FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS

Cybersecurity for small business: Secure remote access

Share This Page

Andrew Smith, Director, FTC Bureau of Consumer Protection
Feb 22, 2019

TAGS: Bureau of Consumer Protection | Consumer Protection | Privacy and Security | Data Security | Small Business

Punching a time clock in and out isn't how small businesses run these days. Employees are on the road, others are working from home, vendors are accessing your data at off hours – and you're generating ideas 24/7. How do you maintain high security standards when employees and others may need to connect to your network remotely from a variety of devices? When we met with small business owners across the country, that question came up a lot. As part of our Cybersecurity for Small Business campaign, we have a fact sheet of things to consider in securing remote access to your network.

How to protect devices

Whether employees or vendors use company-issued devices or their own, if they're connecting to your network, security should be priority #1:

- Change any pre-set router passwords and the default name of your router. And keep the router's software up-to-date, which may mean regular visits to the manufacturer's website for the latest security patches.
- 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 data stored on the device if it's lost or stolen – a particular concern if the device contains sensitive information.
- Change smartphone settings to stop automatic connections to public Wi-Fi.
- Keep up-to-date antivirus software on all devices that connect to your network.

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 home. WPA2 and WPA3 are the only encryption standards that will protect information sent over a wireless network.
- Use public Wi-Fi only when they're also using a virtual private network (VPN) to encrypt traffic between their device and the internet. Public Wi-Fi may be convenient, but it doesn't provide a secure connection on its own. (Have you thought about getting an enterprise VPN for all employees to use?)

What to do to maintain security

Your best defense against cyber risks is an in-the-know staff:

- When planning new employee orientation and periodic security refreshers, put secure remote access on the agenda.
- Write your cybersecurity policies in a way even less tech-savvy staff can understand, distribute the policies to your employees, and include the *why* – concrete reasons why cyber compliance is essential to the health of your business.
- 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 security standards.
- Warn your staff about the risks of public Wi-Fi.

Give your staff the tools to help maintain security

Your employees and vendors look to you to set the security standard. Have you implemented these practices?

- Require employees to use unique, complex network passwords.
- Remind them not to leave open workstations unattended.
- Consider creating a VPN for employees to use when connecting remotely to your network.
- Require multi-factor authentication to access areas of your network that have sensitive information. (This requires extra steps beyond just logging in with a password – like a temporary code on a smartphone or a key inserted into a computer.)
- If you offer Wi-Fi for guests or customers at your place of business, make sure it's not connected to your business network.
- Build security requirements into your vendor contracts, especially if the vendor will be connecting remotely to your network.

Download the FTC's remote access fact sheet for more information.

ftc.gov