



# SMART DEVICES. SECURITY VICES.

We operate in a mostly mobile world. Our smart devices and constant connection help us get work done, but also expose us to vulnerabilities.

The fact that we are all constantly connected to our jobs, work applications, and company databases creates security risks we all have to be aware of to prevent anything bad from happening.

## ✓ DO

### Do authenticate

Enable two-factor authentication for added security.

### Do use passwords

Secure your device with strong passwords.

### Do secure

Visit and make transactions on secure sites only. Check for the **https** in the url, and padlock icon in the address bar that signal a site is secure.

### Do encrypt

Use a virtual private network to encrypt your online traffic, especially when connecting to a company network.

## ⊘ DON'T

### Don't download

Don't download programs or applications that you do not trust.

### Don't connect

Never connect to unsecured open wifi hotspots.

### Don't access

Don't pair your Bluetooth® unit to your phone or laptop in a public area where your pin can be compromised.