NOCCCD
Security Awareness Training

Information Services

Fall 2018

Agenda

- Data Security and PII
- Laws, Policies, Guidelines
- Malware
- Social Engineering
- Mobile Devices
- Home Networks
- Passwords

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

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

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.

Approved Guidelines for Use

- Social Media
- Website
- Cloud Solution Security Measures
- Mobile Computing

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

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?

Threat Vectors

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

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

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

Anatomy of Malware

Malware is built combining two sets of code:

- The Mechanism
- The Payload

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

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

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 cryptocurrency
  - Significant slowing and/or overheating can occur
- Backdoor
  - Creates opening for remote access
  - Gains control of computer for unauthorized actions
- Spyware
  - Tracks your computer/Internet activity
  - Reports activity to creator

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

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
- Phishing Attacks
  - Know the classic signs (Review Handout)
  - Look before you click on links
  - Never provide personal or login information

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

Recent Phishing Example

Reply Reply All Forward IM

Tue 2/13/2018 8:30 AM

Leach, Heidi (Cancer Ctr) <LeachHeidi@centracare.com>

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

Nocccd Shared Document.pdf
255 KB

NORTH ORANGE COUNTY
COMMUNITY COLLEGE DISTRICT

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

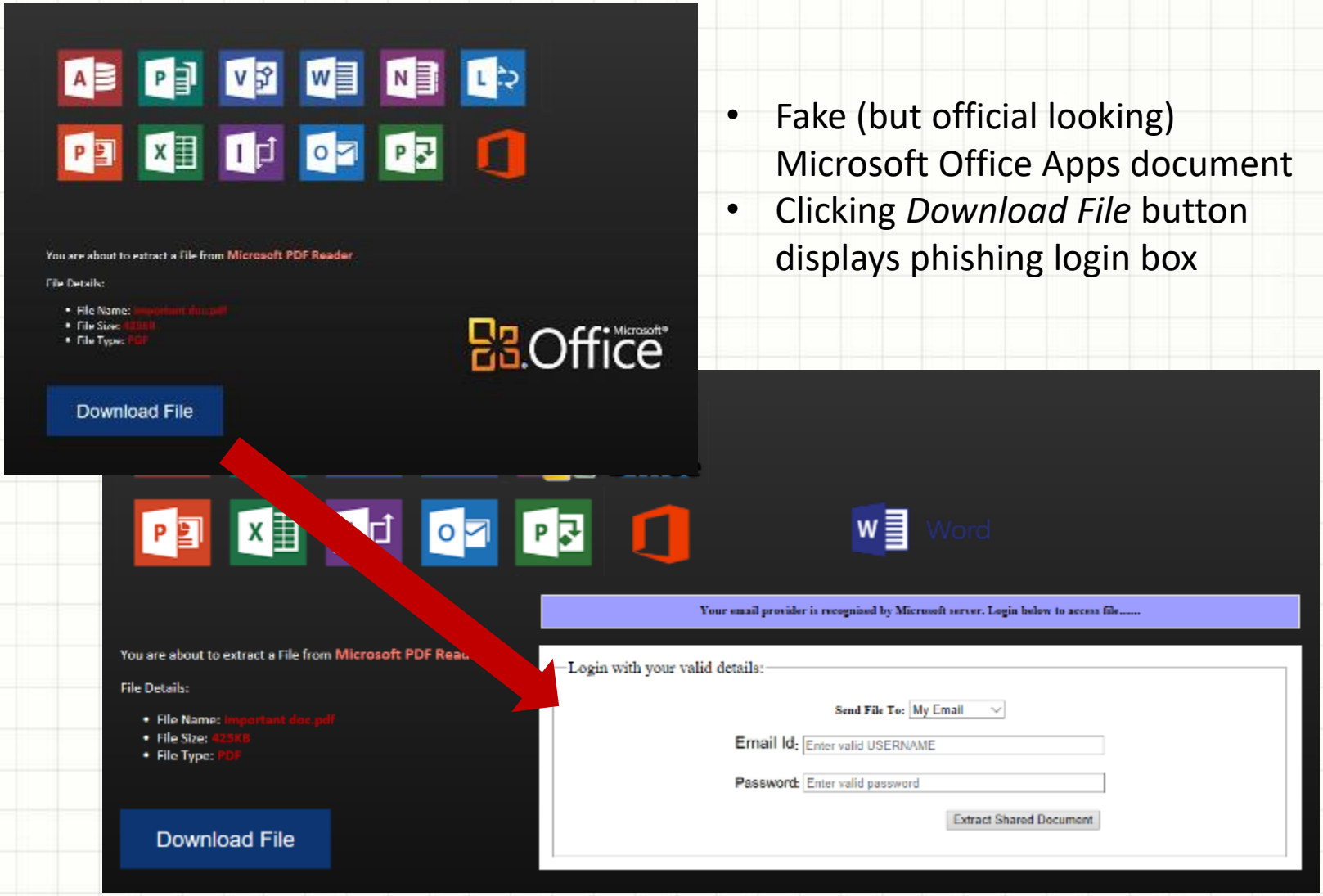
Dear Colleagues

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

- Allegedly from Chancellor Marshall. Sender email address doesn't match.
- Suspicious attachment that message insists on opening
- Oddly worded message when compared to other genuine communication

Phishing Example Attachment



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

Social Media

- Separate work and personal lives
  - Think about what you post. Privacy at risk.
  - Nothing truly deleted (backups and screenshots)
- Review security settings
  - Privacy
  - Audience (approved viewers)
- Be cautious when clicking on article links
  - Preys on emotion with “hot button” topics
  - Often leads to hacked websites or phishing

Mobile Devices

- Applies to smartphones, tablets, laptops
- No technical support
- Network use
  - Secured vs Unsecured Wireless
  - Work-related activity
- Threat vectors
  - Communication (email, phishing, social media)
  - Poorly written or compromised app
- Responsible for any stored work-related data
- Delete all work-related items when separating from your position within the District

Home Networking

- Connected Devices
  - Desktop Computers
  - Mobile (phone, tablet, laptop)
  - Internet of Things (IoT) Devices
- Cybersecurity Issues
  - Router Setup (admin account, SSID, etc)
  - Privacy Concerns (phone home)
  - Security Updates
  - Separate Networks (Primary, Guest, etc)
- Strong Passwords (router and all devices)

Passwords

- First and last line of defense to your data
- How passwords can be cracked or obtained
  - Phishing attacks
  - Spyware (keyloggers)
  - Guessed using personal information
  - Written down and stored in physical location
  - Commonly used or weak password
- Weak vs Strong Passwords

Weak Passwords

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

Top 25 Worst Passwords of 2017

1. 123456
2. password
3. 12345678
4. qwerty
5. 12345
6. 123456789
7. letmein
8. 1234567
9. football
10. Iloveyou
11. admin
12. welcome
13. monkey
14. login
15. abc123
16. starwars
17. 123123
18. dragon
19. passw0rd
20. master
21. hello
22. freedom
23. whatever
24. qazwsx
25. trustno1

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
  - Words in any language, slang, dialect, jargon
  - Proper names (person, place, organization)
  - Not based on personal information
  - Word or number patterns

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

Password Protection Standards

- ✓ Do not hint at the format of passwords
- ✓ 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

Data Security Is Your Responsibility

- Stay updated on new or existing security threats via our blog (CaTT Tales)
- Practice safe computing habits online
- Be concerned about privacy
- Be aware of issues when mixing work with personal on your PC or other devices
- Create strong passwords for every system
- See something, say something!

Questions?

Contact Information

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

Newsletter (CaTT Tales)
https://bookit.nocccd.edu/concrete5/

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

Email Address
ishelpdesk@nocccd.edu

Phone Number
(714) 808-4849