



Road Warriors – Keeping systems and data safe and secure while working remote

Laptops and netbooks, mobile and Wi-Fi Internet connections, remote access and VPNs – these are the daily tools of telecommuters, teleworkers and road warriors. The benefits this cutting-edge technology brings to the companies and employees are obvious, especially in terms of lowering costs and increasing productivity on a pace that follows a natural business flow and real time interactions.

But besides the undisputable advantages, the same technological boost is responsible for placing the off-site workers among the most exposed users in the IT&C world.

The current e-threats landscape already offers more than 2,000 new and mutated viruses per day, almost 50,000 phishing attempts per month and more than 1,000,000 hijacked computers that spread bots, rootkits, Trojans and other malware during one year. Adding to these cyber menaces, remote staff is also faced with the risks of laptop theft or data interception, while companies usually confront with intruders that attempt to access the corporate network posing as employees.

To safeguard and secure the integrity of remote systems, corporate network and business data, probably the best strategy is a multi-tiered approach that covers three main aspects: physical, connectivity and data.

The Physical Tier – Protecting Your Laptop

On one hand, laptops and netbooks are twice as expensive as the classical desktop solutions, especially because they include state of the art technology, designed to fulfill users' expectations in terms of computing power, storage, and connectivity.

On the other hand, they allow users to store and carry an entire workspace or office anywhere in this world. Laptops also hold this added value consisting in data and information employees store and update with each and every day of work, whether we talk about the latest business plan or the elaborate expenses report a manager expects by the end of the month.

For these two main reasons, laptops and their data are one of the most wanted prey for regular thieves. The following 10 simple rules and recommendations may prevent users from losing their systems and data stored within.

#1 Probably the simplest and cost effective way to secure a laptop is to use a security cable. Usually, thieves are looking for preys that are easy to catch (or, in this case, to detach).

#2 Label and tag your laptop and all its accessories, as well as removable peripherals.

#3 To prevent unauthorized access or laptop displacement, use motion sensors and alarms.

#4 When travelling, try to carry your laptop in a briefcase which does not hold the laptop

producer logo. Choose instead a bag or backpack with similar protection elements, but with a casual design.

#5 Avoid carrying your laptop when it is not really necessary. If possible, store the data you need on a CD, Flash Disk or memory card. Thus, you prevent laptop theft plus you can move around faster, saving time and energy. Plus, you could travel more freely, especially when you have to fly, avoiding a supplemental airport security check.

#6 Do not leave your laptop bag or briefcase locked in your car or in the car's trunk. Take it with you and watch it all the time.

#7 Same advice when you go shopping: do not leave your laptop unattended in your shopping cart while you choose products from the shelf; those few seconds you read a label are more than sufficient to lose it for good. In the worst case, use the store's lockers or luggage compartments or ask the store staff to deposit your laptop in a safe place during your visit.

#8 At the hotel or conference center, you can store your laptop in a safety-deposit or in the hotel/center vault.

#9 Subscribe to a laptop tracing and tracking service.

#10 If you are the victim of a theft, contact the authorities and provide a detailed description of the circumstances, while also specifying the exact laptop model and its features.

The Connectivity Tier – Protecting Your Network

Telecommuters, teleworkers and road warriors usually require the same level of access to resources and information as those back at the office. Whether we talk about connecting to the organization network from an Internet Café, a handheld device, mobile phone, home desktop or company laptop, the approach should consider three factors: users, policies and technology. Users should be aware that ensuring the security of their systems and the integrity of the corporate network is their responsibility too.

A decent policy should provide a clear definition of the current set of procedures for establishing a connection to the corporate network, while also specifying the access level for each user and the type of content that can be accessed, downloaded and uploaded.

Also, it should cover details about the security solution (antimalware, firewall, antispam, antiphishing or integrated defensive suite) that the organization adopted and the role that the user has in maintaining it as up-to-date as possible to prevent the corporate network from being compromised via e-threats.

In terms of technology, when establishing the connection with the organization's network the following 10 tips could be useful for preventing unwanted' access to business resources.

#1 Always make sure your antimalware and firewall are appropriately configured and turned on.

#2 Make sure you have disabled any files, folders and printers sharing.

#3 Do not install any program or application that might require resource sharing without the permission of your system and/or network administrator.

#4 Do not store within your laptop files containing user names, passwords, PINs or any other sensitive data which may grant access to your organization's network or resources.

#5 Refrain from employing a public unencrypted Wi-Fi access. If more reliable connections are not available, at least you should appeal to a combination of Wi-Fi Protected Access (WPA), anonymizers, as well as software but also hardware appliances that can provide encryption.

#6 When you are not using your Wi-Fi, turn it off to avoid attackers' potential intrusion.

#7 Ideally, you should use an encryption method which prevents file access as well as data interception. Ideally, a Secure Sockets Layer/Transport Layer Security (SSL /TLS) protocol

could provide enough security and data integrity for the Web-based communications over the Internet, such as the Web-based corporate e-mail.

#8 If you need access to the e-mail client, organization's database or other resources stored on the corporate network, you should employ an Internet Protocol Security Virtual Private Network (IP Sec VPN), which creates a secure tunnel and encrypts all digital traffic between the laptop and the network.

#9 Avoid typing sensitive personal information (such as user names and passwords, social security number, bank account or credit card numbers) and refrain from any on-line transactions from a computer in a public Internet Café, via unsecured Wi-Fi connections or using a system that is not protected by a reliable security and encryption solution.

#10 Avoid using your business laptop for personal purposes.

The Data Tier – Protecting Your Business Sensitive Information

Probably the most important asset any road warrior carries is the data he or she stores on his or her laptop. Ideally the data should be protected against malware, phishing, hijacking, hacking or other e-threats. The 10 hints that follow could help preventing valuable business information:

#1 Install and activate a reliable antimalware, firewall solution and spam filter. Update your antimalware, firewall and spam filter as frequent as possible, with the latest virus definitions and suspicious applications/files signatures.

#2 Scan your system frequently.

#3 Check on a regular basis with your operating system provider – download and install the latest securities updates, malware and malicious removal tools, as well as other patches or fixes.

#5 Do not open or copy on your computer any file, even if it comes from a trusted source, before running a complete antimalware scan.

#6 Use a system/domain password which contains more character types. A strong password should include a combination of at least 8 characters consisting of small letters, capitals, as well as special characters. Also, do not use the same password or similar passwords to log on to your computer and to access the corporate network, business e-mail or e-banking accounts.

#7 If you use Microsoft® Windows®, disable the Guest account and auto-logon option. Create access passwords for all the users registered within the same machine. Also, avoid using the Administrator account unless it is really necessary for system updates and special installations.

#8 If you do not use your laptop for a while, suspend the current session, either by locking your system or by logging off.

#9 Do not download and store business content onto public computers. You risk compromising your company interest and face a lawsuit for disclosing sensitive information.

#10 Avoid storing onto your laptop a large amount of sensitive business data for a longer time frame. Download them at least once a month onto a secure desktop system or transfer them on mobile storage media, such as CDs, DVDs, and Flash Disks etc. Also, periodically create backup copies for all the information and files you store on your laptop, on several media types (a DVD set and a Flash Disk).