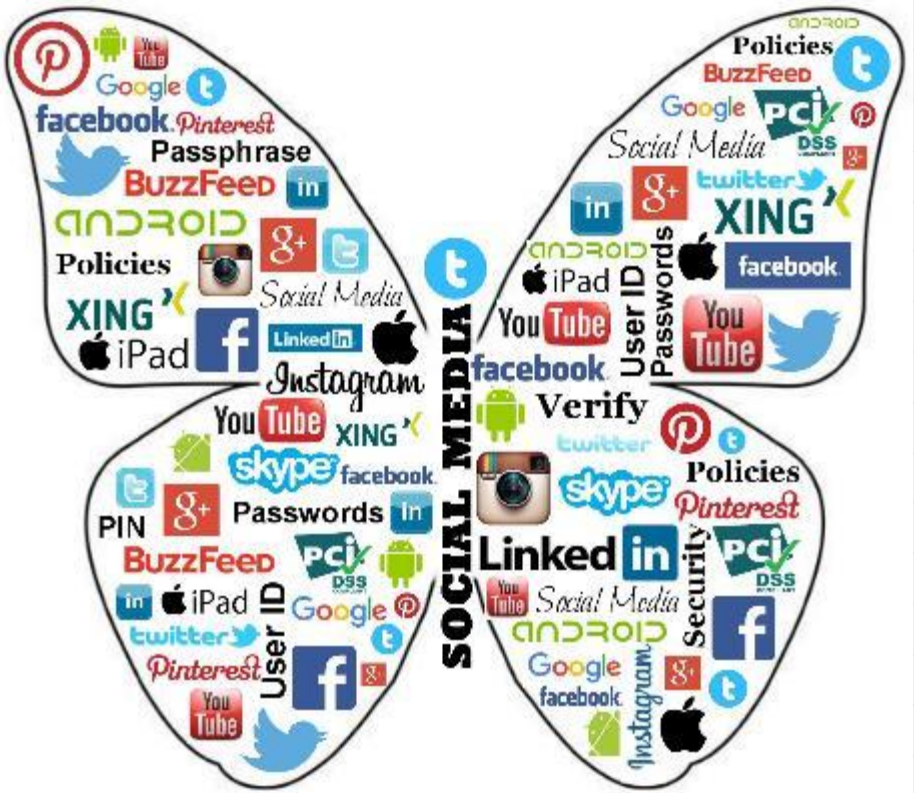
Playing it Safe in the Social Media World: What Staff Should Know



June20, 2016

Agenda

- Why do we care about data security?
  - State and Federal laws
  - Local policies and Guidelines
- Why concern about Cloud Services?– Google Drive, Drop Box, etc.
- What risks are there with Social Media?
- What E-mail risks are there?
- What should I know about Websites & ADA/Section 504?
- How do I handle Mobile Devices – District Owned Devices & “Bring Your Own Device”?
- What are my rights regarding Copyright and reposting of digital items?
- A few other reminders…….
- Questions?

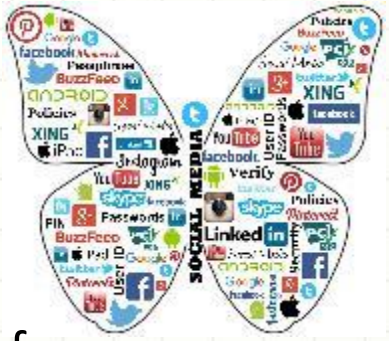
Why do we care about Data Security?

- According to Osterman Research, Inc. the **typical** information worker **spends 153 minutes per day working in email and 51 minutes in social media – 42.5 percent of a typical eight - hour day** – not to mention the various work - related and personal use of the web that takes place on a daily basis.
- Consequently, security for all of these tools must be of paramount concern for decision makers because of the substantial opportunity that they represent for ingress of malware and other threats. For example, our research found that during just the last 12 months:
  - **74** percent of organizations have been infiltrated with malware through **Websurfing**
  - **64** percent have experienced malware infiltration through **email**.
  - **22** percent have experienced an accidental or malicious leak of sensitive or **confidential data through email**
  - **14** percent of organizations have had malware enter the corporate network through **social media or other Web 2.0 apps**
- http://www2.trustwave.com/rs/trustwave/images/Best_Practices_in_Email_Web_and_Social_Media_Security_Trustwave.pdf

Federal and State Laws

- **FERPA** -The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99) is a Federal law that protects the privacy of student education records.
  - http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html
- **HIPAA** - Privacy Rule which creates national standards to protect individuals' medical records and other personal health information.
  - http://www.hhs.gov/hipaa
- **California Breach Notification** - Protects Personally Identifiable Information.
  - http://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=CIV&sectionNum=1798.29
  - http://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=CIV&sectionNum=1798.82
- **Privacy**, etc…….it is also just the right thing to do!

Local Policies & Guidelines



- Be familiar with the district and know what is expected of you
- Board Policies and Procedures:
  - http://www.nocccd.edu/files/3720apfinalreviseddcc2015-11-23_24854.pdf
  - http://www.nocccd.edu/files/3740apfinal_032904_24987.pdf
  - http://www.nocccd.edu/files/3750ap_072505_25047.pdf
- Social Media Guidelines
  - http://www.nocccd.edu.php54-2.dfw1-1.websitetestlink.com/files/social-media-guidelines-01-25-16-dcc-approved_13356.pdf
- Website Guidelines:
  - http://www.nocccd.edu.php54-2.dfw1-1.websitetestlink.com/files/website-guidelines-dcc-approved-1-26-15_13395.pdf
- Cloud Solution Security Measure Guidelines:
  - http://www.nocccd.edu.php54-2.dfw1-1.websitetestlink.com/files/cloud-solution-security-measure-guidelines-dcc-approved-1-26-15_12243.pdf
- Mobile Computing Guidelines:
  - http://www.nocccd.edu.php54-2.dfw1-1.websitetestlink.com/files/mobile-computing-guidelines-dcc-approved-8-24-15_13319.pdf

Cloud Services

- Most new development of systems is offered in the cloud as the only option – Why?
- Once something is in the cloud even if you delete, it is not gone!
- Only protection is the contract / End User Licensing Agreement – Read it!
- Refer to Cloud Solution Security Measure Guidelines at: http://www.nocccd.edu.php54-2.dfw1-1.websitetestlink.com/files/cloud-solution-security-measure-guidelines-dcc-approved-1-26-15_12243.pdf
- User authentication
  - Identify data being used and validate it if needed
  - Review vendor security processes & procedures

Google

Dropbox

Social Media

- Most used Social Media sites:
  - You Tube
  - Facebook
  - Snapchat
  - Instagram
  - Twitter
  - Google+
  - Pinterest
  - YouVine
  - Tumblr
  - iFunny
  - Reddit

- Source: Ruffalo Noel Levitz, “2015 E-Expectations Report,” July 2015

Social Media

Top 7 Social Media Security Practices: https://www.solutionary.com/resource-center/blog/2015/01/top-7-social-media-security-practices/

- Separate Work from Personal – e-Discovery; Free Speech; Privacy
- Understand how security settings work
- Understand how to restrict your posts to the audience you want
- Remember just because you delete something does not mean it is gone – everything is stored on a backup server somewhere
- Remember this is a cloud based service in most cases, treat it as such
- If you don't want it seen on the front page of the paper or in a Tweet don't write it!
- Refer to the Social Media Guidelines: http://www.nocccd.edu.php54-2.dfw1-1.websitetestlink.com/files/social-media-guidelines-01-25-16-dcc-approved_13356.pdf

- Social Media - https://www.youtube.com/watch?v=YLWmjpPoJHk

Email

- What is phishing? Does anyone know enough about you to pose as you? https://www.lookout.com/resources/know-your-mobile/what-is-phishing
- Don't open ANY attachments that end in .exe or .scr AND unless you know the person and you were expecting them to send something. Call them and see if they sent you something.
- Never send passwords, credit card, SSN etc.
- Don’t send anything you don’t want to see in the newspaper or on Twitter!

Videos:

- Phishing - https://www.youtube.com/watch?v=wZwxxdXmazs
- Sloppy Email Scanner - https://www.youtube.com/watch?v=rdsqOgqjCgU&li[illegible]9125B50EF9C4&index=1

Website

- Anything on a public site is available to the world!
- Remember, you are representing the District if you use one for District business
- Follow Website Board Policy: http://www.nocccd.edu/files/3740bpfinal_032904_24978.pdf
- Website Guidelines offer additional suggestions: http://www.nocccd.edu.php54-2.dfw1-1.websitetestlink.com/files/website-guidelines-dcc-approved-1-26-15_13395.pdf
- Consider ADA/Section 508 requirements!

Mobile Devices

- District Owned Devices governed by BP/AP 3720
- BYOD (Bring Your Own Device)
  - Use is optional and District not responsible
  - No technical support
  - Wired or wireless network use is governed by each campus
  - myGateway not mobile responsive at this time
  - Don't expect privacy
  - BP 5500 will apply to your students' usage
  - Put in your syllabus the expectations for these devices; you cannot require them of students
  - Wipe the device of college business upon separation
  - Don't share personal information
  - Contract provisions will apply
- Use of personal device may become public if used for business!
- Refer to Mobile Computing Device Guidelines: http://www.nocccd.edu.php54-2.dfw1-1.websitetestlink.com/files/mobile-computing-guidelines-dcc-approved-8-24-15_13319.pdf

Copyright

- District copyright governed by BP/AP 3750:
  - http://www.nocccd.edu/files/3750ap_072505_25047.pdf
- Another good source of information:
  - http://www.nocccd.edu.php54-2.dfw1-1.websitetestlink.com/files/knowyourcopyrights_85467.pdf
  - Link when possible – check online
  - Check the library
  - Fair Use – understand if it is covered
- A few words on using images……

A Few Other Reminders!

- **Passwords** – don't share as it violates Board Policy; use a phrase; never use personal information
- **Computers** – log off when you leave your work location

Passwords

- **The Simplest Security: A Guide To Better Password Practices** http://www.symantec.com/connect/articles/simplest-security-guide-better-password-practices
- While we may find them annoying, and even take them for granted, it is important to remember why passwords are important: **passwords are often the first (and possibly only) defense against intrusion** (MacGregor). They protect personal information – information we don't want anyone and everyone to know. In our personal lives, this means financial information, health data, and private documents. In a professional context, this may encompass anything considered crucial to the success of the organization: trade secrets, financial data, intellectual property, customer lists, etc.
  - **Passwords can be cracked** in a variety of different ways. The **most simple is the use of a word list or dictionary program** to break the password by brute force.
  - Another easy way for potential intruders to nab passwords is through social engineering: **physically** nabbing the password off a **Post-It from under someone's keyboard** or through imitating an IT engineer and **asking over the phone**.
  - Many users create passwords that can be guessed by learning a minimal amount of information about the person whose password is being sought.
  - A more technical way of learning passwords is through **sniffers**, which look at the raw data transmitted across the net and decipher its contents. "A **sniffer can read every keystroke** sent out from your machine, including passwords"

Passwords

- **CHOOSING GOOD PASSWORDS – WHAT *NOT* TO DO**
  - **What NOT to use:** no words, proper nouns, or foreign words, avoid words with a number tacked on at the end. No personal information (names, pets, addresses, phone numbers, etc)

- **A STRONG PASSWORD REQUIRES:**
  - **A strong, effective password** requires a necessary degree of complexity. Three factors can help users to develop this complexity: length, width & depth.
    - **Length:** It is generally recommended that passwords be between six and nine characters. Longer passwords are harder to crack. Simply put, longer is better.
    - **Width:** Width is a way of describing the different types of characters that are used. (uppercase, lowercase, numbers, special characters, etc)
    - **Depth:** Depth refers to choosing a password with a challenging meaning – something not easily guessable.

Passwords

- **CHOOSING GOOD PASSWORDS – WHAT *TO* DO:**
  - Stop thinking in terms of pass*words* and start thinking in terms of *phrases*. "**A good password is easy to remember, but hard to guess.**" (Armstrong) The purpose of a mnemonic phrase is to allow the creation of a complex password that will not need to be written down. What may be most effective is for users to choose a phrase that is has personal meaning (for easy recollection), to take the initials of each of the words in that phrase, and to convert some of those letters into other characters (substituting the number '3' for the letter 'e' is a common example).
    - Example: the phrase "**A good password is easy to remember"** can translate to: **Agp1e2r**
    - Example**: "Our family loves to go to Hawaii**" can translate to: **ofL2g2h**, or **0Fltg2H**
  - **Avoid using the same password on multiple accounts**. Doing this creates a single point of failure, which means that if an intruder gains access to one account, he or she will have access to all of the user's accounts.
  - Users should **never disclose** their passwords to anybody unless they know them to be authorized (i.e., systems administrators). Even then, passwords should only be disclosed in person (not over the phone or by e-mail) to a known, trusted source.
  - If possible, do not write your passwords down.
- In order to ensure their ongoing effectiveness, passwords should be **changed on a regular basis**. How often one should change passwords really depends on the account. Online financial accounts should be changed every month or two. Corporate network passwords should be changed every 3-4 months.

Worst Passwords of 2015

- 123456
- password
- 12345678)
- qwerty
- 12345
- 123456789
- football
- 1234
- 1234567
- baseball
- welcome
- 1234567890
- abc123
- 111111
- 1qaz2wsx
- dragon
- master
- monkey
- letmein
- login
- princess
- qwertyuiop
- solo
- passw0rd
- starwars

Jimmy Kimmel - https://www.youtube.com/watch?v=opRMrEfAIiI
Password Minder - https://www.youtube.com/watch?v=_u8Rss3W4Wg

Resources

- California Community College Legal: http://extranet.cccco.edu/Divisions/Legal.aspx
- Chancellor's Office Legal Advice Guidelines: http://extranet.cccco.edu/Portals/1/Legal/Guidelines/Legal_advice.pdf
- ADA/Section 508 – Chancellor's Office: http://extranet.cccco.edu/Divisions/StudentServices/DSPS/StatutesRegulations.aspx

- Skimmer - https://www.youtube.com/watch?v=ll4f0Wim4pM

Questions?

Contact information:

Deborah Ludford
dludford@nocccd.edu
(714)808-4866

Nicholas Wilkening
nwilkening@nocccd.edu
(714)808-4875

Thank You!