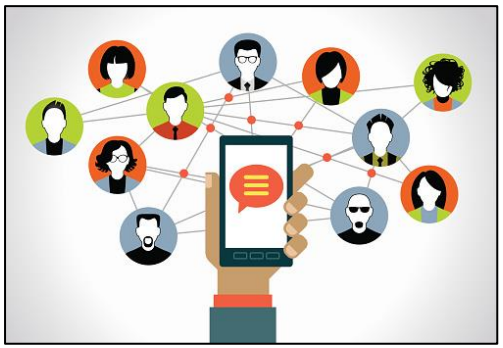
Mobile Security

Why Is Mobile Device Security So Important?

- Mobile security hasn't progressed as fast as smartphone adoption and use, making it a vulnerable area for attacks. Rapid progress in the mobile industry and introduction of apps, rooted phones (e.g. jailbreaking an iPhone), and cloud access has made mobile phones particularly vulnerable.
- Your mobile device contains as much access to data as your computer. Your mobile phone:
  - Contains personal sensitive data (name, age, passwords, addresses, etc.)
  - Contains university information
  - Provides access to your organization's network

These points make your mobile phone a valuable target for hackers.

For example, while hackers can only phish you through email on your computer, hackers can phish you through emails, texts, and calls to your mobile phone. Additionally, apps have given hackers new ways to download malware straight on to your devices. While the official stores (e.g. Apple store, Google Play Store, etc.) have controls in place to reduce malware on apps, some still get through and other online downloadable apps can contain malware.



25% of all mobile devices in an organization will be exposed to a network attack in the first month, and this grows to over 40% in the first three months (Skycure, 2016).

How Does a Breach Affect You and Your Organization?

The **average cost** of infection to an organization per mobile device.[1]

$9,485

230%

The increase in the number of malware **infected apps** from 2014-2015.[2]

If your phone is breached, hackers can:

- Access your personal and sensitive information (name, age, home address, etc.)
- See, send, and manage calls, emails, instant messages, social media, and texts.
- Use your internet connection to access all other files and devices on the network.
- View, manage, and create personal and corporate files, photos, apps, etc.
- Gain access to your cloud, stored credit cards, web browser, and saved passwords.
- Use your device to hack others, send spam, etc.

1. Ponemon Institute, 2016. 2. Symantec, 2016.

A Hacker's Common Practices

There are five common ways that mobile devices are breached:

1. Device Loss or Theft	In the U.S., 5.2 million smartphones were lost or stolen in 2014.[1] These devices are now in the hands of malicious individuals and if they are able to access the phones, they can use it as their own.
2. Unsecured Networks	Infected Wi-Fi networks can be used to hack your smartphone when you connect to it. Most users are unaware they are being hacked, but this gives the hacker full access to your phone. Most infected Wi-Fi networks are public as they are easier to access and manipulate.
3. Malicious Apps	Hackers have found ways to disguise apps as enterprise apps to get into the app stores. These apps contain malicious malware that can do many things, one of which is give the hacker full access to your phone and any network you connect to. Official app stores are policed but apps from unofficial app stores or websites are more likely to be malicious.
4. Phishing	While phishing on computers is usually done through email, hackers have a lot more methods of phishing on smartphones. Hackers are able to phish through calls, texts, emails, and social media. They usually disguise themselves as a trusted organization, such as your mobile carrier, bank, or government to get your personal information.
5. Unaware Users	Unaware users are one of the biggest threats to mobile security. Users have ultimate control on their device, from what they store on it to how often it gets updated. In 2015, 62% of smartphone users did not protect their phones with passwords.[2] This means anyone with physical access to their phones can take full control of it. Updates for software are provided to protect against the latest threats, so when users don't update in a timely manner, it leaves their phone vulnerable.

Be Proactive

Stay Alert

- Don’t download apps from unofficial app stores or from websites. If you have to, be vigilant and use antivirus protection.
- Install a “find my phone” app to locate it if lost or wipe/lock them if stolen.
- Consider the access/permissions you are giving an app.
- Be suspicious of calls, emails, texts, etc. that ask for personal information such as user names and passwords.
- Ensure your phone has access control measures in place (fingerprint locks are safer than passwords).

Stay Updated

- Continuously update your apps and operating system (OS) to protect against the latest threats.
- Ensure you have an active and updated antivirus. New antivirus software will detect malware, privacy leaks, viruses, etc.
- Use VPNs when connecting to public Wi-Fi networks.

Reporting and Contact Information

If you have any general questions:

– Bruin Support Services at 1.800.756.7920

A private, non-profit institution founded in 1966, Bellevue University is accredited by the Higher Learning Commission through the U.S. Department of Education. For general information, please call 1.800.756.7920.