



# Security Awareness Tips

## Physical Security

### **Lock your workstation before you leave your desk.**

Did you know there are keyboard shortcuts other than CTRL+ALT+DEL that you can use to lock your desktop? You can save a keystroke by using the following...

Windows Key+L

To make things even easier, create a desktop shortcut.

1. Right click any empty area of your desktop
2. Click New
3. Click Shortcut
4. Type in the following: `rundll32.exe user32.dll, LockWorkStation`
5. Click Next
6. Name your shortcut
7. Click Finish

Now it's as easy as a single click!

### **Don't leave thumb drives or other small devices lying around.**

Laptops and handhelds aren't the only things that can be stolen from your workspace. When not in use, thumb drives and other small devices (wireless cards, headphones, cell phones, etc.) should be stored in a safe place. At the very least, put them in a desk drawer so they're out of sight.

### **Control access to sensitive information.**

In today's workplace, most sensitive information (financial, personal, etc.) is stored in digital format. However, it's not uncommon for someone to print hard copies to take with them or to file away in their desk or office. When you send sensitive information to a printer, make sure you pick up the copies as soon as they are processed. Also try to adhere to a clean desk policy. Put away papers when your desk or office is unattended and when you leave at the end of the day.

### **Control access to buildings and work areas.**

Each one of us has a responsibility to ensure that our building is secure. When you enter the building from a side door or after hours, make sure the door closes properly and check to see that no one has slipped in behind you. If you see someone you don't know

wandering around, don't be afraid to ask which room they're looking for or who they're visiting. It's better to be safe than sorry!

### **Hackers aren't the only threat to your computer.**

Food and drink are common causes of computer damage. Try to keep them away from your computer and removable devices. Liquids can be especially damaging to laptops. If a spill occurs, you should clean up the mess as soon as possible.

[http://www.ehow.com/how\\_113592\\_clean-keyboard-spills.html](http://www.ehow.com/how_113592_clean-keyboard-spills.html)

[http://www.ehow.com/how\\_113626\\_clean-laptop-spills.html](http://www.ehow.com/how_113626_clean-laptop-spills.html)

## **Wireless Security**

### **Securing your wireless network – priceless!**

Laptop - \$1,000

Wireless router - \$100

Being able to be connected to the internet anywhere in your home without cables – priceless.

Or is it priceless? The manufacturer's default settings for wireless access points are typically wide open. This means anyone can potentially connect to your wireless network and use your bandwidth or maybe even gain access to your system(s). What can you do?

1. Configure your AP to at least use WEP (Wired Equivalent Privacy)
2. Don't broadcast the SSID.
3. Change the default SSID to something that doesn't easily identify your network (i.e. don't use your house or apartment number).
4. Change the default channel (which is usually 6 for 802.11 b/g networks) to 1 or 11.
5. Use a password/passphrase and make it strong.
6. Configure your AP to use MAC filtering.

### **Wireless Hotspots... should you connect?**

Because wireless hotspots are for open use, they don't provide much protection for your data. When using a wireless hotspot try to limit activity to web surfing only. You should also disable peer-to-peer networking, file sharing, and remote access. Always use a good personal firewall and of course make sure all your software including your OS is the updated and patched.

You shouldn't use hotspots for online checking, paying bills, or for making purchases that require you to give out confidential information such as a credit card number.

### **Turn off your wireless AP when it's not in use.**

Turn off your wireless access point when you know you won't be at home or when it's not in use. Your AP can't be accessed by hackers when it is not powered on. So, turn it off and limit the amount of time you leave yourself open to attack.

### **Encrypt data that's being sent over a wireless network**

To help protect your data when it's being sent over a wireless network, you should use some type of encryption. If possible, instead of WEP (Wired Equivalent Privacy) use WPA (Wi-Fi Protected Access). You can also use VPNs (Virtual Private Networks) to protect your data or IPSec (Internet Protocol Security). The drawback is that each of these require both the sending and receiving networks to be configured for this.

### **Know the range of your wireless access point.**

Wireless knows no boundaries. After setting up your wireless access point, make sure to test its range. See if you can connect to it from outside your home. If you can, someone else can too. (NOTE: Even if you can't connect, others may still be able to if they have a higher powered antenna.) Also remember to secure your AP with at least WEP (Wired Equivalent Privacy). This will keep the honest people honest.

## **Phishing**

### **How to spot a phishing email...**

It could be a phishing email if

- There are misspelled words in the e-mail or it contains poor grammar. This is especially apparent if the phisher's first language is not English and the text was translated by a computer or web site like Babel fish.
- The message is asking for personally identifiable information, such as credit card numbers, account numbers, passwords, PINs or Social Security Numbers.
- There are "threats" or alarming statements that create a sense of urgency. For example: "Your account will be locked until we hear from you" or "We have noticed activity on your account from a foreign IP address."
- The domain name in the message isn't the one you're used to seeing. It's usually close to the real domain name but not exact. For example: Phishing website: [www.regionsbanking.com](http://www.regionsbanking.com) Real website: [www.regions.com](http://www.regions.com)

### **Never respond to an email asking for personal information.**

Companies that you do business with will never ask for account information, credit card numbers or PIN information in an email message. If you have any questions about an email you receive that supposedly comes from your financial institution, call the local branch office. Do NOT respond to the email.

### **Never click on a link in an email message.**

The underlying code of a URL in an email message might not take you to the legitimate site. Example -- The URL says eBay.com but the underlying link takes you to a web site in China, Thailand or Brazil. If you want or need to visit a web site referenced in an email, type the URL yourself.

### **If you think you are a victim of identity theft, call the local police department and file a police report.**

Once you have a case number, you can call any of the three credit bureaus and have a fraud alert placed on your account. The fraud alert will last 90 days. The Federal Trade Commission has forms, checklists and other resources for you to use on their web site: <http://www.consumer.gov/idtheft/index.html>

Contact information for the three credit bureaus is:

Equifax: 1-800-525-6285; [www.equifax.com](http://www.equifax.com); P.O. Box 740241, Atlanta, GA 30374-0241

Experian: 1-888-EXPERIAN (397-3742); [www.experian.com](http://www.experian.com); P.O. Box 9532, Allen, TX 75013

TransUnion: 1-800-680-7289; [www.transunion.com](http://www.transunion.com); Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790

### **Review your credit report at least once a year.**

Everyone is entitled to one free credit report each year. You can order yours at: <https://www.annualcreditreport.com>

## **Online Security**

### **Remember that any email or instant message you send could come back to haunt you.**

Once you send an e-mail, it has a very good chance of being saved in someone's mailbox or archived on a server somewhere forever. How many e-mails do you still have from 1996? Here is a recent list of people who probably wish they could take back an email or two... Oliver North, Monica Lewinsky, Patricia Dunn (the former Hewlett-Packard chairman), Bill Gates, Harry Stonecipher (once Boeing's president and chief executive), Henry Blodget (the Wall Street analyst who predicted Amazon.com's stock price would skyrocket to \$400 per share in 1998).

Instant Messages can also be saved or archived and used at a later date to embarrass you. Former Rep. Mark Foley and Paris Hilton might be able to shed additional light on that subject. Just remember... be careful about what you put in writing and who you send it to.

You can find additional information on IM privacy through the following links.

AIM Privacy Policy

[http://www.aim.com/tos/privacy\\_policy.adp?aolp=0](http://www.aim.com/tos/privacy_policy.adp?aolp=0)

Yahoo! Privacy

<http://privacy.yahoo.com/privacy/us/mesg/>

Windows Live - Terms of Use

[http://tou.live.com/en-us/default.aspx?HTTP\\_HOST=tou.live.com&url=/en-us](http://tou.live.com/en-us/default.aspx?HTTP_HOST=tou.live.com&url=/en-us)

### **Stay safe when buying or selling online.**

Internet auction sites and online stores make shopping a breeze during the holiday season. But buying or selling merchandise online can have risks. Visit the following sites to learn more about keeping your online accounts and personal information secure and how to guard against fraud.

PayPal Identity Protection

<https://www.paypal.com/idprotection?ssPageName=CMDV:AB>

eBay Security & Resolution Center

<http://pages.ebay.com/securitycenter/?ssPageName=CMDV:AB>

### **If you download FREE software, make sure you don't get more than you bargain for.**

Free software that you download could be just what you think it is, a single software package. However, many times free software comes bundled with other unwanted, harmful programs including spyware, viruses, and worms. To help keep your computer free from unwanted guests, make sure the site you are downloading from is one you know and trust. Also verify that your operating system and anti-virus software have been updated and patched BEFORE you click the download button!

### **Email isn't the only online communication that has security risks.**

Instant Messaging has become a popular way for people to communicate over the Internet. In some instances it has even replaced email. What some people don't realize however is that instant messaging has many of the same security threats that email does... and then some. Instant messaging can transfer viruses and other malware, provide an access point for Trojans, and give hackers an easy way to find victims. If you use instant messaging

on a regular basis, you need to be aware of the security risks associated with it and take steps to protect yourself. Take the following quiz and see how safe you are.

[http://www.microsoft.com/athome/security/quiz/im\\_safety.aspx](http://www.microsoft.com/athome/security/quiz/im_safety.aspx)

See the following links for more on instant messaging safety.

[http://www.wiredsafety.org/safety/chat\\_safety/im/index.html](http://www.wiredsafety.org/safety/chat_safety/im/index.html)

<http://www.kidsturncentral.com/topics/computers/im5.htm>

[http://www.wiredkids.org/kids/personal\\_information\\_safety/im\\_safety/imclients.html](http://www.wiredkids.org/kids/personal_information_safety/im_safety/imclients.html)

<http://www.microsoft.com/athome/security/online/imsafety.aspx>

### **If you access the Internet from a shared computer, make sure you don't leave anything behind!**

Being able to access the Internet from different locations – the library, a computer lab at school, an Internet café – is a great convenience, but it can also pose a security risk to personal information. If you do access the Internet from a shared computer, here are a few things you need to remember.

1. Don't check the "remember my password" box.
2. When you're done, make sure you log off completely by clicking the "log off" button before you walk away.
3. If possible, clear the browser cache and history.
4. Never leave the computer unattended while you're logged in.

### **How "Security Aware" are you?**

We've reached the end of National Cyber Security Awareness Month. Do you believe you're a little more Security Aware? Can you identify the threats that exist in your environment and the steps you should take to avoid them? Take the following quizzes and find out.

Phishing [http://www.onguardonline.gov/quiz/phishing\\_quiz.html](http://www.onguardonline.gov/quiz/phishing_quiz.html)

Spyware [http://www.onguardonline.gov/quiz/spyware\\_quiz.html](http://www.onguardonline.gov/quiz/spyware_quiz.html)

Spam [http://www.onguardonline.gov/quiz/spam\\_quiz.html](http://www.onguardonline.gov/quiz/spam_quiz.html)

Online Shopping [http://www.onguardonline.gov/quiz/shopping\\_quiz.html](http://www.onguardonline.gov/quiz/shopping_quiz.html)

Wireless [http://www.onguardonline.gov/quiz/wireless\\_quiz.html](http://www.onguardonline.gov/quiz/wireless_quiz.html)

Identity Theft [http://www.onguardonline.gov/quiz/idtheft\\_quiz.html](http://www.onguardonline.gov/quiz/idtheft_quiz.html)

P2P File Sharing [http://www.onguardonline.gov/quiz/p2p\\_quiz.html](http://www.onguardonline.gov/quiz/p2p_quiz.html)

Online Auction [http://www.onguardonline.gov/quiz/auctions\\_quiz.html](http://www.onguardonline.gov/quiz/auctions_quiz.html)

Social Networking [http://www.onguardonline.gov/quiz/socialnetworking\\_quiz.html](http://www.onguardonline.gov/quiz/socialnetworking_quiz.html)