

Monthly E.C.C. Information Security Briefing

Date: March 20, 2017

Internal News:



- **REMINDER:** Campus-wide password reset coming April 18, 2017!
 - Please adhere to these guidelines for the creation of strong, complex passwords:
 - A minimum of 10 characters in length
 - A combination of UPPER-CASE & lower-case letters, numbers, and symbols (an example):
ReSeTmYpA\$\$wOrD!
 - A phrase that is easy enough to remember, but complex enough to deter someone from easily guessing it
 - Use this webpage to test the strength of your passwords:
 - <https://howsecureismypassword.net/>
 - The longer the time (in days/months/years) determines how long it would take a hacker using the usual password-cracking software to hack your password

- **Update on Forcepoint Triton AP-Web rollout**

- The month-long test environment in the Library was successful
 - Malicious activity is now being blocked on machines in the Library
- The Forcepoint clients will begin to be rolled-out campus-wide beginning in April, 2017
- I will be meeting with the Deans of each department to give them an overview of what Forcepoint does and what (if any) impacts to their unique environments may occur after deployment



- **New ITS Cyber Security webpage!**

- Contains all the latest cyber security articles, guides, and URLs
- Check it out: <http://www.elcamino.edu/administration/techservices/infosec.asp>



- **Write in with your IT security questions:**

- If you have any questions about cyber security, please send them to:
 - pyoder@elcamino.edu
- Any questions that may be of interest to a wide audience will be posted the following month!

External News:



- **Forecast: Sunny, with a chance of stolen credentials**
 - Malicious weather app found on Google Play!
 - Full story: <http://www.welivesecurity.com/2017/02/22/sunny-chance-stolen-credentials-malicious-weather-app-found-google-play/>



- **8 things you need to know about spyware**
 - Full story: <http://www.welivesecurity.com/2017/02/17/8-things-know-spyware/>

Tip of the Month:



- **SCAM ALERT: Can you hear me?**

- You've heard us repeatedly say, "Just don't click!". With this new scam, it's now "Just don't say YES!". Scammers are now calling you on the phone and asking you questions that will result in a "yes" response. They are recording your voice and then using it as evidence against you when they fraudulently sign you up for services and/or products. When the bank/credit card company fraud departments investigate the incident, the scammers are playing your recorded voice back to the investigators thereby proving that you agreed to the subscription or purchase. It may sound far-fetched, but the threat is real.
- Full story: <http://on.ktla.com/6GMrJ>