



# INFORMATION SERVICES

Presented by Deborah Ludford, District Director, Information Services

[dludford@nocccd.edu](mailto:dludford@nocccd.edu)

714-808-4866

<http://www.nocccd.edu/information-services>

# 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, it's not gone!
- Only protection is the contract / End User Licensing Agreement – Read it!
- Refer to Cloud Solution Security Measure Guidelines on our website at:  
[http://www.nocccd.edu/Departments/IS/documents/Cloud\\_Solution\\_Security\\_Measure\\_Guidelines.pdf](http://www.nocccd.edu/Departments/IS/documents/Cloud_Solution_Security_Measure_Guidelines.pdf)





# SOCIAL MEDIA



- 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/Departments/IS/documents/Social\\_Media\\_Guidelines.pdf](http://www.nocccd.edu/Departments/IS/documents/Social_Media_Guidelines.pdf)
- **Social engineering** refers to psychological manipulation of people into performing actions or divulging confidential information. A type of confidence trick for the purpose of information gathering, fraud, or system access.
- <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!



# 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/Departments/IS/documents/Mobile\\_Computing\\_Guidelines.pdf](http://www.nocccd.edu/Departments/IS/documents/Mobile_Computing_Guidelines.pdf)

# A FEW OTHER REMINDERS!

- Passwords – don't share; use a phrase; never use personal information
- <https://www.youtube.com/watch?v=opRMrEfAlil>
- Computers – log off when you leave your work location
- And the newest threat is Ransomware!
- *Ransomware* is a type of malware that severely restricts access to a computer, device or file until a ransom is paid by the user.



# QUESTIONS?

Contact information:

Deborah Ludford

[dludford@nocccd.edu](mailto:dludford@nocccd.edu)

(714)808-4866

Nicholas Wilkening

[nwilkening@nocccd.edu](mailto:nwilkening@nocccd.edu)

(714)808-4875

Thank You!