In this column for the March 2009 issue, we share sobering security advice from Mischel Kwon, who presented at the May 2008 SIM APC meeting at the invitation of APC member Skip Bailey, CIO of the DOJ’s Bureau of Alcohol, Tobacco, Firearms, and Explosives.

Mischel acknowledged that CIOs are already knowledgeable about IT security by virtue of their roles but may be less aware of the exploding growth of organized groups targeting individual executives. The primary interest of these national governments, organized crime, industrial spies, and terrorists is not bringing down a system; it is gathering information.

Seventy percent of an organization’s security budget is typically spent on compliance matters, but two of the biggest security protection gaps today are due to email and social site usage on the Internet. Mischel thus focused the majority of her talk on these types of security risks and actions that APC members and other executives can take to improve the security of their personal information. Here is a summary of her recommendations:

- Avoid surfing the net with the same computer used for company or personal business. Sports and social networking sites are notorious places for harboring keystroke logging malware. Once an individual clicks on one of these sites, a keystroke logger can access whatever is typed on a computer, such as passwords. One method of protection is to use a “virtual machine” every time one logs on to the Internet. While less user friendly than other forms of access, this software essentially cleans and reimages a computer every time it is used. “Cookies” are a good place to store malware, she noted. It is therefore best to erase them after every Internet use.

---

1 The Advanced Practices Council is an exclusive Society for Information Management forum for senior IT executives who value directing and applying pragmatic research, exploring emerging IT issues in depth, and sharing different perspectives with colleagues in other industries. Madeline Weiss is the APC Program Director and Blake Ives was the APC research director at the time of this presentation. The column was prepared with the assistance of Heather Smith, a Senior Research Associate for the APC.
• **Don’t preview attachments from people you don't know.** Phishing and Web site redirects have become considerably more sophisticated. Hackers will often send an email with an attachment that looks like it has come from a company insider, often from a company executive. Once the attachment is opened, malware is downloaded automatically. From a security point of view, previewing is the same as opening, and this type of malware is often not detected by virus checkers.

• **Delete personal identification information from your cell phone.** Cell phones should not be considered private, and users should have no expectation of privacy when using them, including text messaging. It is extremely easy to hack into a cell phone and obtain an individual’s home phone number, address and family names and photos. (Mischel illustrated this with a video that is available on the Internet.) If a company phone directory is on your cell phone, put only first names so that individuals cannot be traced if the phone is hacked or physically lost.

• **Ensure Bluetooth connections are in “non-discoverable” mode.** Most Bluetooth devices (e.g., Blackberries, cell phones, and in-car computers) are pre-set to “discoverable” mode, which enables a hacker to find and easily hack into them with their own cell phones. Once in, they have full access to all information on the device and can also make calls through others’ devices. If you need to be in “discoverable” mode for some activities, for example to connect, change the mode only for the few seconds needed to do this, and do not name the device with your full name.

• **Don’t assume hotel Internet connections are safe.** Even if there is a wall connector in a hotel room, chances are that hotel Internet connections are made wirelessly between floors. A hotel is really a huge, unprotected wireless cloud with wide-open connections, so treat everything you do online in a hotel as not private. Even encrypted networks, while safer, are not immune from attack.

• **Use a separate machine for personal business.** Doing online banking, online shopping, and filing taxes online must be a risk-based decision. If an executive does undertake these activities, different machines should be used for personal business (such as online banking) and for surfing the Net.

Never allow children to use your personal or business computer as they tend to be big users of the most commonly infected websites (e.g., Facebook, YouTube, and university sites). Furthermore, if a home router is used for wireless access, it should be less than two years old because earlier models have poor firewall protection. She also recommended turning the “file sharing” features of a computer off. Most new computers come with an infrared data access (IrDA) feature turned on, which effectively opens up any computer to the world; this access point can be covered with a small sticker.

• **Be careful with all movable computing devices and storage.** Never put an unknown USB device in your machine and never leave a laptop in a car or “asleep.” Even if a laptop is encrypted and password protected, it is relatively easy for a hacker to pick up passwords and files. Memory sticks can be used to quickly download key information simply by putting them in a USB port for a few seconds.

• **Use shields for all RFID-enabled cards.** Many organizations, such as Amex, the Passport Office, and hotels, are adding RFID chips to their cards and other documents to improve identification and authentication. However, these chips are very hackable from a wide range. Mischel illustrated this problem with a video showing how a dummy with an RFID-enabled passport could be targeted by terrorists and the chip used to trigger an explosive device. The best way to protect against this is to always use the shield provided or to disable the chip.