March 13, 2020

To all TVCC College Employees,

Cybercriminals are working overtime trying to exploit Coronavirus and 'work-from-home' situations. As College staff shift to a 'work from home' model for a short while, it is important to keep in mind our existing information security practices, and to adopt extra security measures. As you receive instruction and remote access to the College network, please pay attention to the following best practices:

Keep College data 'on College technology': IT will provide directions for connecting to our virtual desktops (Remote connections) from home.

- Do not screenshot items and save them to your home computer.
- Do not save confidential information from email, email attachments, Network drives, or other sources to your personal technology.
- If you checked out a laptop, treat this as you would personal technology; laptops are a high-theft target, any confidential College data stored on a stolen laptop would be considered a data breach by the State of Oregon and the Department of Education.
- Virtual desktop allows you to access 'My Documents', network drives, and other College data just as if you were in the office. Save to these locations as you normally would.

Antivirus Software:

- If not already installed, install Antivirus (A/V) and scan your computer at home, (yes, this includes Macs also.)
- Some free A/V options include: Sophos Free, Webroot Paid, and Bitdefender Paid.
- In addition to the above A/V, MalwareBytes free is an excellent second level of defense (you can install and use both.)
- Never disable A/V, in fact many malware infections start with a user disabling their A/V per request of the malware.

Secure Your Home Computer:

- Install recommended security patches for Windows or iOS and reboot as required. These are usually enabled by default, however it's a good idea to double-check that you're up to date. Google will make this verification easy, or feel free to email IT Help desk (helpdesk@tvcc.cc) for more information.
- Laptops (personal or College) are high-value targets for theft. As stated above, ensure these are locked up at home safely, and do not store any College information on them (even if they belong to the College.) Please do not leave technology in vehicles.
- Verify that your home computers and laptops auto-lock, and require a password to unlock.
- If you share your computers with family members, log out of all College connections before allowing others to use the technology. Also, kids are great at finding computer viruses – see above regarding A/V.

Cloud Storage:

- As always, do not store College confidential information on cloud storage services such as DropBox or Google Drive. The InfoSec risks are similar to storing College data on personal technology.

TVCC Email on Phones: If your phone is setup to connect to TVCC's email services they must be secured as well.

- Phones should require a passcode, swipe pattern, fingerprint, or face ID to unlock.
- Phones must auto-lock after 3-5 minutes.
- Enable any 'find my phone' type services, and verify that you can locate your phone remotely.
    - These services also allow the ability to wipe the phone remotely in case of loss.
- Failure to follow these steps could result in our College reporting a data breach to the State of Oregon and the Dept. of Higher Ed.

InfoSec Support: The IT office will provide guidance via standard operating procedures:

- Forward questionable emails (phishing, spam,) helpdesk@tvcc.cc. If you have questions about the email, let us know – better safe than sorry.
- Help Desk tickets – for any and all IT support needs.

Increased cybercrime activity: Hackers continuously monitor our web site and try to exploit new events.

- Expect increased phishing emails purporting to be from College leadership – report to helpdesk@tvcc.cc as normal.
- Expect increased phishing emails, or malware on the internet relating to COVID-19. There have already been reports of malware infections under the veil of Coronavirus trackers, etc.

Dangers of working from home:

- Working from home technology means you are outside of the College firewall and other defensive technologies. Use extra caution.
- Working outside of our normal environment and routine increases our chance of human error. Remember to be extra cognizant and watch out for phishing emails, malware, unsolicited attachments, etc.
- In a nutshell: Question everything, trust your gut, and reach out to IT. Our goal is to protect and support you through these unnerving times.

Scott Carpenter
Chief Information Officer
Treasure Valley Community College
scarpenter@tvcc.cc
541.881.5773