Information Security

Ben Seaberry

District Council

October 24, 2019

National Cybersecurity Awareness Month

- National Cybersecurity Awareness Month 2019
- SJECCD Board Resolution in Support of Cybersecurity Awareness Month
- Cybersecurity Basics https://www.malwarebytes.com/cybersecurity/
- How to Stay Safe Online https://staysafeonline.org/stay-safe-online
- Cyber Tips and Resources https://www.dhs.gov/stopthinkconnect-toolkit
- FBI Scams and Safety https://www.fbi.gov/scams-and-safety

Cybersecurity Threats @ SJECCD

- Phishing – Email, Text, Voice, Social Media
- Spear Phishing – Direct Deposit, Loans
- Hijacked Email - Impersonation
- Ransomware – Encrypted Files, Fake Threats
- Malware/Spyware – Key Logger, Monitor Activity Botnet, Attachments, Links
- Identity Theft - Personally Identifiable Information (PII)
- Computer/Network Access

Cybersecurity Threat Protection (1)

- Use strong passwords; Use different passwords; Use a passphrase; Use a password wallet
- Keep a safe backup copy of important files
- Keep antivirus and all software up to date
- Do not follow any unsolicited email with a link to enter your username and password
- Do not click unknown hyperlinks through email or online; Do not open unknown attachments
- Check email address of sender (impersonations abound); [EXT] means External email sender
- Do not necessarily trust an email from someone you know; Do not trust requests for personal information or money, etc., without non-email verification

Cybersecurity Threat Protection (2)

- Do not leave computer unlocked; Log out of applications when done; Log off computer when done;
- Do not let others view PII on your screen
- Only store PII if necessary AND if authorized AND on an encrypted hard drive AND password-protected,
- Encrypt PII email
- Two-factor authentication (request)
- Don’t use unknown USB keys; Don’t store PII on USB keys
- Don’t enter passwords into a public computer
- Use VPN on public wireless
- Do not transmit PII on unencrypted network

Cybersecurity Awareness - Next Steps

- Internal Phishing Campaign with voluntary online training for those who “take the bait” (TBA soon)
- Board Policy and Administrative Procedure updates with respect to Information Security and Privacy
- Cybersecurity training for new employees
- Cybersecurity updated training for all employees
- Cybersecurity awareness for students
- Cybersecurity advanced training for selected departments
- Two-factor authentication
- Encrypted email

Cybersecurity Reporting

- Notify your Supervisor
- Notify ITSS – ITSS Help Desk or itsecurity@sjeccd.edu
- Notify Local Police