Monthly ECC Information Security Briefing
June 26, 2018

ECC Internal News

The Cybersecurity Office has submitted new/revised Board Policies & Administrative Procedures for approval:

- The existing policies had not been updated for many years, and there was a distinct need for additional policies to cover all the modern aspects of our current computing environment (such as social media), as well as Disaster Recovery operations.
- The updated policies bring us closer in line with the current standards set forth by the Chancellor’s Office:
  - BP-3720.1 (Student Computing Access) - revised
  - BP-6160 (Computer and Network Use) - revised
  - AP-6160 (Computer and Network Use) - revised
  - AP-6162 (Change Control) - new
  - AP-6164 (Data Classification) - new
  - AP-6166 (Disaster Recovery) - new
  - AP-6168 (Logging Monitoring) - new
  - AP-6170 (Network Security) - new
  - AP-6172 (Physical Security) - new
  - AP-6174 (Remote Access) - new
  - AP-6176 (Security Incident Response) - new
  - AP-6178 (Secure Operations) - new
  - AP-6180 (Social Media) - new
- You can find all of ECC’s Board Policies and Administrative Procedures at:
  - http://www.elcamino.edu/administration/board/policies.aspx
External News

MyHeritage suffers data breach - account details of 92+ million users compromised
- Link to full article: https://www.helpnetsecurity.com/2018/06/06/myheritage-data-breach/

Facebook confirms sharing user data with Chinese electronics companies

Data Breach Watch

U.S. Higher Education Breaches for May 2018:
- University at Buffalo, NY
- Northwest University, WA
- Global University, MO
- University of Toledo, OH
- University of Vermont, VT
Tip of the Month

Tech Support Scams – Beware!

A - You get an urgent call or email from a tech support company, saying your computer has a problem. Should you give the company remote access to your computer to make repairs?

B - A warning announcing “suspicious activity” or “security threat detected” appears on your computer screen. Should you call the number shown on the screen to talk to a technician?

C - One of these tech support companies asks you to pay for its services, maybe by using a gift card (like from iTunes or Amazon) or wire transfer. Should you?

The answer to all of these questions is: **No!**

Your computer is almost certainly fine. Legitimate tech support companies don’t operate this way. Tech support scammers make false claims that they are associated with legitimate
computer companies to make you believe them. The person who calls or who gives you a toll-
free number to call is a scammer who wants to steal your money.

If you give someone control of your computer they can install malicious software that helps
them steal your personal information.

Anyone who asks you to pay for anything – including tech support services – with a gift card is
scamming you. No legitimate company will ever ask you to pay with a gift card. If someone
wants you to pay with a gift card, please tell the FTC at FTC.gov/complaint.

Cyber Security Trivia

The trivia question for this month is:

- Web sites with SSL (Secure Socket Layer) can improve the security of online transactions, but
  which of the following is NOT a function provided by SSL?
    A. Encrypts the contents of an online transaction
    B. Verifies the identity of the recipient
    C. Verifies that both sides have agreed to the conditions of the transaction, preventing
       either side from denying of ever having made such a commitment
    D. Prevents packet sniffing

- Email your answer to: pyoder@elcamino.edu

Write in with your IT security questions:

If you have any questions about cyber security, please send them to: pyoder@elcamino.edu

All current and previous issues of the Monthly E.C.C. Information Security Briefing are posted online at:
  - http://www.elcamino.edu/about/depts/its/techservices/infosec.aspx
Paul T. Yoder
Information Systems Security Specialist
El Camino Community College District
pyoder@elcamino.edu