What You Need to Know to Secure Your IoT Devices

December 7, 2016
by Ari Lazarus
Consumer Education Specialist, FTC

Today's hackers are attacking a lot more than just computers. They're going after 'Internet of Things' (IoT) products – like internet-connected cameras and refrigerators and using them to create havoc on the internet.

In October, hackers used the "Mirai" malware to attack unsecured IoT devices, turning them into zombie computers to overwhelm and shut down popular websites including Netflix, Paypal and Twitter.

Attacks like that are more than just an inconvenience. They can put your information at risk. So what can you do to reduce the risk of compromise to your home network and smart products?

- **Don't just click "next" when you set up your IoT device.** Review the default settings carefully before making a selection, and use the security features for your device. If it allows you to set up a passcode lockout ("three strikes and you're out") and enable encryption, you can add a layer of protection to your device.

- **Download the latest security updates for your IoT device.** To be secure and effective, the software that comes with your device needs updates. Before you set up a new device, and periodically afterwards, visit the manufacturer's website or the device's settings menu to see if there's a new version of the software available for download. To make sure you hear about the latest version, register your device with the manufacturer and sign up to get updates.

- **Change your pre-set passwords.** The manufacturer may have assigned your device a standard default password. Hackers know the default passwords, so change it to something more complex and secure.

- **Want to know more? Check out the FTC's additional tips on** Online Security, including how to create a strong password and username for your router, and how to check for security updates.