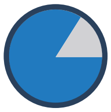
SECURITY
INNOVATION

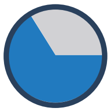
THE RISE OF MOBILE SECURITY: Are You At Risk?

There are **320 million people in the United States**[1] and **90% own a cell phone**.[2]

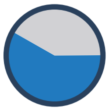


84% of mobile users utilize the same smartphone for business and personal use

42% store password and login information within apps on their smartphone



66% store personal data on their smartphone



62% of smartphone users do not use a password

Nearly 66% of Americans are now smartphone owners.[3]

Up to **190 million people** can be accessing the Internet via their mobile phone, connecting with various networks, insecure or otherwise, and putting their personal information at risk. **Anything you have saved on your phone is at risk!**

3 Most Common Mobile Security Breaches:

DEVICE LOSS & THEFT

The most common mobile "breach" is a staff member leaving a phone on the bus or in a taxi. This could allow access to company data but is more likely to lead to a flurry of expensive foreign calls and the loss of the device.

MALWARE

Even more malicious malware might take over a phone's data connection, send spam emails, infect other devices on the network or even harvest passwords. This is an increasing problem as hackers begin to target mobile devices and operating systems instead of desktop computers.

UNSECURED NETWORKS

Another danger is the rogue Wi-Fi network, set up by hackers to trap people logging on at airports, stations, or coffee shops. This has been common in Asia but is less often used, so far, in North America or Europe.

An Ounce of Prevention...

There's no denying the potential for mobile devices to improve efficiencies and lower costs for workers in industries of all types. You also can't deny the potential security vulnerabilities mobile devices present. Regardless of who owns a mobile device, employees should use the device in a secure and responsible manner to protect other employees, company assets, business reputation and **business mission.** Utilize the following best practices to help safeguard against loss and mitigate risks without placing a burden on your workforce.

✓ **Require Strong Authentication, Use Password Controls**
Password protection helps limit the costs and dangers of losing a phone. Users should be instructed to enable and use passwords to access their mobile devices. Companies or organizations should decide if some number of failed login attempts should cause the device to wipe its internal storage clean.

✓ **Equip Your Device with Anti-malware Software**
Mobile operating systems such as iOS and (*especially*) Android are increasingly becoming targets for malware. Anybody who wants to use a mobile device to access the internet should install and update anti-malware software for their device — especially for anyone who wants to use such a device for work.

✓ **Choose Your Applications Carefully**
Staff must be just as careful downloading software as they are with desktop machines. Organizations should establish policies to limit or block the use of third-party software. This is the best way to prevent possible compromise and security breaches resulting from intentional or drive-by installation of rogue software, filled with with backdoors and "black gateways" to siphon information into the wrong hands.

✓ **Avoid Unsecured Wi-Fi Hotspots**
Employees should treat Wi-Fi access with caution — or have unlimited data contracts so they don't need to use such open access points. Make sure devices aren't set to automatically connect to unsecured hotspots or even other Bluetooth devices.

✓ **Secure Mobile Communications**
Most experts recommend all mobile device communications be encrypted simply because wireless communications are so easy to intercept and snoop on. Any communications between a mobile device and a company or cloud-based system should require use of a VPN for access to be allowed to occur.

1. US Census Bureau. December 29, 2014
2. Pew Research Center Internet Project Survey, January 9-12, 2014
3. Smith, Aaron. U.S. Smartphone Use in 2015. Pew Research Center. April 1, 2015. http://www.pewinternet.org/2015/04/01/us-smartphone-use-in-2015/
4. Tittel, Ed. 7 Enterprise Mobile Security Best Practices. CIO Magazine. February 13, 2014. http://www.cio.com/article/2378779/mobile-security/7-enterprise-mobile-security-best-practices.html
5. Oates, John. The three most common mobile security breaches. The Telegraph. July 7, 2014. http://www.telegraph.co.uk/sponsored/technology/4g-mobile/data-security/10630309/mobile-security-breaches.html
6. Tittel, Ed. 7 Enterprise Mobile Security Best Practices. CIO Magazine. February 13, 2014. http://www.cio.com/article/2378779/mobile-security/7-enterprise-mobile-security-best-practices.html