Norse Secure

Laptop and Mobile Phone Safety Guide
September 2010

Laptops, smartphones, portable drives, etc. have made life easier in many ways, and they allow us to be productive when on the go. However, the freedom and mobility doesn't come without significant risks. Mobile devices are much more likely to be stolen than traditional desktop computers, and there are several security issues related to laptop and portable devices you need to be aware of, including:

- Physical protection of the device
- Prevention of data leakage
- Maintaining control of network connections
- Prevention of malware and viruses
- Smartphone security

Physical protection:

Think of your laptop as a stack of cash. To be more accurate – about $1500 or more. When you leave your office in the evening, would you leave your wallet lying on your desk? No. You want to lock your device in a secure cabinet, locked drawer, or if you take it with you, keep it in the trunk or other locked area - out of site when in transit. Within the past year, many NKU laptops have been stolen from locked offices, unlocked cabinets and drawers, and both locked and unlocked cars.

Prevent data leakage - use Identity Finder to Remove Sensitive Data and Encrypt Windows 7 systems:

While a stolen laptop in and of itself is an unfortunate occurrence, the often-related security breach is something that can easily be avoided.

NEW! 'Identity Finder' Software:

Don't let your system be the reason for a data breach at NKU -- sensitive information can't be breached if it doesn't exist! You may not realize the amount of data that has been collected within your system via attachments, spreadsheets, reports, word documents, etc. Often these files are long forgotten but still stored within the hard drive or your portable drives. Identity Finder can help you find, protect, and remove sensitive information on your Windows or Mac computer by:

- Searching your system or portable devices for unwanted and sensitive data
- Discovering – you may have SSN's, Credit Card, Passwords, etc. (and you don't even know it)
- Compliance - removing, masking or encrypting the data –keeping NKU data SAFE from a breach.

To find out more about how you can use Identity Finder on your system, visit our website or call x6911.

Encryption for Windows 7:

"Encryption" – simply means the information stored within the system is unreadable to anyone except those with proper access. Encryption will help keep data within systems secure and safe from breaches. Bitlocker is a Microsoft utility available with Windows 7, which encrypts the hard drive. Read more about it by clicking here. If you have a Windows 7 system, we STRONGLY encourage the use of encryption to keep data safe.

Maintain control over your connections:

Did you know that unsecured wireless traffic can result in a data breach? Sitting at hotspots for WiFi usage can be dangerous if you haven't taken security precautions. Keep your firewall turned on, keep antivirus up-to-date and scanning regularly, and be sure you use secure wireless – such as NKU_Encrypted when here on campus. If you do use an internet cafe, use the NKU VPN to access your network files, the internet, etc.

Prevention of malware, viruses and phishing:

- Malware is non-discriminate…it's like water finding a small crack and seeping in. If you have a vulnerable system and/or don't use caution – it will find you. Your best bet is to keep your operating system and anti-virus up-to-date and scanning regularly, use caution when visiting websites, clicking on unknown attachments, and use common sense when browsing the internet – especially social sites.
- Phishing has become quite sophisticated – so remember - NEVER SHARE YOUR PASSWORD AT ANY TIME, FOR ANY REASON. If you think something doesn't look right – call our IT Service Center at x6911, or forward the suspicious email to abuse@nku.edu.
- Social sites are breeding grounds for malware. For important safety tips see: www.ConnectSafely.com or http://www.microsoft.com/security/malwareremove/default.aspx.
- Many shopping and consumer sites have been invaded with fake links and malware which are often quite clever and convincing. Banking sites have also been spoofed. Be sure it is YOUR bank site before you enter your account information.

Know how to protect your SmartPhone:

Smartphone usage increased an estimated 64% from 2009 to 2010. But little thought is given to the security of these powerful mobile computing devices when using them to browse, check email or other computing needs.

- General safety tips from the National Institute for Standards and Technology can be found at: http://csrc.nist.gov/publications/nistpubs/800-124/SP800-124.pdf. Additional tips from PC Magazine: http://www.pcmag.com/article2/0,2817,2339121,00.asp
- Many states (including KY) have banned texting while driving. Use your phone wisely and don't text (or email) and drive!

For security information for several Smartphone types – click on the phone type:

- BlackBerry
- iPhone
- Droid "Mobile Defense"
- Windows Mobile

Make security a habit:

A dose of common sense and a few preventative measures will help keep your computing devices and data safe. (We hope we haven't made you too paranoid!) Use caution when traveling and keep your device within view or locked up at all times. Use your antivirus regularly; don't be careless when connecting from 'hotspots', and use caution when browsing the web from your computer or mobile device.

THANK YOU FOR DOING YOUR PART IN KEEPING NORSE SECURE!

For assistance: ***By phone:*** (859)572-6911 ***On the web:*** http://it.nku.edu/itsc/servicecenter.php

Also - bookmark the NKU IT Security site for more information, tips, guidance and policy updates.