POWERED BY

California Community Colleges

Information Communication Technologies (ICT)
& Digital Media Sector Team

www.ictdmsector.org

COMMUNITY COLLEGES
SAN DIEGO & IMPERIAL COUNTIES
CAREER EDUCATION

Careered.org

Cybersecurity Basics

By Duane Rinehart, MBA
Regional Director, Employer Engagement

29 OCT 2019

Regional Directory of Employer Engagement

- California Community Colleges:
  - ICT Regional Director in San Diego / Imperial Counties
  - Professor in San Diego Continuing Education
- Corporate:
  - Scripps Research : Research Programmer in Metabolomics and Mass Spectrometry
  - Senior Marketing Consultant to Qualcomm, Microsoft, Cisco, Karl Strauss, ViaSat, Welk Resorts
- Academic:
  - MBA – The Ohio State University
  - Master in Information Systems Management – Keller, (DeVry University)
  - BA in French, The Ohio State University
  - BA in International Studies, The Ohio State University

Duane Rinehart

Anti-Virus Protection

- Many rogue applications infect workstations, servers and mobile devices every year. The majority can be easily prevented with stock anti-virus software. The key is to update the virus definitions on a regular basis.
- Windows 10 has anti-virus protection built-in
- Apple and Linux do not have built-in apps but they are easily installable (search for “antivirus for Mac” on major search engine)
- Many but not all consumer mobile devices (e.g. smart phones) come with built-in anti-virus software provided by vendor.
- Wireless devices (e.g. Chromebooks) generally do not have anti-virus software unless user installed it from the app store.
- Problems arise when employees connect non-company devices at work.

Malware Protection

- Similar to viruses, malware may enter the network from any point and travel to any connected device. Malware is any malicious application that interrupts business processes on a computer. It is critical to do regular scans on all devices to ensure each device is clean.
- Windows 10 has built-in anti-malware protection (see Virus & Threat Protection in Settings menu)
- Apple and Linux do not have built-in apps but may be downloaded and installed
- Mobile and wireless devices generally do not have anti-malware protection however it may be available in the respective app stores

Secure Passwords

- Users must have authorization to use company resources and historically passwords have been employed. As passwords proliferate however, many users have difficulty remembering their passwords and make “cheat sheets” for organization (i.e., Post-it notes under keyboard or text file with all the passwords). Some recycle the same password for all systems.
- For systems that still use passwords, require long, non-dictionary word passwords with special characters (e.g. #$%)
- To remember passwords [entered in a browser], consider a password manager app. User will need only 1 password to unlock but each service will have a secure password.

Multi-Factor Authentication

- As passwords alone can be problematic, consider augmenting security on IT systems with other factors. Many user devices already have built-in capabilities such as a fingerprint reader. When combined (password + other factor), security is enhanced.
- “Factors” may include:
  - Something you are: fingerprint, retina scanner, voice recognition
  - Something you have: keycard, USB dongle, mobile device
  - Something you know: password, security questions

Spam & Phishing

- E-mail [and to a certain extent collaboration software like Slack] are used extensively for communication within and between companies. Hackers know this and try to exploit users through fake e-mail and malicious links. You may not easily stop users from clicking on links so pre-filtering messages so they never hit users' inboxes may be next best thing.
- It is best to enable e-mail filtering on hosting provider (e.g. Office 365) and check "Spam" or "Junk Mail" periodically to ensure real messages are not included.
- Even if your IT staff has the expertise to setup a mail server in-house the filtering can be very time consuming – not recommended for smaller companies.

Document Security Policies and Procedures

- Users (not technology) are frequently the target of hackers as they can be fooled. This technique is termed “social engineering” and **cannot** be overcome through technology. The best way to minimize this risk is to document security policies and procedures; and educate users regularly.
- Subscription services for cybersecurity awareness (e-newsletters) can provide content and third parties can provide Internet-based or on-site training

Backup & Test

- All data in the organization should be backed up to an off-site location as part of a disaster recovery plan. IT staff should do mock restores at least annually to ensure systems are storing correct data and it can be recovered in a timely manner without compromising security.
- Backup procedures should be incorporated into business continuity plan (templates available online)