Monthly E.C.C. Information Security Briefing

Date: December 5, 2017

ECC Internal News Bytes:

- 18 Tips to Safeguard Your Mobile Devices, Social Media (Part 2 – Your Mobile Phone)
  - Be wary of what you install on your phone, and keep patches and iOS versions up-to-date!
  - Faculty – you are encouraged to share this with your students!

- Be sure to set PINS and passwords. This is your first line of defense in case your phone is lost or stolen. Also, set your phone to lock automatically between 30 seconds to 5 minutes after it’s idle.
- Only install apps from trusted sources. Check the reviews, confirm the legitimacy of the app store, and compare the app sponsor’s official website with the app store link to make sure they’re the same. Many apps from untrusted sources contain malware that can steal information and install viruses.
- Understand app permissions before accepting them. Check the privacy settings for an app before you install it. Be cautious about what access to your personal information you give apps.
- Be smart on open Wi-Fi networks. If unsecured, cybercriminals within range of the connection can get to your personal information. It’s wise to not use an open network unless you really have to.
- Wipe data on your old phone before getting rid of it. Your personal information is private for a reason, and you want to keep it that way. Reset the device to its factory settings before you donate, resell or recycle it.
- Report stolen smartphones. Did you know there’s a stolen phone database? Well, there is, so be sure to report the theft to local law enforcement, then register it with your wireless service provider. Other providers will be alerted, and they can set up remote “bricking” so it can’t be used without your permission.
- Don’t modify your smartphone’s security settings. This undermines the built-in security features and can make the device more susceptible to attack.
- Backup and secure your data. Contacts, documents and photos should be stored in the cloud, on a computer or on a portable storage device so you can restore the information if it gets erased, lost or stolen.
- Install security that enables remote location wiping. This might be a default on your phone or an app. It can remotely locate and erase all of the data on your phone if it’s stolen or lost. Some apps also offer loud alarms to find your phone (even if it’s on silent), as well as to help locate lost devices.
- Access updates and patches to your software. Set these up to automatically update so you reduce the risk of exposure to cyber threats.

External News Bytes:

- **T-Mobile API Bug May Have Leaked Customer Account Data**
  - A bug in T-Mobile's wsg.t-mobile.com API may have allowed attackers to access customer data that can be used to carry out phishing attacks or worse. The flaw only required an attacker to know or guess a victim's phone number to grant access to information including billing account numbers, email addresses, and phone IMSI. The vulnerability was discovered by Secure7 Founder Karan Saini who told Vice's Motherboard that an attacker could have had access to the information of all 76 million customers. "That would effectively be classified as a very critical data breach, making every T-Mobile cell phone owner a victim," Saini said.
What Country Does My Anti-Virus Software Come From?

- Since the Kaspersky Anti-Virus controversy emerged, more and more people are asking that question!
- This is a really cool Wiki tool to show you just where your AV software comes from:

Data Breach Watch

- U.S. Higher Education Breaches For October, 2017:
  - Creighton University (Omaha, NE)
  - Cabrillo College (Aptos, CA)

Tip of the Month:

- Hacked Robo-Vacuum Could Spy On Your Home
  - LG SmartThinQ smart home devices were totally hackable prior to a recent security update, according to new research. The HomeHack vulnerabilities in LG’s SmartThinkQ mobile app and cloud application created a means for hackers to remotely log into the SmartThinQ cloud application and take over the
user's LG account, CheckPoint security experts said. Once in control of an account, any LG device or appliance associated with that account could be controlled by the attacker – including a robot vacuum cleaner, refrigerators, ovens, dishwashers, washing machines and dryers, and air conditioners. Devices could be switched on and off, settings changed and more. IoT hackers might be able to gain control of the LG Hom-Bot vacuum cleaner's video camera. The technology streams live video to an associated LG SmartThinQ smartphone app as part of its HomeGuard Security feature. Hacking the system therefore creates a spying risk. The vulnerabilities in the SmartThinQ mobile app allowed researchers to create a fake LG account before using this to take over a user's legitimate LG account, and in turn gain remote control of the user's smart LG appliances. Check Point disclosed the vulnerability on July 31. LG fixed the reported issues at the end of September. Users of the LG SmartThinQ mobile app and appliances should ensure they have updated to the latest software versions from the LG website. To address the specific vulnerability identified by Check Point, users should update their LG SmartThinQ app to the latest version (1.9.23), either via Google play store, Apple's App Store or via LG SmartThinQ app settings.

- 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/administration/techservices/infosec.asp