Crisis management: using technology to safely work from home

Stay safe and secure when you work from home with these best practices.

If you’re an employee:

- Use strong passwords.
- Keep your software up to date on laptops and mobile devices.
- Back up your laptop daily.
- Reboot your computer daily so that your antivirus program can be updated.
- Lock your computer when you take a break.
- Be extra vigilant of email phishing scams.
- Prevent the access of inappropriate internet sites from your work laptop.
- Do not download files from unknown sources on the internet or email.
- Do not leave sensitive work documents in the common areas of your house.
- Be careful of what others can see in your house when you’re on video chats.
- Shred any sensitive documents that you print at home.
- Rebooting your cable modem daily can improve your Internet speed and fix connection issues.
If you’re an employer:

- Take “work from home” training.
- Create a dedicated hotline or email for your employees to report cybersecurity issues.
- Enforce stronger password requirements for data on your cloud networks.
- Discourage the use of personal emails for company work, including the forwarding of work emails to personal emails.
- Provide secure laptops for your employees to work from home.
- Use encrypted VPN to connect to company systems and data.
- Disable USB drives to prevent unauthorized downloading of company files.
- If your employees use their personal computers, check the security controls (e.g., antivirus, malware, etc.) on the computers before granting access to company data.
- Restrict data access for employees who use shared computers at home.
- Add additional manual controls (e.g., an extra approval for wires).
- Temporarily disable or restrict access for furloughed employees.
- Create and enforce procedures to collect company equipment or files from terminated employees.