



8 CYBERSECURITY TIPS for working remotely

1



DO use a secure connection to ensure encryption of data when accessing business applications or services over the internet.

2



DON'T use the computer in an accessible place in the house where others may see what is on the screen. If you have to use your kitchen table turn everything so your family can't see your screen.

3



DON'T access critical medical or business systems from computers that your family shares and may already be compromised. If a hacker has installed a key-logging system on your unsecure family computer, they can get the password to your most sensitive business systems. Use a business system or have your IT department or vendor inspect your home computer before use.

4



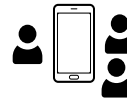
DON'T print documents unless you can immediately secure them from unauthorized viewers. Remember, if you didn't print it you wouldn't have to worry about it.

5



DON'T throw away sensitive or regulated printed business documents. Shred them.

6



DON'T have business phone calls to discuss patients, clients or workforce members where anyone else can hear the confidential information.

7



DON'T fall for email scams asking for money transfers, sensitive information, gift card purchases, or payroll direct deposit redirections without TALKING to the person making the request to verify it.

8



DO log off if you have to walk away, even for a minute, which may turn into 10 or 20.

Source: *CompTIA, 2020*