Compromising Behaviors

Don't Leave Your Business Exposed

Office DEPOT

What Compromises Your Business?

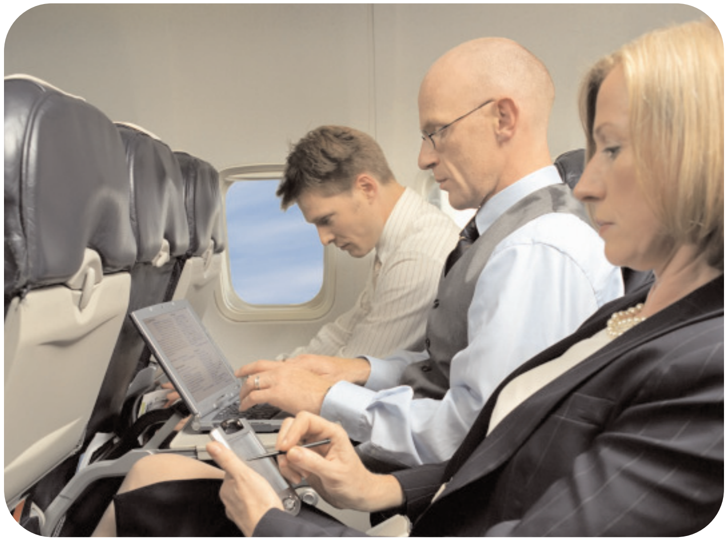
1

Can simple activities like leaving your computer on at night, working on your laptop at the airport or on the plane or even talking on your cell phone expose your company's confidential business information? The answer is a resounding "Yes!" In fact, these everyday activities are actually compromising behaviors that can leave your business vulnerable to security risks.

According to the FBI and recognized security organizations, industrial espionage costs U.S. companies between $24 billion and $59 billion annually. But, if you think this is only an issue for big companies to worry about, think again. Small businesses are just as vulnerable to security breaches as multinational corporations. According to the Small Business Technology Institute, more than half of all small businesses in the U.S. – as many as 13 million – experienced a security breach in the past year alone.

Today's security breaches are not just the result of high-tech computer hackers. In fact, it is the common, everyday behaviors that can also make businesses vulnerable.

That's why Office Depot has teamed up with **Ira Winkler**, one of the world's foremost security experts, to provide businesses with important, cost-effective and helpful solutions for keeping business information safe and secure. Throughout his career as a government agent, and now as a consultant to businesses of all sizes, Winkler has seen most security vulnerabilities occur as the result of human errors or system loopholes. Therefore, following a few basic guidelines will help any business ensure its company intelligence and information will remain secure.



Are You Security Smart?

2

Still not sure if your business is at risk? Then take the Office Depot Security Smarts quiz below and see how you measure up.

Office Depot Security Smarts Quiz

- □ Do you answer business calls outside of the office in public spaces?
- □ Do you work on a laptop outside the office and if so, does it have a privacy filter?
- □ Are your passwords stored in places that might be accessed by other individuals?
- □ Do you share passwords?
- □ Can your colleagues guess your passwords?
- □ Is your computer's virus protection software updated daily?
- □ Do you have a firewall on your PC?
- □ Do you have a security cable for your laptop to keep it attached to your desk or workspace?
- □ Do you log out of your computer before leaving work every night?
- □ Do you log out of your computer when going to meetings?

If you've checked one or more boxes, it's time to take a look at the basic behaviors that could compromise your business.

Helpful Security Solutions

From the Security Smarts quiz, it is apparent that different types of everyday behaviors can compromise a business. By following these tips and solutions from Ira Winkler and Office Depot, you can improve your Security Smarts to help defeat even the most tenacious snoops.

Stay Safe with Simple Security Precautions

3

Stolen laptops are not the only way people obtain confidential business information – they can also see what is on your computer screen and read the details over your shoulder if you are working in a public place like an airplane. Take these precautions to protect your information and computers when working both inside and outside the office.

□ **Use security software.** Every PC must have antivirus, anti-spyware and a personal firewall installed to protect your computer files from being compromised. Keep your software updated as new viruses and spyware bugs are released virtually every day. Like operating systems, security software can update itself automatically if it is set-up to do so. One protective software package is the Office Depot Internet Security Suite, which protects against viruses, spyware, hackers and phishing scams that may result in lost files, identity theft and poor computer performance.

□ **Back-up data regularly.** The most common way to lose data is by not backing it up on an external hard drive, a disk or using a mobile USB flash drive. Get into the habit of conducting regular data back-ups, such as nightly or weekly. When traveling, it's a good idea to store data in two locations, such as on a PC and on a USB flash memory drive. This way you always have a back-up of your business-critical documents.

□ **Always use passwords and keep them safe.** Passwords are a simple way to protect your information but make sure it's not the default password because hackers know those passwords. Do not write down your password, keep it in a secure location and do not share it. If you need to share your password, change it as soon as you can. If you have trouble remembering passwords, the Microsoft Fingerprint Reader could make life easier by eliminating the need for passwords. Simply log on to your PC and password-secure Web sites with the touch of a finger. Some laptops, such as the Toshiba P105-S6014 17-inch notebook, now come equipped with built-in fingerprint-reader based password-protection.

□ **Have a plan to recover your laptop if it's lost or stolen.** Register your laptop with the manufacturer and put the serial number information in a safe place so it can be reported to local law enforcement. One of the best ways to recover your laptop if it is lost or stolen is to utilize Computrace Lojack software.

□ **Be cautious when opening confidential information.** Reviewing documents when traveling or working outside the office can maximize productivity, but if the files include sensitive information, always make sure no one can see what you are working on. A good way to ensure your information remains safe from wandering eyes is to install a laptop privacy filter so only you can see the information. For example, the 3M™ Notebook Privacy Filter darkens screen data from a side view allowing only the user to view information on-screen.

□ **Put your laptop on lockdown.** Secure your notebook from theft by attaching a cable lock, which tethers it to a desk or other surface. Cable locks are portable and can go on the road so if you use a laptop at a business center, it can also be secured.

□ **Keep your PC's operating system up to date.** Just like you put on your seatbelt when driving a car, the most basic security protection for your PC is to make sure the operating system, like Windows, is up to date. This is first line of defense to keep your PC safe against hackers and other malicious individuals. An easy way to stay protected for Windows users is by activating the Windows Updates Service.

Office DEPOT

Stay Safe with Simple Security Precautions

Practice Safe Networking. If you are using wireless networking in your home or office, make sure that the set-up is secure. If it's easy for you to connect to your network without a password or with a default password, then it is also easy for a casual hacker to get onto your network and see the information being sent back and forth. Therefore, using passwords and other wireless protections, such as firewalls, are critical. Many wireless routers have built-in firewall and security to shield and protect your wireless communication from intruders. Make sure you use a model that ensures you can transmit sensitive information securely.

It is also necessary to be cautious while using wireless and other networking technologies in public places such as cafés, bookstores or airports. Be sure to disable wireless and Bluetooth functions on your computer while on an airplane or working in public because people with comparable Bluetooth connections can get access to your information. If you leave your wireless network card activated while traveling, your data can be stolen while you are sitting on a plane, in a hotel or elsewhere.

Always Remember that People Are Listening. While talking on your cell phone outside of the office, be conscious of your surroundings and keep your voice low whenever possible. Practice this same approach for business discussed in public spaces like a restaurant, coffee house or airport. While it's great to take a client out for a meal, an employee from your competitor could be sitting at the next table. If you need to talk business, consider using code words to discuss confidential projects.

Dealing with Dumpster Divers. One way snoops find out information about your company is by going through the trash and looking at documents that are left out on desks overnight. Make it a company policy to clean up desks before people leave at night so that sensitive information is stored safely and in locked cabinets.

If your business deals with confidential information, it's a good idea to shred it before discarding. For confidential discarding, use a diamond-cut shredder to cut documents and credit cards into tiny, unusable pieces, like the Ativa shredder.

Savvy Business Communication. The latest way that corporate spies are seeking information is by trying to get it from an unsuspecting employee. If a call is received from someone you do not know, first confirm their identity and why they need the information. Establish guidelines for dealing with information and how it can be communicated inside and outside of the organization.

Recommended Security Products

3M™ Notebook Privacy Filter: darkens the PC's screen so that only the user can view information on-screen.

Toshiba P105-S6014: this 17-inch notebook with built-in fingerprint-reader based password-protection.

Microsoft® Fingerprint Reader: could make life easier by eliminating the need for passwords. Simply log on to your PC and password-secure Web sites with the touch of a finger

Computrace Lojack software: a good way to help recover your laptop if it is lost or stolen.

Targus® Defcon Cable Lock for Notebook Computers: tether a notebook to a desk or other surface with a cable lock. These portable locks and can go on the road to use at a business center or other public space.

Office Depot® Internet Security Suite: Protect against viruses, spyware, hackers and phishing scams that may result in lost files or theft.

Ativa™ Shredder: shred anything containing confidential information before discarding.

Ira Winkler's Security Checklist

PC Security

- □ Install antivirus software on all PCs
- □ Install anti-spyware software on all systems
- □ Install personal firewall software on all systems
- □ Set software, including operating system and antivirus, to update automatically
- □ Back up all files at least weekly; back-up critical data more frequently
- □ Use surge protection power strips on all PCs
- □ Use uninterruptible power supplies on critical PCs
- □ Enable Windows Update Service on all PCs

Online Security

- □ Avoid browsing questionable Web sites
- □ Never click on the links in spam messages
- □ If you use wireless networking in your home or office, make sure it is secure
- □ Install Personal Firewalls on all PCs and an integrated firewall on a broadband connection

Password Security

- □ Never tell anyone your password – administrators will never need it
- □ If you do disclose your password, change it as quickly as possible
- □ Never write down your password
- □ Don't hide passwords around the office – if you can figure out where to hide something, someone else can figure it out too

Business Communication Security

- □ When disclosing any sensitive information to anyone, confirm their identities and their need for the information
- □ If you do not know the person you are talking to, check with their supervisors or the person whom the information is about when appropriate

Office Security

- □ Turn off computers at the end of the day
- □ Lock your offices when they are unoccupied
- □ Buy a combination lock box to store keys – don't just hide them in the office
- □ Do not leave sensitive information out in your office space
- □ Lock sensitive information at the end of the day
- □ Shred any information that may be sensitive
- □ Escort all visitors
- □ Lock all cabinets

Background

About Ira Winkler:

Ira Winkler is president of the Internet Security Advisors Group and is considered one of the world’s most knowledgeable security professionals. A former intelligence specialist at the National Security Agency (NSA), Mr. Winkler’s expertise extends to Internet security, information warfare, information-related crime investigation, and industrial espionage. Dubbed a “Modern Day James Bond,” he specializes in penetration testing, where he gains access to companies, both technically and physically, to find and repair an organization’s weaknesses. An accomplished author, Mr. Winkler's latest book, “Spies Among Us: How to Stop the Spies, Terrorists, Hackers and Criminals that you Don's Even Know You Encounter Every Day,” seeks to educate companies about their potential vulnerabilities and the cost-effective solutions.

About Office Depot:

With annual sales of over $14 billion, Office Depot provides more office products and services to more customers in more countries than any other company. Incorporated in 1986 and headquartered in Delray Beach, Florida, Office Depot conducts business in 22 countries and employs 47,000 people worldwide. The Company operates under the Office Depot®, Viking Office Products®, and Viking Direct® brand names.

Additional press information can be found at:
http://mediarelations.officedepot.com.
Broadcast quality B-Roll/Video (digital or tape) is available at www.thenewsmarket.com/officedepot.
Registration and video are free to the media.