

Keep your home and community safe with **secure WiFi at home.**

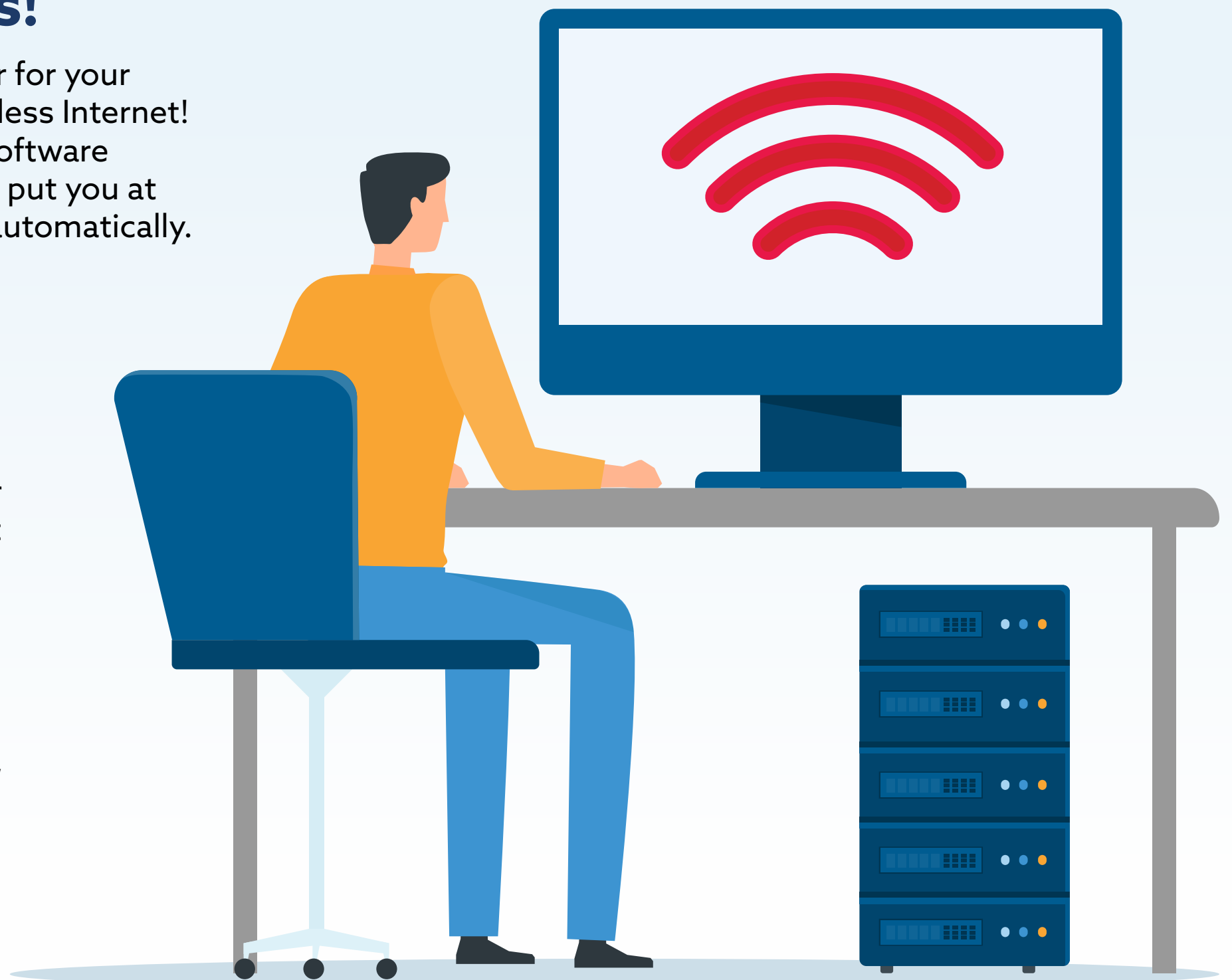
Update your wireless router software on a regular basis!

Internet providers often give you a Wireless Router for your home. This is what allows your home to have Wireless Internet! Annual software updates are your responsibility. Software updates address security vulnerabilities that could put you at risk, but these routers do not update themselves automatically.

Create separate WiFis for different purposes.

You can create different wireless networks on your router without additional cost. Setting up different networks helps stop the spread of infection.

- ✓ **Guest Network**
For folks who don't live with you.
- ✓ **Smart Device (IoT) Network**
For "Smart" devices like TVs, thermostats, toys, or other appliances that access the internet.
- ✓ **Work From Home Network**
It's always a good idea to separate your work and personal devices.



Five steps to securing your personal WiFi:

- 1. Password-protect your wireless network and WiFi router device.**
WiFi routers have a separate password, which differs from the password you use to access your WiFi. Both passwords should be changed annually.
- 2. Select WiFi Protected Access Version 3 (WPA3).**
This is currently the best protection for your WiFi.
- 3. Choose a safe name for your WiFi.** Names that identify you, your address, or what you use your network for can give attackers an edge.
- 4. Disable Remote Access Capability**
- 5. Don't set your WiFi to be administered remotely,**
from the internet, or outside your home.

**A secure personal WiFi keeps NH safe.
For more cyber safety resources, visit:**

www.theatomgroup.com/mcdp