Simplifying cybersecurity tools

6 basic security practices to get started

❑ **Implement employee training and security awareness**
  Establish regular security training and promote security awareness for all employees using tools such as bi-monthly phishing simulation campaigns.

❑ **Help protect devices from bad actors**
  Use a mobile threat defense (MTD) solution to help protect devices from phishing/smishing attacks, unsecure Wi-Fi networks and malicious websites.

❑ **Manage your devices and employee accounts**
  Install a mobile device management (MDM) solution to help manage devices, employee access, privileges and policies, to separate business from personal applications and better control vulnerabilities in software and hardware.

❑ ** Adopt Acceptable Use Policies (AUP)**
  Establish Acceptable Use Policies for your mobile devices to set user access to your data according to your organization’s needs.

❑ ** Secure your networks**
  Use firewalls and containerized networks to help prevent unauthorized access to systems, devices and ports within your network and to stay current with vulnerability patches on hardware and software.

❑ ** Practice identity and access management**
  Limit access to data and information through multi-factor authentication and by granting employee access only to the extent required to do their jobs.

It shouldn’t take a compromise to step up your game.

Learn more.
Contact your Verizon Business Account Manager to discover how Verizon can help protect your business. www.verizon.com/business/products/security/mobile-device-endpoint-security/