



# TAKING SECURITY HOME

## Working Remotely & Securing Your Home Office

Make security a priority with the following guidelines -

### ✓ Stay Committed to General Security - Organizational Policies Still Apply

Working away from the office does not exempt employees from following policies, which were designed to prevent data breaches and to maintain the privacy of your employees, customers, clients, and business associates. Circumventing policy in any way undermines those efforts.

### ✓ Separate Work and Personal Data

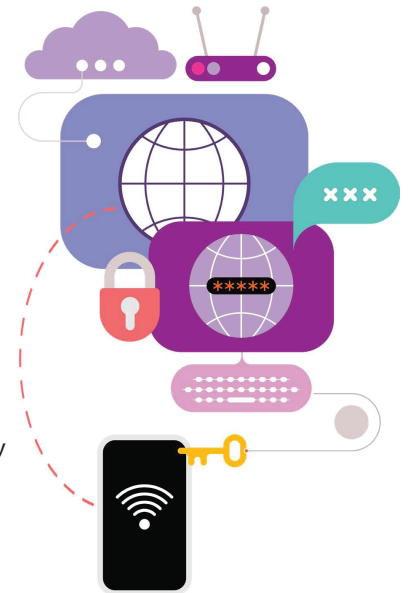
Employees should use organization-issued computers and mobile devices for work purposes only. If you do not supply organization-issued devices, be sure to update your policies about using personal devices to access your organization's data or networks, and consider creating separate user accounts, which will allow you to isolate work accounts from personal accounts by setting up specific logins for each.

### ✓ Secure Home Network Awareness

Employees should update their username and password of their router immediately upon working from home. Most routers ship with default login credentials that are public knowledge, which means anyone within range could log in and change settings. Employees should protect their network with a strong, unique password. They should never use the same password for their network and router. If you need help with general router maintenance or advanced network security options, there are plenty of "how-to" guides on the web that offer great advice in easy-to-understand language.

### ✓ Helpful Tips

- Update software, and enable automatic updates where available
- Think before you click!
- Remain skeptical of all requests for sensitive information
- Shred or destroy sensitive documents before discarding or keep secured until coming back into the office



Use a virtual private network (VPN). A VPN is software that encrypts your internet connection and prevents others from viewing your internet traffic. Employees should be required to use VPN to access your network.



Lock workstations. When not in use, always lock workstations and ensure no one else in the household can access work-related information or accounts.




Beware of smart devices. Ensure voice-controlled smart devices can't listen in on any discussions that involve confidential information. Ideally, have employees remove smart devices from their workspace.



Watch out for phishing scams. Cybersecurity experts warn about phishing scams tied to the pandemic. These emails are designed to take advantage of people's curiosity.

Working from home will continue to grow in popularity as more and more organizations embrace remote culture. So organizations also need to embrace remote security to maintain the privacy of your employees, customers, clients and business partners.

 If you have any questions, please ask!  
(314) 439-4700

