



5 STEPS TO PROTECTING YOUR DIGITAL HOME

More and more of our home devices - including thermostats, door locks, coffee machines, and smoke alarms - are now connected to the Internet. This enables us to control our devices on our smartphones, no matter our location, which can in turn save us time and money while providing convenience and even safety. These advances in technology are innovative and intriguing; however, they also pose a new set of security risks.

SIMPLE TIPS

The Stop.Think.Connect.™ Campaign encourages you to follow these simple steps to secure your connected devices.

1. **Secure your Wi-Fi network.** Your home's wireless router is the primary entrance for cybercriminals to access all of your connected devices. Secure your Wi-Fi network, and your digital devices, by changing the factory-set default password and username.
2. **Enable stronger authentication.** Always enable stronger authentication for an extra layer of security beyond the password that is available on most major email, social media and financial accounts. Stronger authentication (e.g., multi-factor authentication that can use a one-time code texted to a mobile device) helps verify that a user has authorized access to an online account. For more information about authentication, visit the new Lock Down Your Login Campaign at www.lockdownyourlogin.com.
3. **Keep a clean machine.** Keep software up to date and install updates for apps and your device's operating system as soon as they are available. Keeping the software on your mobile device up to date will prevent attackers from being able to take advantage of known vulnerabilities.
4. **Know your apps.** Be sure to review and understand the details of an app before downloading and installing it. Also, check to make sure the vendor or creator of the app is reputable. Be aware that apps may request access to your location and personal information. Delete any apps that you do not use regularly to increase your security.
5. **Consider what you share.** Limit the amount of personal information you share about yourself online. Your full name, phone number, address, school or work location, and other sensitive information should not be published widely. Disable geo-tagging features that let people online know where you are. Limit your online social networks to the people you know in real life, and set your privacy preferences to the strictest settings.

Stop.Think.Connect. is a national public awareness campaign aimed at empowering the American public to be safer and more secure online. The Campaign's main objective is to help you become more aware of growing cyber threats and arm you with the tools to protect yourself, your family and your community. For more information visit www.dhs.gov/stopthinkconnect.



Homeland
Security

www.dhs.gov/stopthinkconnect



STOP | THINK | CONNECT™
