5 IoT Security Tips for Stay-At-Home Workers

SEI New ways. New answers.®

As millions of employees work from home because of the COVID-19 pandemic, Internet of Things security has become more critical than ever as cybercriminals look to exploit the situation. Follow these IoT security tips to reduce your risk:

1. **Turn on security features – and use them.** Most IoT devices have security features disabled by default when you buy them. This, along with default credentials that never get changed, creates easy opportunities for cybercriminals.

2. **Keep certain IoT devices connected on separate wifi networks.** Connect IoT devices such as Ring doorbells or Nest cams to a separate network. This will isolate your home office devices from risks arising from such frequently hacked devices.

3. **Use two-factor authentication.** When configuring an IoT device, take advantage of 2FA, sometimes called multi-factor authentication (MFA). These setups require a combination of passwords, numerical codes, or biometrics. Many people already use tools like the Google Authenticator on their personal devices for 2FA; it's the way of the future, and far more secure than the username/password system we all know so well.

4. **Read the instructions.** Shocking, we know! When setting up a new IoT device, take the time to familiarize yourself with all available security features—and risks. This includes whether the device has a web camera, a microphone, or default usernames and passwords that must be changed immediately. If your new device does have a webcam, consider the location of the device and whether to cover it up.

5. **Shut down devices when offline.** When devices are not in use, they should be completely powered off. This will ensure they're not hacked or abused when left unattended. It's not enough just to put a device into standby mode—far wiser, experts agree, to turn the power completely off.