ACADEMIC COMPUTING AND NETWORKING SERVICES
COLORADO STATE UNIVERSITY

INFORMATION SYSTEMS
COLORADO STATE UNIVERSITY

OFFICE OF TELECOMMUNICATIONS
COLORADO STATE UNIVERSITY

>path FW: 2020

Importance of Home IT Security

As we settle into working from home, we are learning many good lessons related to working remotely. It's also a good time to remind ourselves that some of our practices need to adapt to our new environments. IT security is one of those things.

For this week's column, we wanted to turn it over to the experts to talk to us about "Strong Home IT Security". Many thanks to Kelly Poto with research contributions from the Cybersecurity Internship Team and Information Security Office for being our guest columnists.

Strong Home IT Security

As you get into the swing of working remotely and settle into your home setup, we want to ensure that you and your new environment are as secure as possible. The change in environment does not mean that we change our computer and information security habits. In fact, the risk is even greater in our remote offices and attackers know it. They are attempting to take advantage of the upheaval caused by COVID-19 to encourage you to compromise your access, network, and devices. However, with the

application of a few tips and strategies, you can make your remote environment “Chuck Norris” strong. Here are five simple steps you can take to protect your family, home, and of course, your remote work environment.

Tips and Strategies:

1. Be alert.

Attackers know we are distracted and are employing social engineering techniques which trick us to reveal information that we would not normally reveal, like passwords, usernames, accounts, devices. One way to protect against this is to simply be alert and wary of everything you receive. Ask yourself: does that email seem odd? Would my boss really send that message asking for my password? Does the IRS actually need my bank account number? The answer is NO. When in doubt, do not click.

2. Limit access to the device(s) that you use for work.

Work devices are for work. Do not let family members use these tools and explain why they are unable to do so. Many risks can easily be avoided just by limiting who can access your work devices.

3. Lock your computer when you walk away or it’s not in use.

You lock your computer when you walk away in the office, you should still be continuing this practice at home. Locking your computer ensures the security of the data and work you are performing. In our home environment, this simple practice can protect us from little fingers and furry friends.

4. Make sure your software and device operating systems are up to date.

Apply all patches and updates to applications, software, and device operating systems. Updates patch security flaws that keep your data and devices secure.

5. Use the Virtual Private Network when needed.

Make sure to use the Virtual Private Network (VPN) when you are connecting to CSU applications like Kuali, Oracle, and TimeClock Plus Manager. You do not need to use the VPN for Office 365 applications.
The VPN is a tunnel that encrypts your data allowing you to conduct your work through secure channels. Find instructions for using the Pulse VPN on the ACNS Security page.

Remain aware. You are the greatest defense to thwarting would-be attackers and protecting your family, network, and devices.

Resources:

If you'd like to learn a bit more about best security practices for remote working, check out the following links from trusted resources:

- https://staysafeonline.org/wp-content/uploads/2020/03/NCSA-Remote-Working-Tipsheet.pdf
- https://us.norton.com/internetsecurity-emerging-threats-working-from-home-due-to-coronavirus.html
- https://security-awareness.sans.org/sites/default/files/2020-03/03-SSA-Coronavirus%20-WorkingFromHome-CheatSheet_English%20UK.pdf
- https://www.acns.colostate.edu/security/
- https://www.acns.colostate.edu/keepworking/