MOBILE DEVICE SECURITY BEST PRACTICES

Questions about this document can be addressed to itap-securityhelp@purdue.edu.

Purdue University information security best practices are those steps that you can take on your own to help secure the computing resources that you use. Best practices are not usually related to any particular University information security policy, but are instead a combination of information security tips, tools, and techniques that you can use to protect your resources and data.

Mobile computing devices are devices such as tablets, smart phones, e-readers, and laptop computers. The very features that make these devices useful (portability, access connectivity, data storage, processing power) also make them a security risk to users and to Purdue University when they contain University data. Major features of mobile devices that cause a risk to the user and potentially the University include their small size (they can be easily lost, stolen, or misplaced); weak user authentication mechanisms that can be easily compromised or simply disabled by the user; and their ease of interconnectedness.

As mobile devices become more powerful and ubiquitous, they need to be treated with the same or greater care than personal computers. This document explains general end-user security measures that can be taken on mobile devices. Taking action to personally ensure computer security helps protect everyone from data and identity theft, viruses, hackers, and other threats. Every member of the Purdue community who uses a computing device makes Purdue’s computing environment more secure by following these best practices.

General Security

- Keep your mobile devices with you at all times or store them in a secured location when not in use. Do not leave your mobile devices unattended in public locations (e.g. airport lounges, meeting rooms, restaurants, etc.).
- Mobile devices should be password protected and auto lockout should be enabled. The password should block all access to the device until a valid password is enabled. The password used should be as strong a password as your device will support. Learn more about “creating strong passwords” at http://www.purdue.edu/securepurdue/bestPractices/passTips.cfm.
- Enable a “remote wipe” feature if available. This also includes features that delete data stored on the mobile device if a password is not entered correctly after a certain number of specified tries.
- Do not circumvent security features or otherwise “jailbreak” your mobile device.
- Standard security protocols should be followed. This includes ensuring your device has current anti-virus software and all operating system and application updates and patches. Firewalls should be enabled if possible. Learn more about “End User Security Guidelines” at http://www.purdue.edu/securepurdue/bestPractices/endUserSecurityGuidelines.cfm.
• Wipe or securely delete data from your mobile device before you dispose of it.
• Lost, stolen, or misplaced mobile devices should be immediately reported to the police. If your mobile device contained Purdue data, also inform your IT department about a lost, stolen, or misplaced device. Learn more about “Security Incidents” at: http://www.purdue.edu/securepurdue/bestPractices/securityIncident.cfm.

Transmission Security
• Where possible, data transmissions from mobile devices should be encrypted.
• Wireless access, such as Bluetooth, Wi-Fi, etc., to the mobile device should be disabled when not in use to prevent unauthorized wireless access to the device.
  o In general, keep your wireless connection on hidden mode unless you specifically need to be visible to others.
• If available wireless access should be configured to query the user for confirmation before connecting to wireless networks.
  o For example, when Bluetooth is on, select the “check with me before connecting” option to prevent automatic connections with other devices.
• Be careful when using insecure networks and use the Purdue VPN service to connect to campus resources. Most modern mobile devices are supported with proper configuration.

Application and Data Security
• Do not install software from unknown sources as they may include software harmful to your device. Research the software that you intend to install to make sure that it is legitimate.
• When installing software, review the application permissions. Modern applications may share more information about you than you are comfortable with, including allowing for real time tracking of your location.
• Be careful when storing your personal data on your mobile device. If you lose the device, you could lose your data.
• Follow the University’s “Data Handling Requirements” with respect to Purdue data stored on your mobile device.

Related References

University Data Classification Guidelines
• http://www.itap.purdue.edu/security/procedures/dataClassif.cfm

University Data Handling Requirements:
• http://www.purdue.edu/securepurdue/procedures/dataHandling1.cfm

End User Security Guidelines
• http://www.purdue.edu/securepurdue/bestpractices/endUserSecurityGuidelines.cfm
Security Incident information

Purdue’s VPN Service:
  - http://www.itap.purdue.edu/connections/vpn/

SecurePurdue website
  - www.purdue.edu/SecurePurdue