Compromising Business Behavior: How *Not* To Expose Your Company's Secrets

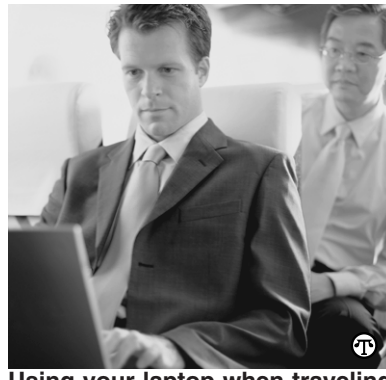
(NAPSA)—Everyday behaviors such as using your laptop at the airport or conducting a business call while walking down a crowded street can jeopardize your company's information.

"Most corporate intelligence losses aren't a result of high-tech crime," says Ira Winkler, president of the Internet Security Advisors Group and author of "Spies Among Us: How to Stop the Spies, Terrorists, Hackers, and Criminals You Don't Even Know You Encounter Every Day." "They're the result of human errors or system loopholes that can be remedied easily and cost-effectively."

Yet many small- and mid-sized companies remain vulnerable because they don't believe they're at risk. According to the Small Business Technology Institute, more than half of all small businesses in the U.S.—or as many as 13 million—experienced a security breach in the past year due to insufficient virus protection, employee manipulation (also called social engineering) or everyday behaviors that disclose business strategies unintentionally.

That's why Winkler teamed up with Office Depot to create a downloadable brochure, called "Compromising Behaviors: Don't Leave Your Business Exposed," with simple, affordable recommendations for protecting corporate information. Among the highlights:

• **Always use passwords and keep them safe.** Passwords are a simple way to protect your information but make sure to avoid basic passwords, like your name or phone number, that could be easily figured out by intruders. Do not write down your password, keep it in a secure location and do not share it. Trouble remembering passwords? The Microsoft Fingerprint Reader helps by eliminating the need for passwords entirely.



Using your laptop when traveling can pose security risks that can be remedied easily.

• **Be cautious when reading confidential information.** Reviewing documents when traveling or working outside the office can maximize your time, but you want to be sure important information is kept safe from prying eyes. One helpful solution: Use a laptop privacy filter like the 3M™ Notebook Privacy Filter, which darkens screen data from a side view—allowing only the user to view information on-screen.

• **Keep your PC and security software up to date.** Just like you put on your seat belt when driving a car, the most basic security protection for your PC is to make sure the operating system is up to date and utilizing the recommended security updates. Likewise, you should always install antivirus software, anti-spyware and a personal firewall to protect computer files. Keep your software updated, as new viruses and spyware bugs are released virtually daily. One protective software package is the Office Depot Internet Security Suite, which shields against viruses, spyware, hackers and phishing scams.

The entire security guide is available at www.officedepot.com/links/security.