Information Technology Services

CYBER SECURITY OFFICE

Monthly E.C.C. Information Security Briefing

Date: May 24, 2017

ECC Internal News:

- **ECC Cybersecurity implements the Tenable Security Center and Nessus Vulnerability Scanner**
    - This industry-standard security software was obtained from the CCC Tech Center
    - This will allow us to:
        - Collect an e-inventory of all ECC computer assets
        - Run vulnerability scans based on popular security frameworks such as NIST and CIS Top 20
        - Be proactive in remediation of vulnerabilities before they become a liability
        - Become compliant with standards such as PCI-DSS and FERPA

- **What is FERPA data, and why is it important to protect here at ECC?**

    - FERPA is the Family Educational Rights & Privacy Act that was enacted to help protect the privacy and confidentiality of student records.
    - It is even more valuable to hackers than HIPAA records because it contains more information:
        - Personally Identifiable Information (PII) – name, address, SS#, DOB
        - Education Record – grades, classes, etc.
        - Health Records – immunization info, school nurse records
        - Directory Information – PII plus place of birth, honors/awards, attendance dates
    - Never store FERPA data on USB drives, unsecured computers, or cloud storage mediums (DropBox)
    - Never send FERPA data as an email attachment (limited data may be acceptable)
    - If you have access to ECC Reporting Services and see this warning at the top, it is FERPA data:

Important Notice: Per FERPA Regulations, the data generated by this process may contain confidential student information. This information should **NOT** be stored on unsecured computer, unsecured drives and devices, or emailed as an attachment.

    - See the complete article on FERPA data on the Cybersecurity website:
        - 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

    - Here's an interesting question I was asked during a class that I conducted recently:
        - Even if I just use Bluetooth for my headphones, am I still vulnerable to being hacked?
            - The unfortunate answer is – YES. Once you enable Bluetooth on your phone or IOT device (for whatever reason), you are a potential target for a hacker.
            - This does not mean that you should never use Bluetooth. Just be more careful when you are out in public places and turn it off when you don't absolutely need it.
            - Bluetooth can be used for "Bluejacking" your enabled device in order to steal your personal information.

External News:

- **WannaCry Ransomware Worldwide Panic**

    - May 12, 2017 – The day the world held it's breath when WannaCryptor was released into the wild
    - More than 150 countries affected
    - Tool originated with the NSA's eternalblue hacking program (one of many recently stolen from the NSA)
    - Unpatched Microsoft systems primarily affected, but Apple OSX may be vulnerable also
    - Designed to spread laterally across the network via Microsoft's SMB ports (139 & 445)

- **Android Geo-Location Spyware Installed By Up To 5 Million Users**

    - SMSVova, disguised itself as a system update app on the Google Play store
    - App would hide itself in the background and report users' geo-locations to attackers
    - Full story: http://www.darkreading.com/endpoint/android-geo-location-spyware-installed-by-up-to-5-million-users-/d/d-id/1328703

- **Higher education breaches for April, 2017:**

    - FAFSA: IRS Data Retrieval Tool
    - University of Louisville

Tip of the Month:

- **Shimmer Me Timbers!**

    - Shimmers are data recording devices placed in ATM machines or Point-of- Sale devices
    - They record the data on your credit card chip as it is read by the underlying machine
    - How do you avoid being targeted by these devices?
        - Keep your wits about you when you're at the ATM, and avoid dodgy-looking and standalone cash machines in low-lit areas, if possible.
        - Stick to ATMs that are physically installed in a bank. Stand-alone ATMs are usually easier for thieves to hack into.
        - Be especially vigilant when withdrawing cash on the weekends; thieves tend to install skimming devices on a weekend — when they know the bank won't be open again for more than 24 hours.
        - Keep a close eye on your bank statements, and dispute any unauthorized charges or withdrawals immediately.
    - More info:
        - https://krebsonsecurity.com/2017/01/atm-shimmers-target-chip-based-cards/