# ON THE GO

## *Part 3: Understanding and reducing the security risks posed by the mobile construction workforce*

By Deb Canning

*In this final installment of a three-part series, Deb Canning, technical services manager for Computer Guidance Corporation, continues to describe the security risks and explains effective safeguards.*

***Physical security.*** As more mobile workers rely on laptops as their primary or only computers, the chances increase that more computers and peripherals will be lost, stolen, or damaged. Physical security is the first layer of protection. Identify who has direct physical access to employees' computers, and consider the following safeguards:

- *Computer locks:* Laptops must be kept in locked cases when traveling, and they should not be left unattended. Available devices include cable security kits, lockdown devices, and disk drive and case locks.
- *Power-on passwords:* Require users to set power-on passwords (i.e., the password is typed in when the PC or laptop powers on) to prevent unauthorized users from booting or logging onto computers.

***Password complexity.*** Passwords should always meet IT (information technology) industry complexity standards, and remind employees to password-protect files, folders, and screensavers.

Set security policies to mandate that all passwords must:

- *Contain eight or more characters*
- *Contain characters from two of the following three character classes:* alphabetic (a-z, A-Z); numeric (0-9); and punctuation/other characters (!@#$%^&*()_+|~-=\`{}[]:";'<>?,./).

However, passwords *must not* be:

- A form of the user-name
- Any word found in the dictionary, whether it is spelled forwards or backwards

***Security logs.*** Microsoft Windows, among other operating systems, is capable of automatically creating a security log that records computer activities. The types of entries that appear in a security log can be selected to conform with the corporate audit policy. The security log can be viewed in "Event Viewer," enabling corporate managers to analyze security events if they need to investigate malicious activities. Security logs are valuable in creating an audit trail that is useful both for computer troubleshooting and for tracking intrusions into the system. Therefore, it is advisable to require that mobile employees enable this feature, and to regularly collect security logs from them.

***Data backup.*** Valuable data can be lost as a result of a hard-drive crash, physical loss of a mobile device, and/or virus infection, among other causes. Therefore, it is important for all mobile professionals to regularly back up important data from their mobile devices. Prudent employees back up changed files daily and schedule a full weekly backup. Often, the most common reason for lost files is not theft or damage to mobile gear, but because backups have been neglected. Mobile professionals must commit to backing up critical data, including e-mail and address books.

There are several different methods for backing up mobile devices:

- *Software programs:* Options are third-party programs or those contained within the operating system. Many mobile professionals have great confidence in third-party programs, while others have found that the backup software included with their operating systems works well, so this choice is based on personal preference.
- *Copy to an external source:* Back up files to an external hard drive or server.
- *Disk cloning:* Copy the hard drive to another source, such as an external hard drive, CD, or DVD.
- *E-mail:* While this is not the most practical idea, it is very useful for backing up smaller files—especially if the hardware is in imminent danger of crashing.

***Firewalls.*** Microsoft Windows includes a basic firewall with every system, which is capable of performing the most important task required of a firewall: blocking bad packets of information from entering the system. Microsoft Windows users should enable the "Internet Connection Firewall" to protect their laptop when using Wi-Fi on the road.

***Antivirus software.*** Computer viruses are everywhere. Without proper antivirus software, a laptop is bound to become infected. Remember that antivirus software is a preventive measure. It is intended to be installed on a clean system, and to be used to prevent an infection from occurring later. Most good scanners will find and clean most viruses. Scanners, when kept current, and properly configured, should be able to find and detect most viruses encountered. Some viruses will do little else other than replicate, but others can adversely affect the performance of the system, and even cause severe harm.

In construction companies, this is of concern not only for files that are shared within the company, but also those that are shared among outside firms that are members of project teams, including architects, engineers, and subcontractors. Do not rely on another firm's virus protection to protect the company's IT system and data.

Common types of viruses include:

- *Polymorphic viruses:* These viruses encrypt or encode themselves in a different way, using different algorithms and encryption keys every time they infect a system.
- *Worms:* Worms are programmed in similar ways as viruses, and they have the ability to self-replicate, causing significant negative impacts on the system; however, these are usually detected and eliminated by antivirus software.
- *Trojan horses:* Although these are malicious codes, Trojan horses do not reproduce by infecting other files like viruses, nor do they self-replicate like worms.

Checking for viruses on laptops is probably the most important weekly maintenance task that mobile professionals should perform. It is extremely important that antivirus software be up-to-date in order for it to be effective, so users should schedule automatic updates and virus scanning.

## CONSTANT CHANGE

Increasingly, workers are on the go, playing an essential role in today's business environment. A mobile workforce offers a construction company the potential for increased employee productivity, business flexibility, responsiveness to customers—and profitability. However, the security risks associated with this unique operating environment and the potential for financial losses cannot be underestimated. That is why it is essential for financial managers to understand the risks and participate in initiatives to develop and maintain a reliable, secure IT infrastructure in an environment in which the only constant is change. ■

**ABOUT the AUTHOR**

Deb Canning is technical services manager for Computer Guidance Corporation, a Scottsdale, Arizona-based developer of financial and project management software solutions for the construction industry. She manages a technical support team and oversees installation of hardware and software, as well as internal IT efforts. She can be reached at 480.444.7000 or dcanning@computerguidance.com.