In A Nutshell…

Mobile Devices & Information Security

The use of mobile devices is rapidly increasing. In 2012, the number of smartphone users around the world topped 1 billion. In the U.S., the number of tablet users doubled from 2011 to 2012 with nearly 70 million users. Mobile devices can hold a lot of sensitive information, including account numbers, confidential work, passwords, etc. Although most of us understand the importance of protecting our computers, many of us don't understand the potential threats to mobile devices and how easily these devices can be misplaced or stolen.

How can I protect my mobile devices and the information on them?

- ☑ Make sure mobile devices (including USB drives) are locked with a password, PIN, or pattern security.
- ☑ Never leave mobile devices unattended. If there are times where devices must be left unattended, make sure to store them in a secure location.
- ☑ Make sure applications you install on your mobile devices are from trusted and reputable sources.
- ☑ Make sure to review mobile application privacy policies and be aware of what the applications access on your device.
- ☑ Make sure mobile device software is up to date.
- ☑ Avoid keeping personal and sensitive data on mobile devices and avoid sending that information via text or email.
- ☑ Install mobile security software to your mobile devices.
- ☑ Periodically back up your important data to another device.
- ☑ Be careful when using public Wi-Fi networks and avoid shopping and mobile banking unless you are certain you have a secure Wi-Fi connection.
- ☑ Avoid clicking on links and attachments in unsolicited emails and text messages.
- ☑ Turn off Bluetooth when not in use.
- ☑ Avoid using USB drives when you don't know who/where it came from.
- ☑ Disable the "autorun" feature from your computer. This will prevent removable devices such as USB drives, CDs, and DVDs from automatically opening and/or playing.
- ☑ If your mobile device supports data encryption, enable this feature.
- ☑ When you recycle or give up your mobile devices, make sure to erase all personal information from the device, SIM cards, and memory cards.

Negligent Employees Cause Most Data Breaches; Mobile Is Key Factor

In a recent data breach study, nearly 40% of organizations in the study had a data breach resulting from a lost or stolen mobile device, including tablet computers, smartphones, and USB drives that contained confidential or sensitive data.

Source: gov.aol.com, 3/22/2012

Where can I get more information?

USB Security	
IT Business Edge *"Ten USB Drive Security Best Practices"*	http://www.itbusinessedge.com/slideshows/show.aspx?c=92432
United States Computer Emergency Readiness Team (US-CERT) Security Tip (ST08-001): Using Caution with USB Drives	http://www.us-cert.gov/ncas/tips/ST08-001
Norton by Symantec *"New Security Risks from USB Flash Drives"*	http://us.norton.com/yoursecurityresource/detail.jsp?aid=usbdrives
Mobile Security	
Help Net Security *"Ten tips for mobile security"*	http://www.net-security.org/secworld.php?id=14158
IT Business Edge *"6 Tips for Better Mobile Security"*	http://www.esecurityplanet.com/mobile-security/6-tips-for-better-mobile-security.html
Stop.Think.Connect *"Safety Tips for Mobile Devices"*	http://stopthinkconnect.org/tips-and-advice/safety-for-mobile-devices/
Better Business Bureau *"BBB tips for securing your mobile device"*	http://www.bbb.org/blog/2013/02/bbb-tips-for-securing-your-mobile-device/
McAfee *"10 Quick Tips To Mobile Security"*	http://images.mcafee.com/en-us/advicecenter/pdf/MobileeGuide_Jan2012.pdf
Identity Theft Resource Center	http://www.idtheftcenter.org/smartphone%20home.html

Hawaii State Department of Education ◆ Data Governance Office
P.O. Box 2360 ◆ Honolulu, HI 96804
P: 808.218.6791 ◆ F: 808.440.2859
E: DGO@notes.k12.hi.us

Data Governance Office Websites
Public content
http://www.hawaiipublicschools.org/VisionForSuccess/SchoolDataAndReports/HawaiiDataSources/Pages/Data-Governance.aspx

Employee-related content
https://intranet.hawaiipublicschools.org/offices/dgo