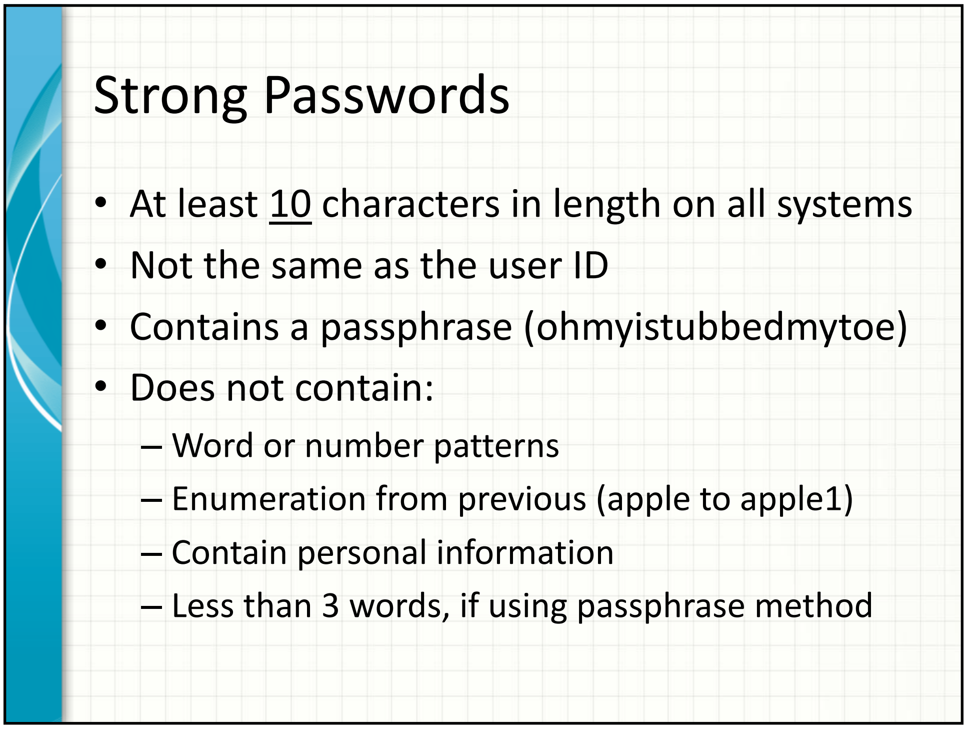
27



Top 25 Worst Passwords

1. 123456
2. 123456789
3. qwerty
4. password
5. 111111
6. 12345678
7. abc123
8. 1234567
9. password1
10. 12345
11. 1234567890
12. 123123
13. 000000
14. iloveyou
15. 1234
16. 1q2w3e4r5t
17. qwertyuiop
18. 123
19. monkey
20. dragon
21. 123456a
22. 654321
23. 123321
24. 666666
25. 1qaz2wsx

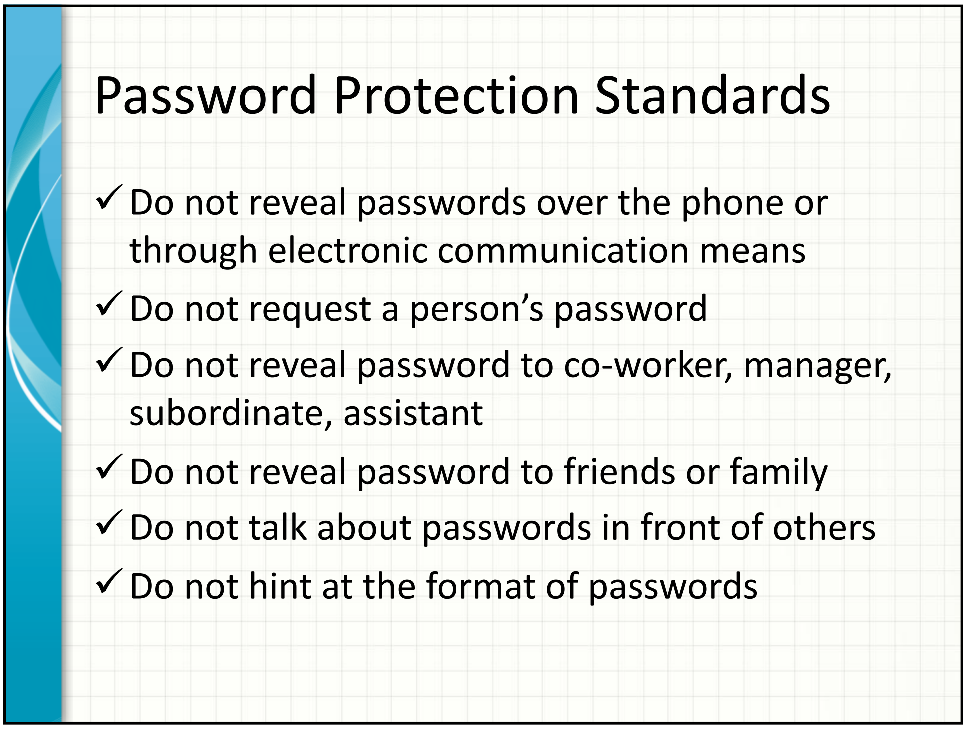
28



Strong Passwords

- At least 10 characters in length on all systems
- Not the same as the user ID
- Contains a passphrase (ohmyistubbedmytoe)
- Does not contain:
  - Word or number patterns
  - Enumeration from previous (apple to apple1)
  - Contain personal information
  - Less than 3 words, if using passphrase method

29



Password Protection Standards

✓ Do not reveal passwords over the phone or through electronic communication means

✓ Do not request a person’s password

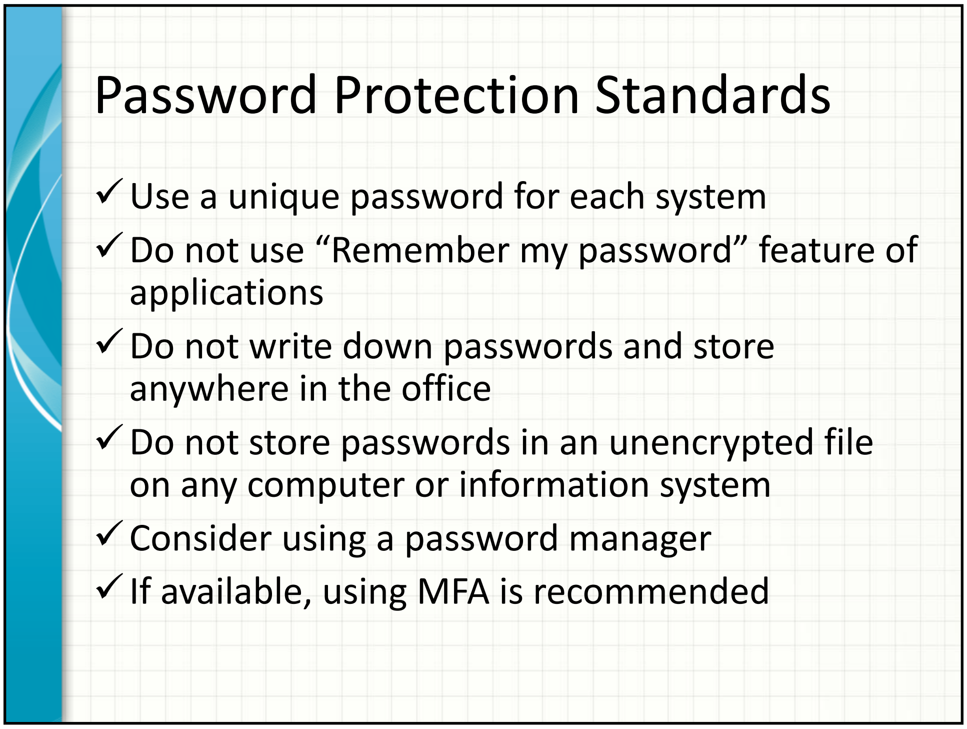
✓ Do not reveal password to co-worker, manager, subordinate, assistant

✓ Do not reveal password to friends or family

✓ Do not talk about passwords in front of others

✓ Do not hint at the format of passwords

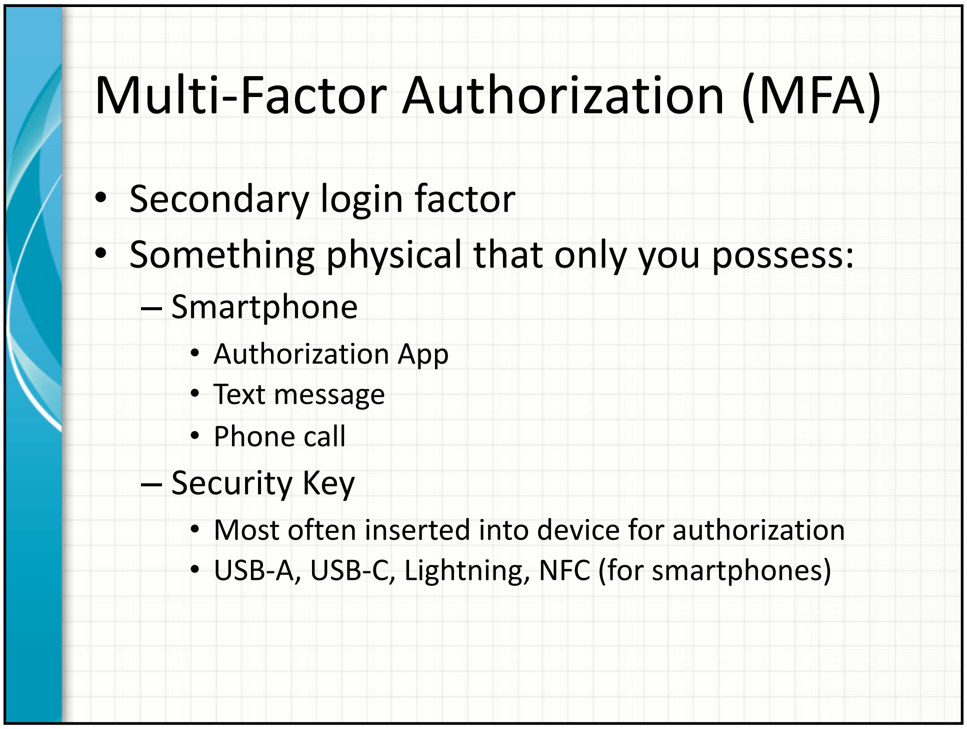
30



Password Protection Standards

- ✓ Use a unique password for each system
- ✓ Do not use “Remember my password” feature of applications
- ✓ Do not write down passwords and store anywhere in the office
- ✓ Do not store passwords in an unencrypted file on any computer or information system
- ✓ Consider using a password manager
- ✓ If available, using MFA is recommended

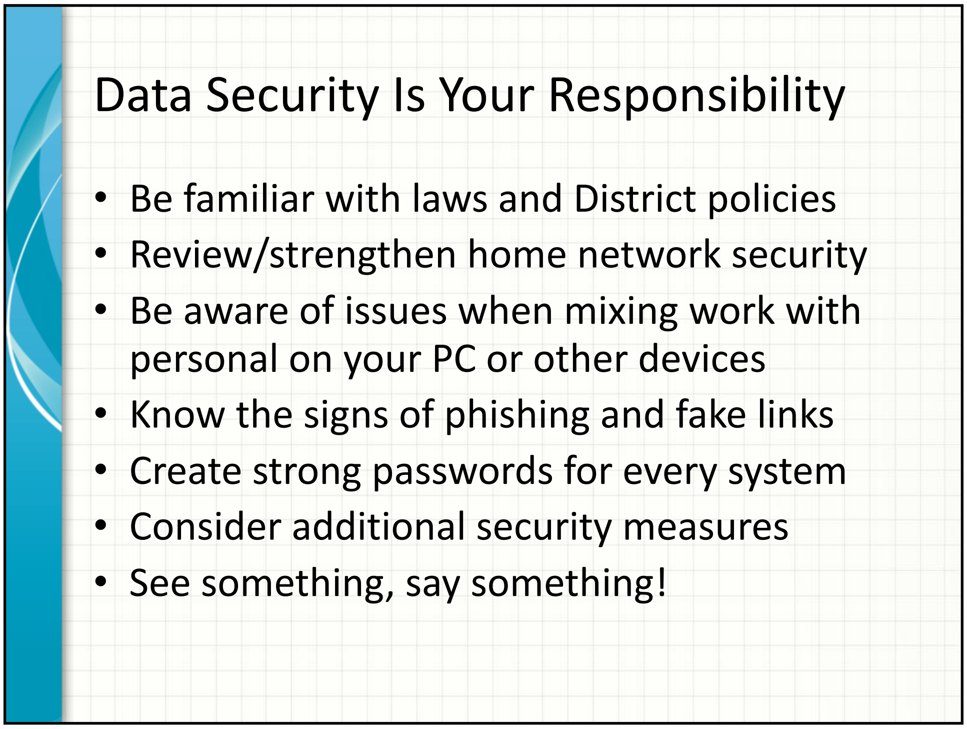
31



Multi-Factor Authorization (MFA)

- Secondary login factor
- Something physical that only you possess:
  - Smartphone
    - Authorization App
    - Text message
    - Phone call
  - Security Key
    - Most often inserted into device for authorization
    - USB-A, USB-C, Lightning, NFC (for smartphones)

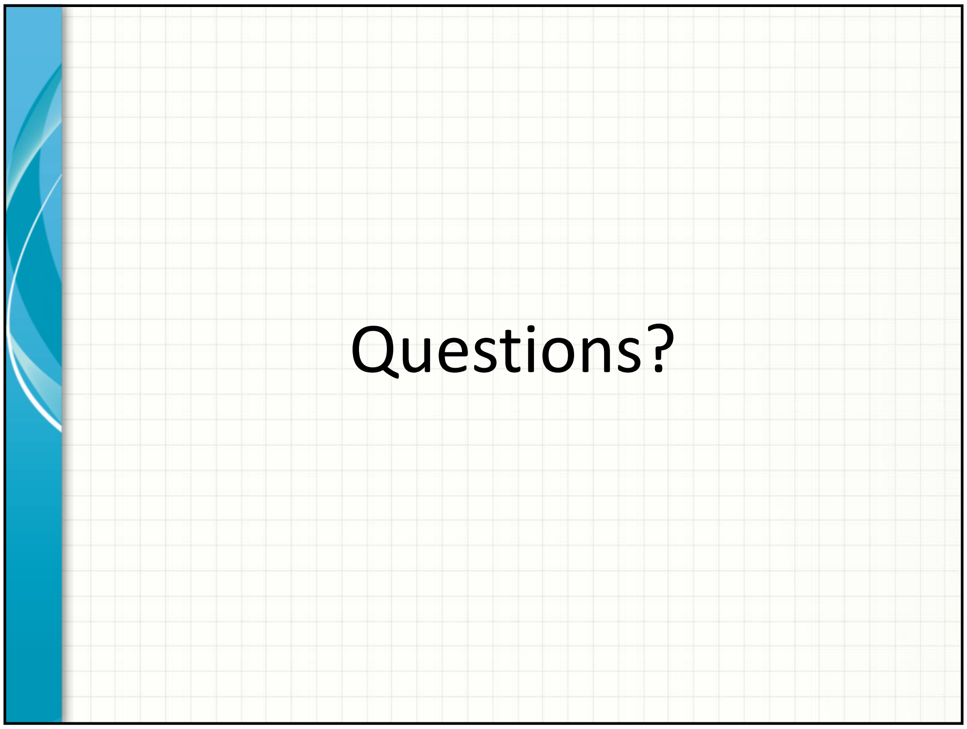
32



Data Security Is Your Responsibility

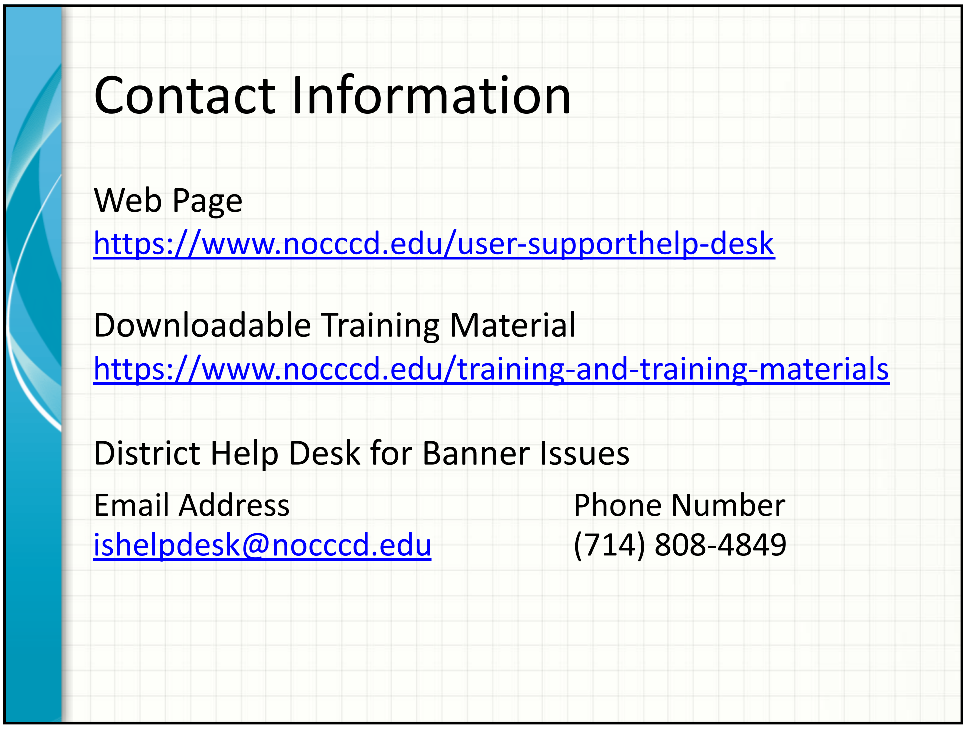
- Be familiar with laws and District policies
- Review/strengthen home network security
- Be aware of issues when mixing work with personal on your PC or other devices
- Know the signs of phishing and fake links
- Create strong passwords for every system
- Consider additional security measures
- See something, say something!

33



Questions?

34



Contact Information

Web Page
https://www.nocccd.edu/user-supporthelp-desk

Downloadable Training Material
https://www.nocccd.edu/training-and-training-materials

District Help Desk for Banner Issues

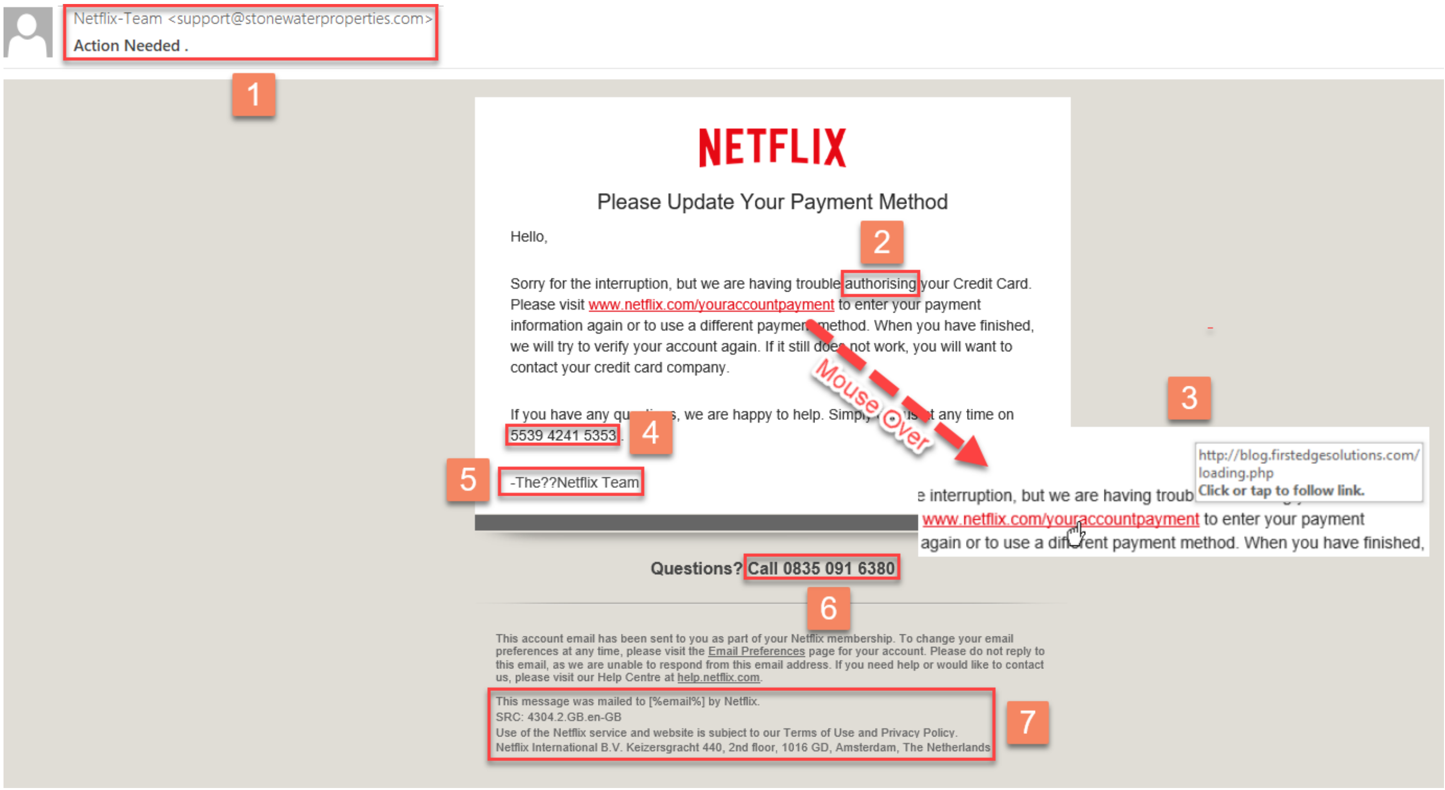
Email Address	Phone Number
ishelpdesk@nocccd.edu	(714) 808-4849

35

Email Phishing Attack Examples

Here is an example of an email phishing attack detected by District IS staff members. The email is allegedly from Netflix, the well-known streaming service. The email is cloned from an actual Netflix communication, but with the message replaced for the phishing attack.

The phishing email was easily detected by the District IS Security team due to a variety of signs that are common to this type of attack. Take a look at the screenshot below of the phishing email. The common signs are highlighted, with explanations provided below the screenshot.



Netflix-Team <support@stonewaterproperties.com>
Action Needed .

NETFLIX

Please Update Your Payment Method

Hello,

Sorry for the interruption, but we are having trouble authorising your Credit Card. Please visit www.netflix.com/youraccountpayment to enter your payment information again or to use a different payment method. When you have finished, we will try to verify your account again. If it still does not work, you will want to contact your credit card company.

If you have any questions, we are happy to help. Simply call us at any time on 5539 4241 5353.

-The??Netflix Team

http://blog.firstedgesolutions.com/loading.php
Click or tap to follow link.

e interruption, but we are having troub
www.netflix.com/youraccountpayment to enter your payment
again or to use a different payment method. When you have finished,

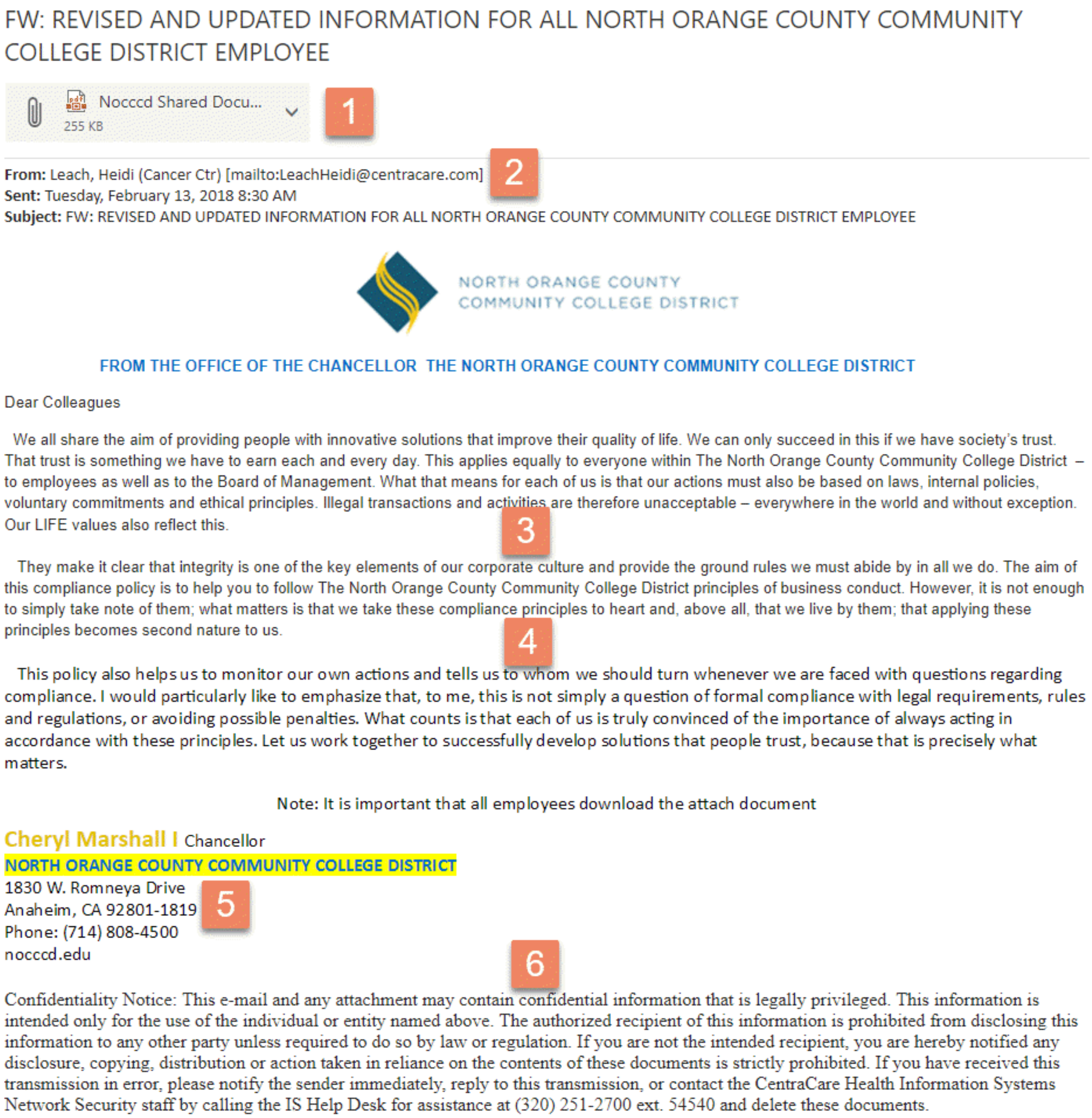
Questions? Call 0835 091 6380

This account email has been sent to you as part of your Netflix membership. To change your email preferences at any time, please visit the Email Preferences page for your account. Please do not reply to this email, as we are unable to respond from this email address. If you need help or would like to contact us, please visit our Help Centre at help.netflix.com.

This message was mailed to [%email%] by Netflix.
SRC: 4304.2.GB.en-GB
Use of the Netflix service and website is subject to our Terms of Use and Privacy Policy.
Netflix International B.V. Keizersgracht 440, 2nd floor, 1016 GD, Amsterdam, The Netherlands

1	Email address does not match sender. Also note the punctuation in the subject line.
2	Not the American spelling of the word
3	Displayed link and the actual destination link do not match
4	Not a valid phone number in the United States
5	Extra characters displayed
6	Not a valid phone number in the United States. Number also differs from the message.
7	Contact information displayed is in a foreign country (The Netherlands)

This phishing attack, allegedly from our Chancellor, Dr. Marshall, was sent to a number of employees across the district in another attempt to steal information. Fortunately, the phishing email was detected immediately and the attack successfully contained shortly thereafter with no theft of sensitive data.



FW: REVISED AND UPDATED INFORMATION FOR ALL NORTH ORANGE COUNTY COMMUNITY COLLEGE DISTRICT EMPLOYEE

Nocccd Shared Docu...
255 KB

From: Leach, Heidi (Cancer Ctr) [mailto:LeachHeidi@centracare.com]
Sent: Tuesday, February 13, 2018 8:30 AM
Subject: FW: REVISED AND UPDATED INFORMATION FOR ALL NORTH ORANGE COUNTY COMMUNITY COLLEGE DISTRICT EMPLOYEE

NORTH ORANGE COUNTY
COMMUNITY COLLEGE DISTRICT

FROM THE OFFICE OF THE CHANCELLOR THE NORTH ORANGE COUNTY COMMUNITY COLLEGE DISTRICT

Dear Colleagues

We all share the aim of providing people with innovative solutions that improve their quality of life. We can only succeed in this if we have society's trust. That trust is something we have to earn each and every day. This applies equally to everyone within The North Orange County Community College District – to employees as well as to the Board of Management. What that means for each of us is that our actions must also be based on laws, internal policies, voluntary commitments and ethical principles. Illegal transactions and activities are therefore unacceptable – everywhere in the world and without exception. Our LIFE values also reflect this.

They make it clear that integrity is one of the key elements of our corporate culture and provide the ground rules we must abide by in all we do. The aim of this compliance policy is to help you to follow The North Orange County Community College District principles of business conduct. However, it is not enough to simply take note of them; what matters is that we take these compliance principles to heart and, above all, that we live by them; that applying these principles becomes second nature to us.

This policy also helps us to monitor our own actions and tells us to whom we should turn whenever we are faced with questions regarding compliance. I would particularly like to emphasize that, to me, this is not simply a question of formal compliance with legal requirements, rules and regulations, or avoiding possible penalties. What counts is that each of us is truly convinced of the importance of always acting in accordance with these principles. Let us work together to successfully develop solutions that people trust, because that is precisely what matters.

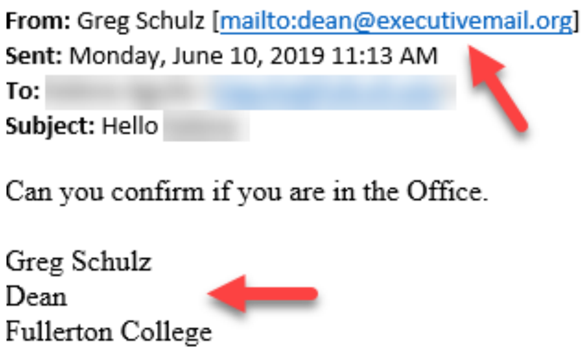
Note: It is important that all employees download the attach document

Cheryl Marshall I Chancellor
NORTH ORANGE COUNTY COMMUNITY COLLEGE DISTRICT
1830 W. Romneya Drive
Anaheim, CA 92801-1819
Phone: (714) 808-4500
nocccd.edu

Confidentiality Notice: This e-mail and any attachment may contain confidential information that is legally privileged. This information is intended only for the use of the individual or entity named above. The authorized recipient of this information is prohibited from disclosing this information to any other party unless required to do so by law or regulation. If you are not the intended recipient, you are hereby notified any disclosure, copying, distribution or action taken in reliance on the contents of these documents is strictly prohibited. If you have received this transmission in error, please notify the sender immediately, reply to this transmission, or contact the CentraCare Health Information Systems Network Security staff by calling the IS Help Desk for assistance at (320) 251-2700 ext. 54540 and delete these documents.

1	Suspicious attachment (generic file name)
2	Email address doesn't match sender (Dr. Marshall at NOCCCD)
3	Terminology in the text is not used within our District
4	Text font suddenly changes
5	Contact information is not correct in some places
6	Legal statement and contact information does not match sender (NOCCCD)

Below are several recent examples of spear phishing, another type of phishing attack targeted at a specific individual, business, or organization. These examples are the ones you will most likely encounter.

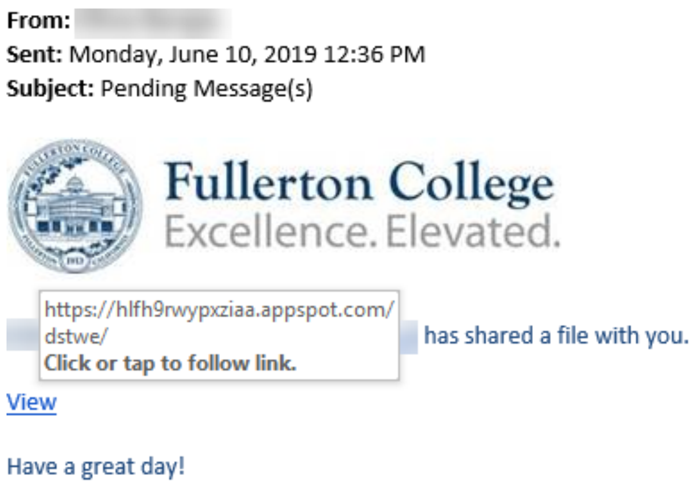


From: Greg Schulz [mailto:dean@executivemail.org]
Sent: Monday, June 10, 2019 11:13 AM
To: [redacted]
Subject: Hello [redacted]

Can you confirm if you are in the Office.

Greg Schulz
Dean
Fullerton College

Email address and listed position (email signature) does not match sender.



From: [redacted]
Sent: Monday, June 10, 2019 12:36 PM
Subject: Pending Message(s)

Fullerton College
Excellence. Elevated.

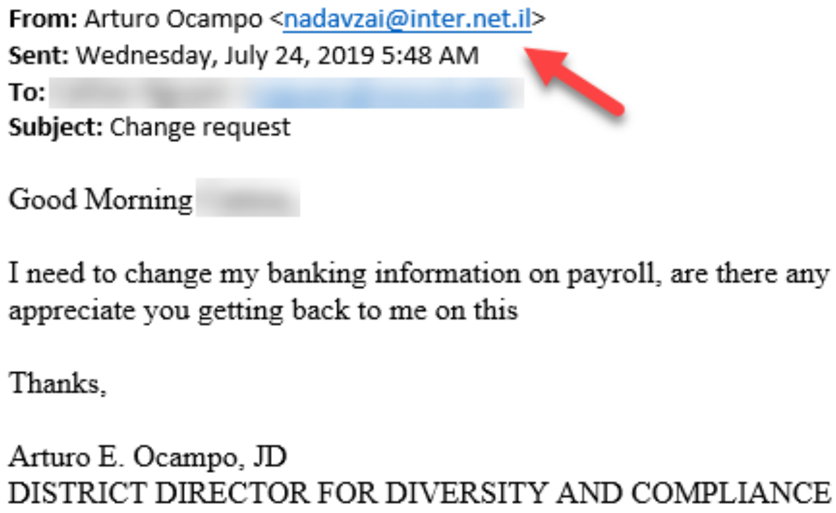
https://hlfh9rwypxziaa.appspot.com/dstwe/
Click or tap to follow link.

[redacted] has shared a file with you.

View

Have a great day!

Pointing at hyperlink reveals a destination address not consistent with Fullerton College.



From: Arturo Ocampo <nadavzai@inter.net.il>
Sent: Wednesday, July 24, 2019 5:48 AM
To: [redacted]
Subject: Change request

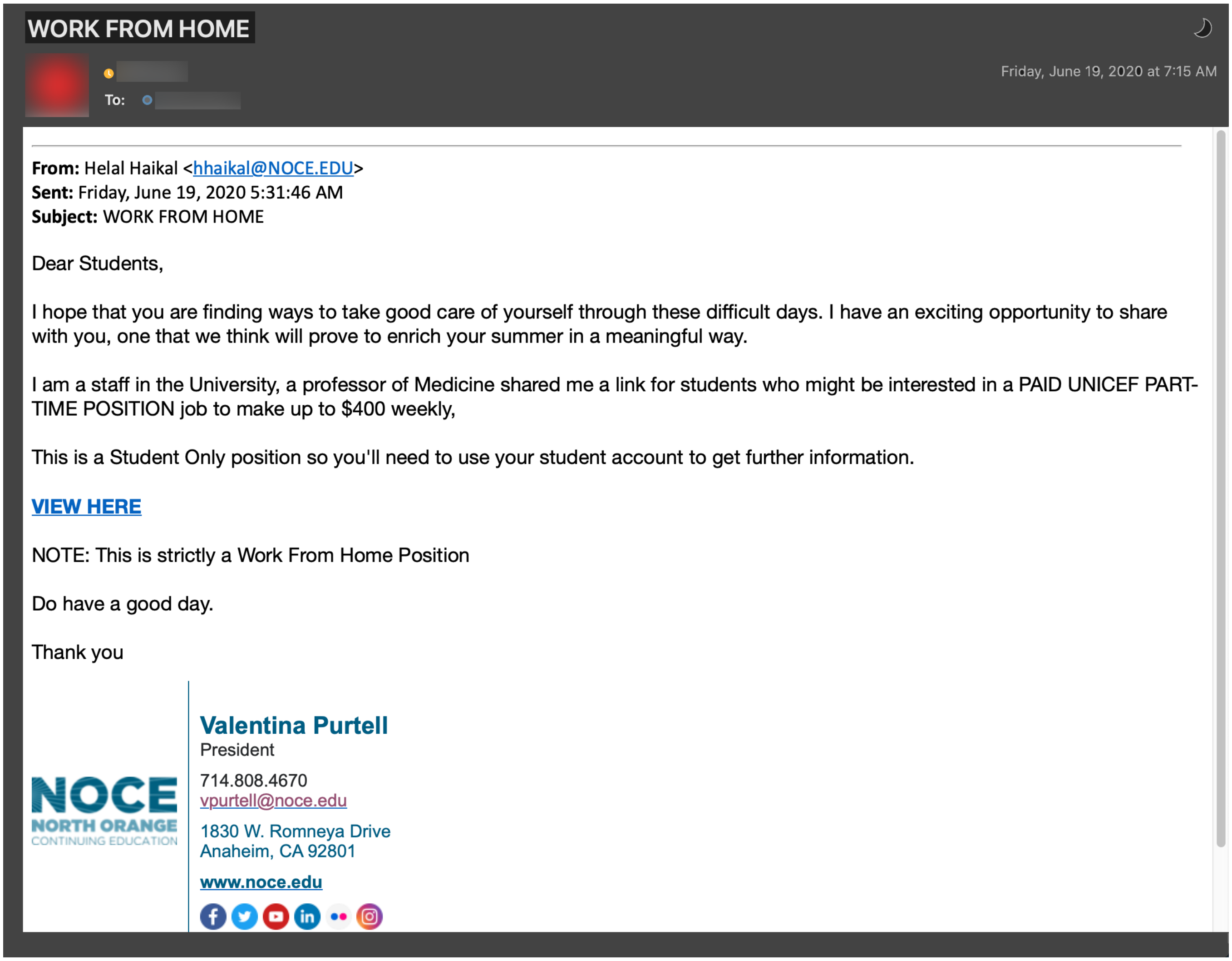
Good Morning [redacted]

I need to change my banking information on payroll, are there any forms I need to fill for this purpose? I will appreciate you getting back to me on this

Thanks,

Arturo E. Ocampo, JD
DISTRICT DIRECTOR FOR DIVERSITY AND COMPLIANCE

Email address does not match sender. Finance-related requests are common in phishing attacks.



WORK FROM HOME

[redacted]

To: [redacted]

Friday, June 19, 2020 at 7:15 AM

From: Helal Haikal <hhaikal@NOCE.EDU>
Sent: Friday, June 19, 2020 5:31:46 AM
Subject: WORK FROM HOME

Dear Students,

I hope that you are finding ways to take good care of yourself through these difficult days. I have an exciting opportunity to share with you, one that we think will prove to enrich your summer in a meaningful way.

I am a staff in the University, a professor of Medicine shared me a link for students who might be interested in a PAID UNICEF PART-TIME POSITION job to make up to $400 weekly,

This is a Student Only position so you'll need to use your student account to get further information.

VIEW HERE

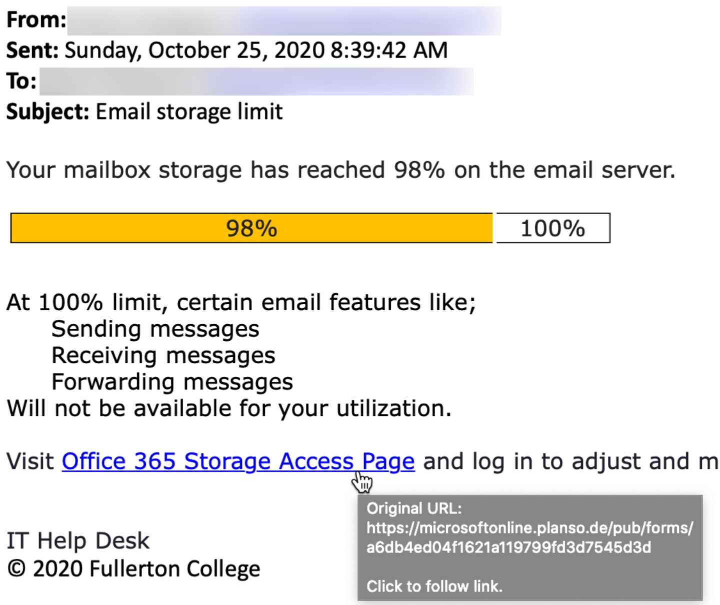
NOTE: This is strictly a Work From Home Position

Do have a good day.

Thank you

NOCE
NORTH ORANGE
CONTINUING EDUCATION

Valentina Purtell
President
714.808.4670
vpurtell@noce.edu
1830 W. Romneya Drive
Anaheim, CA 92801
www.noce.edu



From: [redacted]
Sent: Sunday, October 25, 2020 8:39:42 AM
To: [redacted]
Subject: Email storage limit

Your mailbox storage has reached 98% on the email server.

98% | 100%

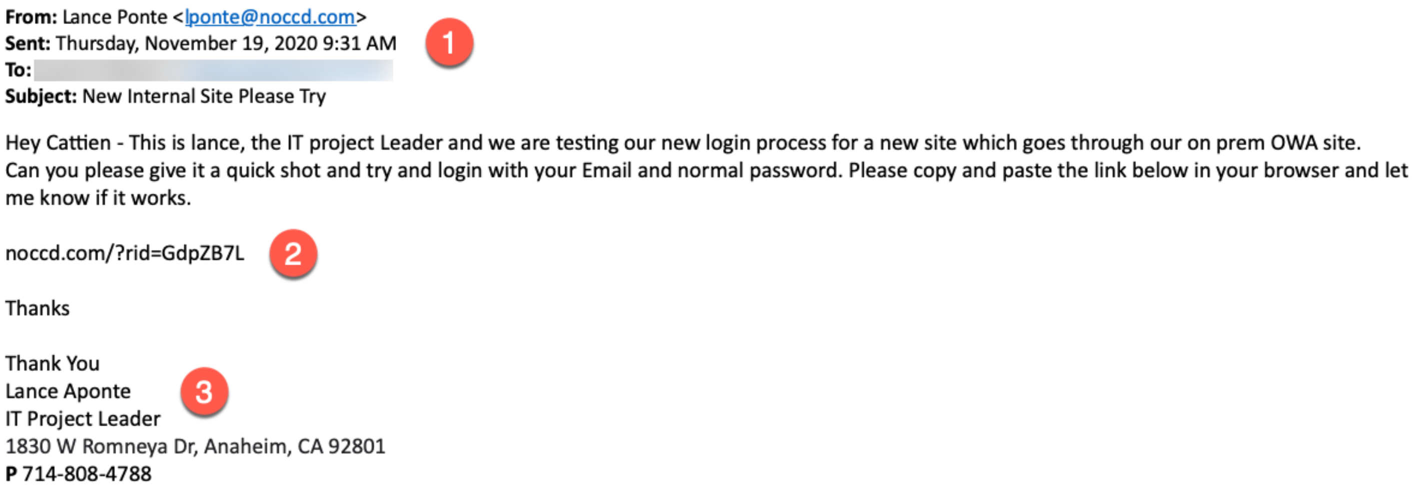
At 100% limit, certain email features like;
Sending messages
Receiving messages
Forwarding messages
Will not be available for your utilization.

Visit Office 365 Storage Access Page and log in to adjust and maintain your Mailbox storage.

Original URL:
https://microsoftonline.planso.de/pub/forms/a6db4ed04f1621a119799fd3d7545d3d

Click to follow link.

IT Help Desk
© 2020 Fullerton College



From: Lance Ponte <lponte@noccd.com>
Sent: Thursday, November 19, 2020 9:31 AM
To: [redacted]
Subject: New Internal Site Please Try

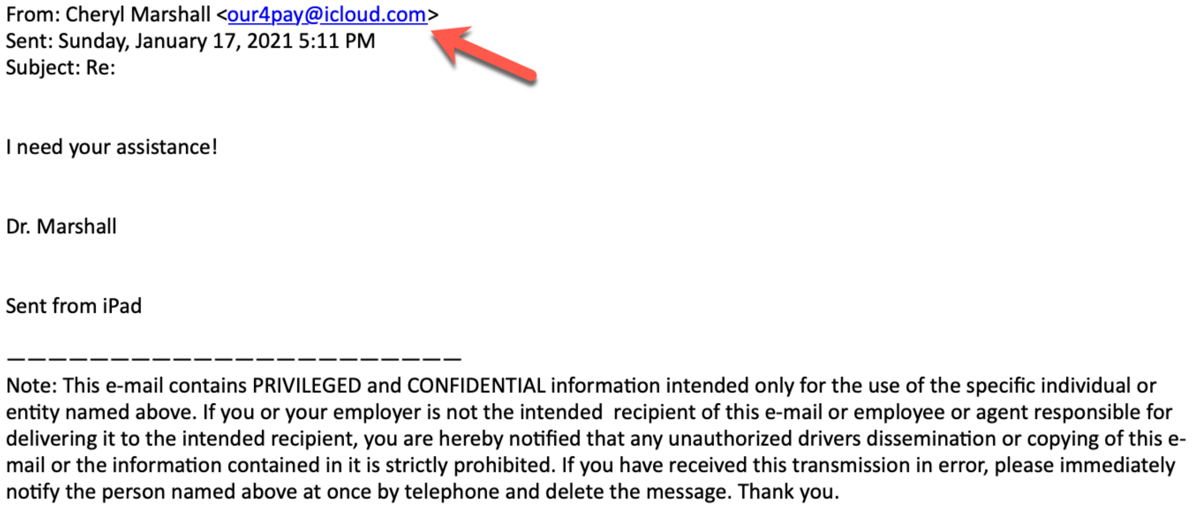
Hey Cattien - This is lance, the IT project Leader and we are testing our new login process for a new site which goes through our on prem OWA site. Can you please give it a quick shot and try and login with your Email and normal password. Please copy and paste the link below in your browser and let me know if it works.

noccd.com/?rid=GdpZB7L

Thanks

Thank You
Lance Aponte
IT Project Leader
1830 W Romneya Dr, Anaheim, CA 92801
P 714-808-4788

Email address doesn't match sender. Look at NOCCCD address for sender and hyperlink. Contact info is inaccurate.



From: Cheryl Marshall <our4pay@icloud.com>
Sent: Sunday, January 17, 2021 5:11 PM
Subject: Re:

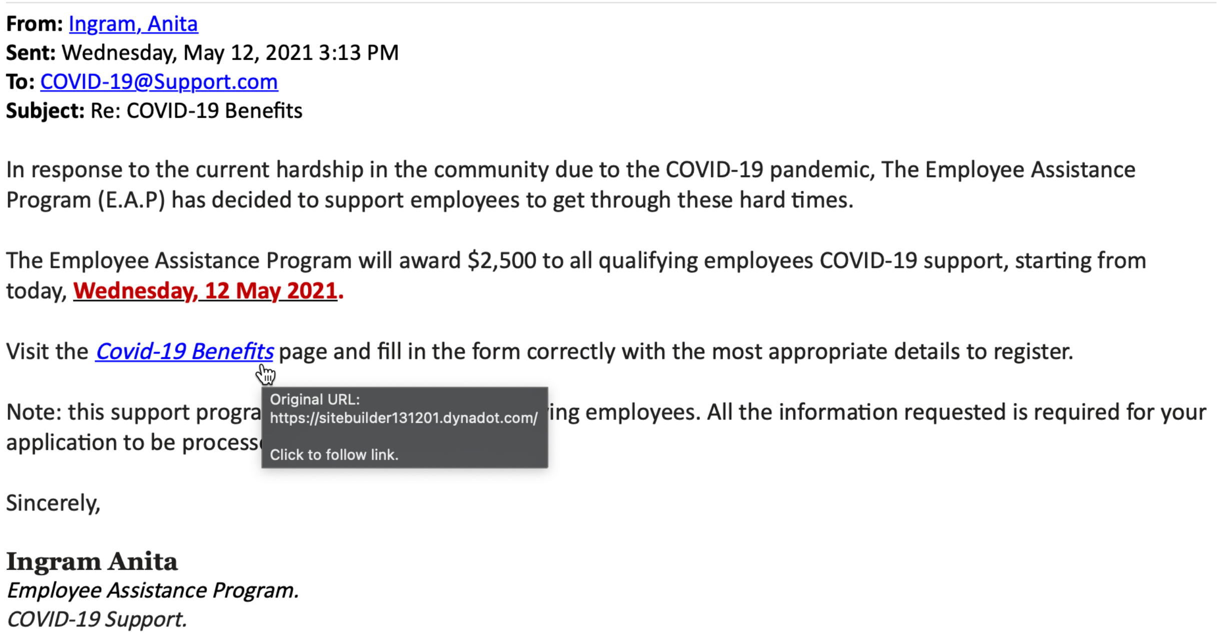
I need your assistance!

Dr. Marshall

Sent from iPad

————————————————————————
Note: This e-mail contains PRIVILEGED and CONFIDENTIAL information intended only for the use of the specific individual or entity named above. If you or your employer is not the intended recipient of this e-mail or employee or agent responsible for delivering it to the intended recipient, you are hereby notified that any unauthorized drivers dissemination or copying of this e-mail or the information contained in it is strictly prohibited. If you have received this transmission in error, please immediately notify the person named above at once by telephone and delete the message. Thank you.

Email address doesn't match sender. Dr. Marshall has a district address.



From: Ingram, Anita
Sent: Wednesday, May 12, 2021 3:13 PM
To: COVID-19@Support.com
Subject: Re: COVID-19 Benefits

In response to the current hardship in the community due to the COVID-19 pandemic, The Employee Assistance Program (E.A.P) has decided to support employees to get through these hard times.

The Employee Assistance Program will award $2,500 to all qualifying employees COVID-19 support, starting from today, **Wednesday, 12 May 2021.**

Visit the *Covid-19 Benefits* page and fill in the form correctly with the most appropriate details to register.

Original URL:
https://sitebuilder131201.dynadot.com/

Click to follow link.

Note: this support progra ing employees. All the information requested is required for your application to be process

Sincerely,

Ingram Anita
Employee Assistance Program.
COVID-19 Support.