Securing Your Home Network

Home network security refers to the protection of a network that connects devices to each other and to the internet within a home.

These days, electronics such as smart TVs, tablets, cell phones, and wearables are linked through the internet. Taking proactive measures to protect our home networks and devices may keep family members more secure when utilizing the world wide web.

Home Network and Device Misconceptions

My home network is not a target of a cyber attack

A cyber attack can happen to anyone and anywhere. Connecting unprotected devices to the internet may make them vulnerable.

New devices are secure right out of the box

Leaving factory settings and passwords unchanged may create opportunities for cyber attackers to gain unauthorized access to your devices.

Setup wireless security

Create strong network passwords for your routers and choose the strongest encryption protocols available such as WPA2, AES, TKIP. If the router is provided by your service provider, verify strong encryption is used and change the default router passwords.

Create a guest password

Some routers allow the setup of separate guest passwords. If you have visitors at home, setup a special password to protect your private network.

Reconfigure default settings

Ensure strong encryption and strong passwords are used with out-of-the-box software and hardware. Verify your device's firmware is up to date. Refer to the manufacturer's user manual for additional instructions.

Install a network firewall

A firewall can block malicious traffic going to your home network and alert you to possible cyber threats.

Install and update antivirus protection

Keep the protection current so it scans for the most recent dangers intended to cause harm to your network and devices.

Protect all devices connected to the internet

Establish passwords, PINs, or other advanced safety measures (if available) for internet enabled devices. Back-up and store important information often.

Move or Disconnect Home Devices

During business meetings / conversations, you should ensure voice enabled smart home devices are not within listening range and ensure your computer screen is out of the field of view of video recording devices.

Citi recommends clients follow industry best practices.

For more information please review information published by:

US-CERT | The US Federal Trade Commission | Europol

1974885 4/20