CONTRIBUTING TO SECURE WIRELESS MICE AND KEYBOARDS IN YOUR WFH FLEET

Maintaining enterprise security is vital in today's world of ever-expanding cyberthreats. The wireless mice and keyboards your employees use every day are an integral part of the overall security landscape.

HERE ARE A FEW THINGS TO CONSIDER WHEN ASSESSING THE SECURITY OF YOUR FLEET'S WIRELESS PERIPHERALS.

- ☐ **Know what devices are connected to your endpoints**. If your organization doesn't provide the mice and keyboards to employees or have a list of approved, acceptable devices, there's no telling what's out there.
- ☐ **Make sure these devices have encrypted connections**. Encrypted connections prevent hackers from using devices like Wi-Fi "sniffers" and intercepting keystrokes and mouse clicks remotely.
- ☐ **Update the firmware on the devices.** Out-of-date firmware can leave devices vulnerable to identified exploits.
- ☐ **Ensure *Bluetooth*® devices employ Security Mode 1, Level 4.** This setting will help secure connections among devices.
- ☐ **Prevent devices with USB dongles from rolling back security firmware.** Devices that can roll back security-related firmware upgrades can expose your endpoints to attack.
- ☐ **Educate your employees on mouse/keyboard attacks.** Along with education on malware and phishing safety, make sure your employees know that strange mouse/keyboard behavior can be a sign that someone has taken unauthorized control.

Logitech solutions help implement security features in your enterprise fleet in a work-from-anywhere world. Explore the latest Logi Bolt devices for your employees today.

logitech | for business