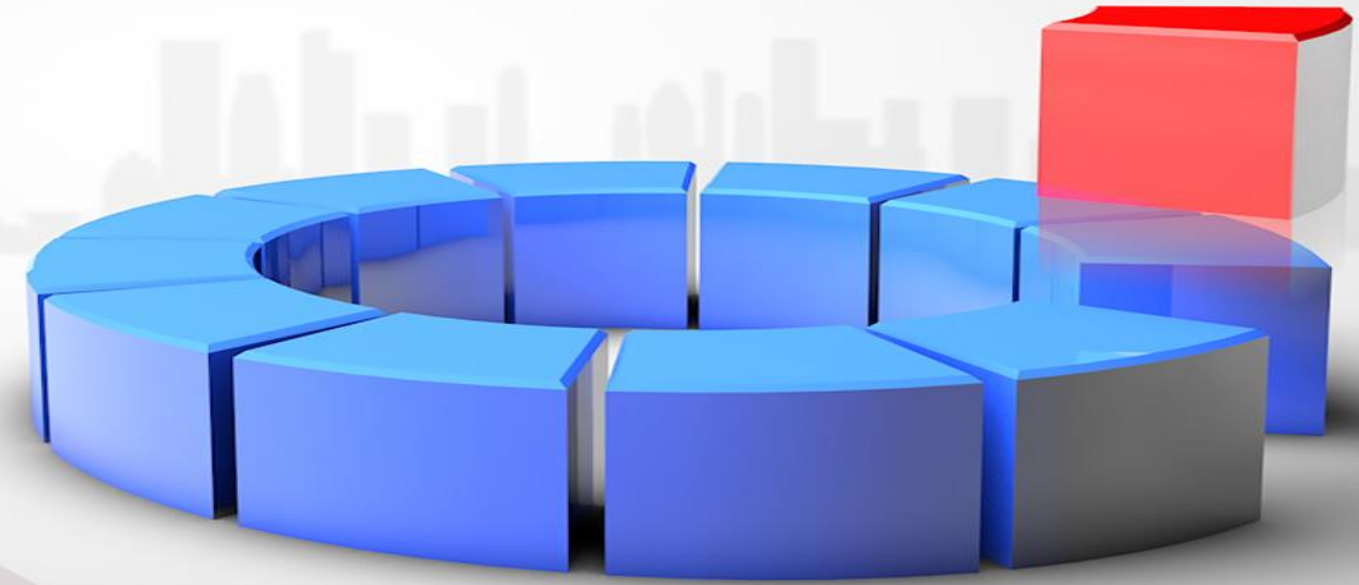
2017 DDI User Group

Building Community Together…

Information Security 101



Information Security 101

Why you should care about information security?

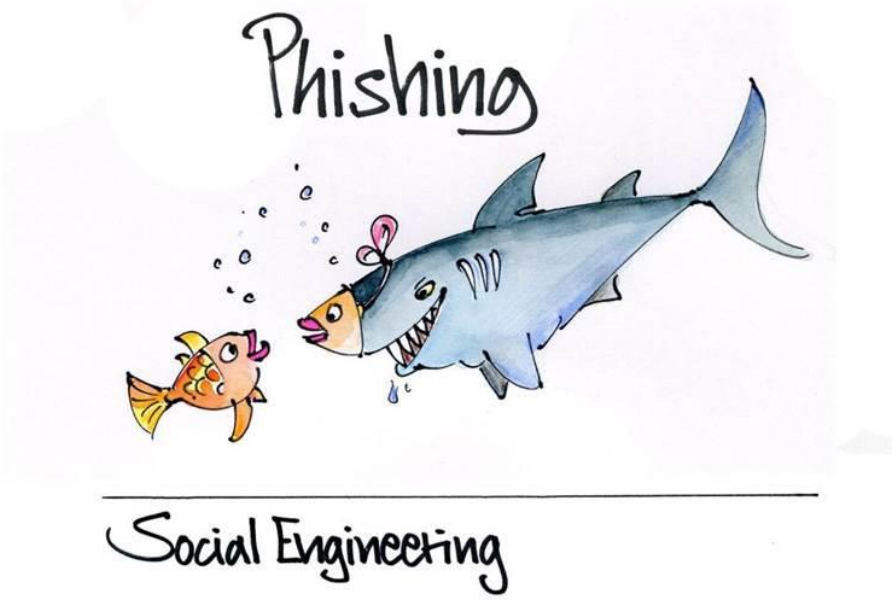
- You are always at risk if you are connected to the internet!
- Your organization is at risk!
- Data can be stolen or destroyed!
- Your organization could face legal consequences!
- Your identity could be stolen!

Harmful things we don’t understand

Common Security Risks

Email is the number 1 attack vector

- Phishing and Social Engineering
- Spam
- Malicious links and attachments
  - Ransomware
  - Remote Control
  - Key Logging
  - Viruses



Common Security Risks

- Denial of Service (DoS), Distributed Denial of Service (DDoS)
- Rogue security software
- Internet fraud
- Data loss or theft
- Drive by download/infected site

Common Security Risks

Example of fake pop-up

What can you do?

As an organization

- Regular security training
- Document procedures intended to mitigate these risks
- Identify compliance requirements- can include HIPPA, Sarbanes-Oxley, or other federal regulations
- Conduct social engineering tests
- Hire an information security firm to conduct a vulnerability analysis

What can you do?

DDI Security policy

It is DDI's policy to proactively safeguard all aspects of our technical infrastructure, systems and services from unauthorized access, alteration or destruction

- Protects *your* data from unauthorized access
- Ensure DDI's systems are always secure
- Ensure DDI's security meets external control audit requirements
- Ensure physical security at DDI data centers

What can you do?

Use encrypted email where appropriate

DDI uses Barracuda email encryption and provides this service for free to hosted email clients

- Protecting financial information
- Compliance with legal requirements
- Provide secure method for sending and receiving
- Easy to use

What can you do?

As an individual

- Keep abreast of the cyber security trends
  - US-Cert
  - reddit security news channel
- Keep all your software updated/patched
- Always use anti-virus/anti-malware software

- Simple precautions such as changing passwords regularly, password complexity
- Use password manager software such as lastpass or passwordsafe
- ***Pay attention***

US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Password Recommendations

Use a password manager

- Remember only one password
- Cross device support – Android, PC, iPhone/Mac/iPad
- Can create very strong passwords, unique for every site
- Can automatically enter username and password

Password Recommendations

Password common sense

- Don’t share your password with anyone
- Use complex passwords- combination of upper and lower case letters, numbers, and special characters, at least 8 characters long
  - https://howsecureismypassword.net/
  - Many experts recommend using a “passphrase”
- Don’t use dictionary words, or easily guessed words
- Don’t share other personal information
  - Mother’s maiden name
  - Dog’s name

References

- Cisco- http://blogs.cisco.com/smallbusiness/the-10-most-common-security-threats-explained
- Symantec- https://www.symantec.com/connect/nl/blogs/business-email-compromise-campaigns-continue-targeting-c-level-employees-despite-warnings
- Fake Pop-ups- https://blog.malwarebytes.com/threat-analysis/2014/11/psa-tech-support-scams-pop-ups-on-the-rise
- https://lastpass.com
- http://keepass.info/
- https://www.reddit.com/r/InfoSecNews/
- https://www.us-cert.gov/

Webinars and Touchbases

Webinars:

- Monthly hour long sessions
- Open Q&A time at the end of the session
- Link to the webinar for future viewing
- PDF setup and checklist guide
- Cost per organization: $75/month

Touchbases:

- Free hour long sessions
- Monthly, Bi-Monthly, or Quarterly
- Discuss open or new requests, software needs, etc.
- Use allotted time for training on DDI-Connect™

LET'S WORK TOGETHER

Discussion, Questions, Comments

Chad Welsh
cwelsh@ddi.org
support@ddi.org
317.713.2480

Security Reminder