Working Outside the Office

You can connect to firm data on a variety of devices and networks when working outside the physical office. Examples of these networks include client corporate office networks, home networks, and public Internet access points found in coffee shops, airports, or hotels, also known as Wi-Fi hotspots. Many of these connectivity options are convenient, but all expose the device to the possibility of malware and expose firm and client data to the possibility of breaches. These breaches include loss or theft of devices as well as interception of transmitted data from the devices. Whether on the move or static, critical data is a lucrative target for hackers.

Remote Access

The broad term “remote access” refers to connecting to the firm network in a manner that is not the method used when in the physical office, such as accessing the firm network from home or while at a client office.

Wi-Fi

H:\OnGuard\Images\eLearningMedia\wifi.pngWi-Fi is a type of wireless network most commonly associated with Internet access. Wireless networks can utilize varying degrees of security, ranging from no security to sophisticated encryption protections. Most public access points found in coffee shops and airports are ***not*** secure.

The term “**hotspot**” is often used to describe a public wireless network set up for Internet access. Its signal is broadcast publicly, and any device with a wireless card can access the Internet by connecting to this hotspot. Secure Wi-Fi requires a password to access the network. Many business offices, law firms, and hotels provide passwords to registered guests for secure access to their Wi-Fi networks. Without the use of encryption, data sent and received can easily be captured by another user on the same network who possesses basic, widely available interception tools.

Travel Concerns

When traveling around the United States and abroad, devices move through airports and other security checkpoints and can potentially access the Internet using public unsecure networks. Travel also increases the potential for device loss or theft. Foreign travel places individuals under the governing laws of another country where privacy and information access are often defined differently.

Best Practices for Working Outside the Office

* Familiarize yourself with firm policies on remote access and connectivity. Following firm procedures provides the best defense against unauthorized access to firm and client data. Keep device software updated to reduce the opportunities for security breaches.
* Use the preferred firm connection option to remotely access firm data.
* Use a password protected Wi-Fi network instead of an open network. Some open Wi-Fi networks are used by hackers to syphon people’s private information, using enticing names like “Free Public Wi-Fi”.

(Continued)

* Be aware of physical surroundings, and use caution when typing passwords or displaying confidential information onscreen. Decrease the risk of theft by limiting the use of devices in densely populated public areas.
* When traveling:
  + Know general laws of destination location in regards to security screening and surveillance;
  + Assume conversations are not private;
  + Transport devices in carry-on bags, not checked bags;
  + Disable device Wi-Fi and Bluetooth settings when not in use to prevent automatic network connecting or unauthorized data access;
  + Do not connect devices to portable storage devices;
  + Consider using temporary or “loaner” devices for the trip.