Information Security

As YCCD employees begin working from home, it is important to remember that handling district data outside of our typical workspaces presents unique challenges. Taking a few additional security precautions when working remotely can help to keep the district's valuable information secure. The following are steps you can take to enhance security.

Please be aware that cybercriminals will be preying upon all of us and using the current emergency to trick us into providing personal or financial information or into infecting our systems with malware. Please be extra cautious when opening emails or attachments from unknown or unexpected sources.

As a way to help you identify emails coming from external resources, YCCD is implementing a warning banner in your email. Here is a sample of the banner you will see.

You will also see a warning indicator in your email list and on your mobile devices.

If you see this banner or warning indicators, please exercise caution before opening the email or any attachments. Be safe and if there are any concerns about an email…please contact the Helpdesk at 530-741-6981 or at helpdesk@yccd.edu

Beware of Phishing

YCCD is a high-value target for cyberattacks, especially during times of uncertainty. Be especially wary of emails that attempt to get you to share your password as a requirement for working remotely. Attackers will often try to exploit an existing relationship by posing as a person you know or trust (such as a colleague or supervisor) and by creating a sense of urgency.

The following links provide additional guidance on how to recognize attempts at phishing and social engineering:

- Avoiding Social Engineering and Phishing Attacks from the US Department of Homeland Security
- Two Simple Rules That Can Spot Nearly Every Email Phishing Scam from Digital Check

Cybercriminals generally tailor email and web-related scams to current topics and trends. With news headlines dominated by information related to pandemics, coronavirus, and COVID-19, you must remain vigilant for scams centering around these subjects. Be cautious and take basic online safety precautions when seeking information regarding COVID-19, including:

- Avoid clicking links in unsolicited email and do not open email attachments from senders you do not recognize.
- Never give out personal financial information through email.
- Use legitimate websites as sources of information regarding COVID-19.

Remember, legitimate services and sites, including the district, never have a reason for you to send them your password. In addition to email, there is at least one known COVID-19 outbreak map being circulated from a non-legitimate website. This particular map loads malware onto the system where it is visited. It is safe to assume that this will also be a commonly used tactic as individuals continue to use resources such as these maps to educate themselves on the current pandemic.

Keep Work Data on Your Work Computer

Whether you are using a district-issued device that connects directly to district resources or accessing resources via a remote desktop connection, avoid storing district data on your personal device.

Protect Your Devices

Enable Firewalls: Adequately protect your computer/system. This includes activating and/or enabling anti-virus software, regularly updating your operating system, and enabling the firewall on your operating system. The following are links to activate the delivered firewall functionality on both Windows and Mac OS:

- Windows Firewall
- Mac OS Firewall

If you are using a personal device and don't have antivirus software installed, then you can get free anti-virus programs for your Windows or Mac OS device via the following links:

- Windows – Avast Antivirusfor Windows or Zone Alarm Antivirusfor Windows
- Mac OS – Avast Antivirusfor Mac

Avoid Public WiFi: If necessary, use a personal hotspot. Public WiFi can introduce significant security risks and should only be used if absolutely necessary.

Keep Your Device With You: Always keep your device with you. Never leave your device or laptop in your car unattended, and make sure your screen can't be seen by those around you. Don't walk away from your laptop or mobile device, even for a minute. Don't ask a stranger to watch your laptop/mobile device for you.

Protect Your Password: Password protection or other appropriate access controls must be enabled on any personal device you use for remote access. If the personal device is to be used by other persons (such as your family members), a separate password/access control protected profile should be setup for the employee, which cannot be accessed by other individuals.

Never share your district password(s) with anyone, including family members.

Report Security Incidents: It is your responsibility to report any information security incidents to ????.

Examples of reportable security incidents:

- Compromised User Account
    - Password was compromised (such as stolen, lost, reset without user knowledge)
    -
    - Restricted data was accessed and/or altered without user knowledge
- Compromised System
    - Computer system intrusion (such as spyware, malware, or key logging detected)
    - Unauthorized access to, or use of, systems, software, or data
    - Unauthorized changes to systems, software, or data
- Lost/Stolen Media with Protected Data. Any media that store high risk and confidential data (for example, a computer, laptop, USB, tablet, external hard drive, paper, photo, and so on)
- Unauthorized Access or Release of Protected Data
    - Release of confidential data to unauthorized personnel either accidentally or maliciously (for example, sent data to wrong email address, accidentally included high risk data in attachment, posting of high risk or confidential data on website, and so on).