**How smart are your devices?**

**Image:** Included in toolkit.

**Alt Text:** Hand ringing the doorbell on a doorbell camera.

Technology has become an integral part of society. We now rely on it to navigate tasks in our daily lives. When new technology becomes available, we are often amazed and excited to incorporate it into our lives.

You’ve probably seen the viral clips online of how smart devices like video doorbells help thwart home break-ins. You may even have one installed in your home, but how can you be sure these popular devices protect you? While they serve a purpose, we shouldn’t ignore security concerns with the devices themselves.

**The Risk-Reward Ratio**

Smart devices like video doorbells, voice-activated assistants, smart TVs and smart home hubs track and share more data than you think. Recently, video doorbells received criticism for the manufacturers handing over data without warrants to law enforcement and without the account owner’s consent. This illustrates a growing divide between our expectation of privacy versus the smart device’s actual privacy policy.

We often overlook the risks of installing and using these modern technology devices due to the expectation that security is already built in and will automatically work to keep us safe. How often have you checked the “*I agree to the terms and conditions*” box without reading the user agreement? We’re all guilty of this, but it’s critical to know that disregarding the agreement puts your personal information at risk and inadvertently grants access to other apps and devices.

**Steps to take with your smart devices**

When leveraging technology in our personal lives, maintaining a cyber-aware mindset is essential to a secure digital environment. Since most technologies only offer some degree of protection in their products, it’s vital to know how to configure them appropriately to be effective. There are ways to safeguard your information while using smart devices, and although it may lengthen the setup process, it’s worth the extra steps to keep you safe.

Remember these tips when you use a smart device:

* Research devices and their known security or privacy issues.
* Read user agreements before you install or update an application.
* Review and adjust your privacy settings to ensure they are beneficial to you. Don’t simply accept the defaults.
* Only enable necessary functions.
* Check the data your apps and devices are storing.
* Delete your recording history frequently or set your smart device to delete recordings automatically.
* Use the mute button or unplug devices when you aren’t using them.
* Turn off the built-in cameras when they are not in use.
* [Update your passwords frequently.](https://consumer.ftc.gov/articles/password-checklist)

It’s no secret that technology brings convenience and new capabilities to our lives—but it shouldn’t be at a cost. Take an active role in protecting your assets and data and maintaining your privacy while using smart devices to boost security protections, control, convenience and efficiencies. By exercising conscious tech habits and caution when using smart devices, we can enhance our security mindsets and protect ourselves.