Monthly ECC Information Security Briefing
June 26, 2017

ECC Internal News

Introduction to the ECC 5-yr. Info Security plan

One of the main goals of the 5-yr. Security plan is to enhance the integration of security into our entire infrastructure - including all networks, systems, and data. To accomplish this, it will mean taking a critical look at what we have in place now, and how we can complement that by either replacing or adding different components and layers of security that all work cohesively together. The end goal should be to have protective measures and controls in place that fit seamlessly together in order to close as many security gaps as possible. This will not only take a significant amount of time and effort to make happen, but also a significant budgetary commitment by ECC stakeholders. Just the Next Gen Firewall Replacement Project alone could cost upwards of $1.5 million. However, compared to the cost of a significant data breach in terms of loss of public confidence, damage of our reputation within the California Community Colleges system, and potential fines and remediation costs – it’s still a bargain.

View/download the 5-yr. Info Security Plan here: http://www.elcamino.edu/administration/techservices/infosec.asp

ECC First Cybersecurity Penetration Test Completed
ECC, in cooperation with the California Community Colleges Tech Center CISO (Jeff Holden), recently conducted a cybersecurity penetration test designed to discover and document the potential weaknesses in our network perimeter as well as internal security settings on servers and endpoints. We appreciate the work that the CCC Tech Center performed as it will help shape our 5-year Info Security Plan by identifying security gaps that need our attention.

**External News**

**Hyundai Blue Link Vulnerability Allows Remote Start of Cars**

- Researchers at Rapid7 discover vulnerability to software v3.9.5 released on Dec. 8, 2016
- Allows “man-in-the-middle” attack over an insecure WiFi connection

**Scientists create “lip password” that ID’s users by their lip movements**


**Data Breach Watch**

**Higher education breaches for May 2017**

- University of New Mexico Foundation
- University of Wisconsin Health
- Augusta University, GA
Tip of the Month

Six Bad Habits That Almost GUARANTEE You’ll Be Hacked!

In a world full of slick social engineering con-artists, you don’t need to be a chain-smoking, inebriated gerbil to realize that you’re vulnerable. Here are six bad habits that will make you a “mark” faster than Usain Bolt can sprint 100 meters - and what you can do to prevent these habits from becoming the “norm”:

**Thoughtlessness**
- When creating online accounts, make sure your security answers are something you wouldn’t post casually on Facebook or can’t be found through a quick Google search.

**Apathy**
- Backup your personal files regularly and test your restore functions at least monthly
- Always be wary about emails from people you don’t know. Check the sender’s address. Check it closely. Social engineers work hard to make their email addresses look legit. Be diligent.
- Don’t download attachments from email addresses you aren’t familiar with and run any downloaded attachments through an antivirus program before opening.
- Don’t click on links! If an embedded link in the email is sending you to a website address, hover over the link (to discover the URL address), then type the URL manually in a browser window instead.

**Gullibility**
- If someone is revealing too much about themselves too early, this is a red flag. If they are showering you with gifts for no reason, beware. If he/she is being overly flirtty out of the blue and out of proper context – they might be trying to manipulate you.
- Don’t fall prey to the “charmer” and never give out private information that you normally wouldn’t give out publically.

**Curiosity**
- Don’t EVER use a USB drive that you found laying around somewhere. Social engineers drop them as bait on busy streets, in airports, in malls, etc. They will almost certainly contain backdoor Trojan programs, self-installing key loggers, or Ransomware.
- Never let anyone you don’t know and don’t completely trust plug anything into your computer. Aside from the USB threat discussed above, there are commercially-available spyware programs that can be easily installed on your computer or cell phone that will allow someone to monitor your emails, passwords entered, phone and text messages, etc.

**Vanity**
• Always double-check to see if someone online is who they say they are. Google search them. Contact them on another social media platform to test their authenticity – this is called identity corroboration.
• Always log into your social media accounts manually, never click on an embedded link to login – that’s just lazy.
• Always verify their given email address with one you have on file for them. They should match-up perfectly to be considered legit.

Greed
• The promise of a “sure thing” – the allure of easy money – it can do strange things to people’s brains. Always do your due diligence – never take anyone’s word for it.
• Never feel pressured into making a quick decision. Patience, when it comes to dealing with money, is always a virtue.
• If it sounds too good to be true, guess what? It probably is.

![This year’s most clicked social media scam lines](image)

Write in with your IT security questions:

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

Paul T. Yoder  
Information Systems Security Specialist  
El Camino Community College District  
pyoder@elcamino.edu