CYBERSECURITY FOR
SMALL BUSINESS

SECURE REMOTE ACCESS

Employees and vendors may need to connect to your network remotely.

Put your network's security first. Make employees and vendors follow strong security standards before they connect to your network. Give them the tools to make security part of their work routine.

HOW TO

PROTECT DEVICES

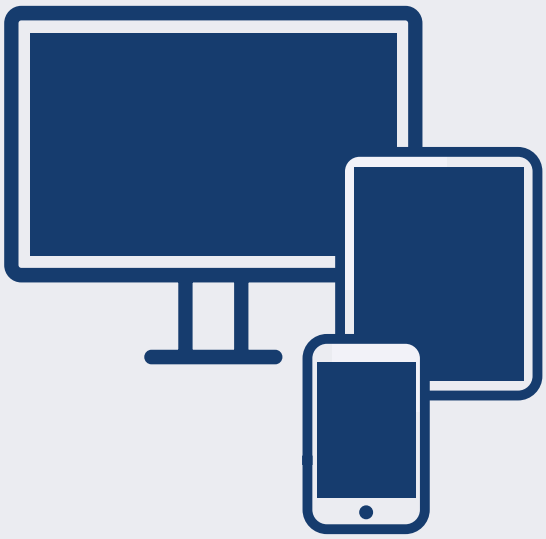
Whether employees or vendors use company-issued devices or their own when connecting remotely to your network, those devices should be secure. Follow these tips — and make sure your employees and vendors do as well:

Always change any pre-set router passwords and the default name of your router. And keep the router's software up to date; you may have to visit the router's website often to do so.

Consider enabling full-disk encryption for laptops and other mobile devices that connect remotely to your network. Check your operating system for this option, which will protect any data stored on the device if it's lost or stolen. This is especially important if the device stores any sensitive personal information.

Change smartphone settings to stop automatic connections to public Wi-Fi.

Keep up-to-date antivirus software on devices that connect to your network, including mobile devices.



LEARN MORE AT:
FTC.gov/SmallBusiness

FEDERAL TRADE COMMISSION

Homeland Security

NIST National Institute of Standards and Technology
U.S. Department of Commerce

SBA U.S. Small Business Administration

CYBERSECURITY FOR

SMALL BUSINESS

HOW TO CONNECT REMOTELY TO THE NETWORK

Require employees and vendors to use secure connections when connecting remotely to your network. They should:

Use a router with WPA2 or WPA3 encryption when connecting from their homes. Encryption protects information sent over a network so that outsiders can't read it. WPA2 and WPA3 are the only encryption standards that will protect information sent over a wireless network.

Only use public Wi-Fi when also using a virtual private network (VPN) to encrypt traffic between their computers and the internet. Public Wi-Fi does not provide a secure internet connection on its own. Your employees can get a personal VPN account from a VPN service provider, or you may want to hire a vendor to create an enterprise VPN for all employees to use.

WHAT TO DO TO MAINTAIN SECURITY

Train your staff:

Include information on secure remote access in regular trainings and new staff orientations.

Have policies covering basic cybersecurity, give copies to your employees, and explain the importance of following them.

Before letting any device — whether at an employee's home or on a vendor's network — connect to your network, make sure it meets your network's security requirements.

Tell your staff about the risks of public Wi-Fi.

Give your staff tools that will help maintain security:

- Require employees to use unique, complex network passwords and avoid unattended, open workstations.
- Require multi-factor authentication to access areas of your network that have sensitive information. This requires additional steps beyond logging in with a password — like a temporary code on a smartphone or a key that's inserted into a computer.
- Consider creating a VPN for employees to use when connecting remotely to the business network.
- If you offer Wi-Fi on your business premises for guests and customers, make sure it's separate from and not connected to your business network.
- Include provisions for security in your vendor contracts, especially if the vendor will be connecting remotely to your network.

LEARN MORE AT:
FTC.gov/SmallBusiness

FEDERAL TRADE COMMISSION

Homeland Security

NIST National Institute of Standards and Technology
U.S. Department of Commerce

SBA
U.S. Small Business Administration