SET SEG

REMOTE WORK BEST PRACTICES

FOR EMPLOYEES

As you work from home, follow these best practices to keep your home and office networks safe.

- **Watch For Phishing Emails**
  Criminals can target you with information that appears to be about coronavirus or COVID-19. Make sure you know and verify the source of the email and be cautious when opening attachments. Click here for examples of COVID-19 themed phishing attacks and steps you can take to avoid them.

- **Be Wary of Phone Calls Requesting Information**
  If you don't recognize the voice, ask for a phone number and extension so you can return the call.

- **Use a Pass Phrase Rather Than a Password**
  Pass phrases of 16 characters or more are more secure and easier to remember. You can use song lyrics, the first line of your favorite book, or a movie quote – but don't reuse passwords across multiple accounts, especially not between work and personal accounts.

- **Use a Password Manager When Possible**
  Apps like LastPass, KeePass, and 1Password all make it simple to login using unique passwords, while only requiring you to remember one strong password.

- **Secure Your Home Wireless Network**
  Remove the default password from your wireless router and use a long pass phrase to join your wireless network. Make sure the Wi-Fi Protected Access 2 (WPA2) protocol is selected.

- **Don't Work From Public Networks Unless Necessary**

- **Keep Work and Personal Accounts Separate**

- **Use Anti-Virus Software**

- **Think Before You Click**

- **Immediately Report Anything Suspicious to Your IT Team**