Protecting from Scams during COVID

South Dakota Attorney General's Warnings:

- Be alert to "phishing" emails – ones that appear to come from legitimate government agencies such as the Centers for Disease Control' especially if the email encourages you to click on a link for more information. Simply delete them without response
- Ignore phone calls' emails' advertising or mail items offering a miracle cure for' or protection against' Coronavirus. These are scams. There currently is no vaccine or cure. When one is available' residents can be sure that the appropriate government agencies will promptly provide information to the public. When receiving these calls do not press a number to be removed from the calling list.
- Don't be fooled by calls or text messages claiming that you are required to pay for testing or to provide personal information as part of a government response to the Coronavirus. These are scams. Be vigilant about not giving out your personal information via phone or any other means – you do not know who you may be giving this information to.
- Businesses should be aware that the Google scam is prevalent at this time. The recorded message asks you to verify your Google account and that failure to do so will result in your business name being dropped from Google. This is a scam' do not press any key to talk to someone or to be removed from the calling list.
- Beware of unauthorized or fraudulent charities or solicitations. Bogus charities will try to solicit donations during these emergencies. Do not donate any funds without doing your homework by visiting charitynavigator.org
- Contact the Attorney General's Consumer Protection Division at (800) 300-1986, or email consumerhelp@state.sd.us of suspected fraud; or visit www.consumer.sd.gov to file a complaint.

Cybersecurity Awareness Info:

- Common tactics:
  - Phishing – emails will contain COVID-19 text and links in an attempt to bait the recipient in launching malware and ransomware to control endpoints, obtain credentials or hold your information for ransom.
  - Scams – With the shortage of medical supplies and PPE equipment, criminals are scamming individuals and companies with false sale of products, collecting upfront payments and never delivering.
  - Mobile Threats – Mobile applications that are pretending to be COVID-19 informational tracking apps, are installing ransomware on your mobile devices and locking the unit until the ransom is paid.
  - Teleworking – As caregivers or family/friends shift to working from home during this time, criminals are looking at this as another potential exploit. Fake VPNs are being created and sold by criminals in hopes to gain access to sensitive information at your home and to your work. Please use every precaution in your home environment as well as at work.