SECURITY CHECKLIST FOR INDIVIDUAL USERS

iVision®

USE A PASSWORD MANAGEMENT TOOL

Use a password management tool and proactively change all duplicated passwords.

USE THE BEST POSSIBLE PROTOCOL

Use the best possible protocol (usually WPA2) for your home wireless internet and frequently change the admin password. Do not leave the default password from setup.

PAY ATTENTION TO BANDWIDTH ISSUES

Pay attention to bandwidth/connectivity issues and always look at what devices are connected to your Wi-Fi. If you don't recognize a device and can't identify what it is – remove it and update your Wi-Fi password.

NEVER LET ANYONE USE YOUR DEVICE

Never let anyone else in the house use your device. They could potentially compromise its security by falling victim to phishing attacks or malicious sites. Your family members may simply want to check their email or browse the internet, but don't let them.

ALWAYS USE YOUR VPN

Use your VPN when connecting to business applications. A VPN encrypts the connection from your machine to the office. It also allows for security updates that you might not normally receive when connecting over the internet.

DO NOT SHARE YOUR WI-FI PASSWORD

Do not share your Wi-Fi password with anyone outside your home. If you have guests, it is best to set up a guest network for them to access the internet. Most routers/access points have this feature, and you can disable the guest network when it's not in use.

KEEP ROUTER FIRMWARE UPDATED

Keep your router firmware updated with the latest releases. These devices have a long history of vulnerabilities. If available, enable auto-update.

KEEP ALL OS AND APPS UPDATED

Keep all operating systems and applications up to date. If this is not happening automatically on your corporate laptop, alert your company's IT support team.

DISABLE AUTOMATIC CONFIGURATION

Disable automatic configuration via WPS (if your router supports it). Having it enabled allows unauthorized individuals the potential to gain access to your network.