101 INTERNET SECURITY TIPS

KNOW HOW TO PROTECT YOUR COMPUTER ONLINE

Introduction

Richard Tong

Email

Recommended Resources

Web Site Hosting Service

Introduction

Using the Internet for business and leisure is a necessity in today's world. As the technology that allows you to work more efficiently on-line increases, techniques used by Internet criminals also adapts. While some on-line crimes are perpetrated only for the criminal to exert power by making your life miserable through damaging your computer, identity theft is a main focus for most Internet thieves. In addition to identity theft threats from hackers, computers can fall victim to viruses, spyware and phishing programs from Internet misuse. While you may think that high-profile or wealthy individuals are the common targets, most hackers are looking for any easy opportunity. The easiest opportunity, of course, is an unprotected computer. Your computer holds all of your most private personal and financial information, so proper security is a must to keep you and your files safe.

1. Activate protection systems.

If your operating system comes standard with a built-in firewall, spam blocker, anti-virus software or other security application, be sure that it's activated. Your Internet service provider may provide an e-mail spam filtering service that should also be turned on.

2. Upgrade your protection.

Using security software won't help if it's not up to date. Be sure that you are using the latest versions of spam, spyware and virus-detection software. The most current software will be ready to handle the most current on-line threats. Also remember to renew subscriptions if the software registration expires at some point.

3. Use anti-virus software.

You should always have anti-virus software on your computer. These programs scan all files that are downloaded from e-mail or opened from the hard drive to ensure that they are safe from malware before use. When these programs detect a virus, they are able to isolate and destroy it so it does not infect your computer.

4. Use anti-spyware programs.

Just like anti-virus programs, spyware protection is also necessary. These programs scan your computer for spyware, browser hijackers and other malicious programs. Both free and commercial anti-spyware products are available.

5. Update automatically.

Set both your operating system and security programs to update automatically. Your virus-detection software needs to adapt as new threats become known. Allowing the software to do automatic updates will ensure that you always have the highest level of protection

6. Use a secure browser.

If you use an older version of Windows, upgrade your browser to Internet Explorer 7 or Firefox 2. Both of these browsers have built-in features to detect on-line threats.

7. Block Pop-ups.

Set your Internet browser to block pop-ups from websites and advertisements. This will minimize spyware and the chances of clicking on an ad that loads malware onto your computer.

8. Install a security toolbar.

Toolbars with security features offer an additional line of defense. Most include features that block pop-ups, spam and known phishing sites. Some are even able to detect potential consumer scams.

9. Create User Accounts.

Create a user account that is separate from the default administrator account. Only log in as the administrator when making configuration changes to the computer. When the administrator account is used infrequently, the access to change configurations will be more limited to hacking. You may also want to create an individual user account for each member of the family who uses the computer. This will allow for each person to keep his or her information private.

10. Turn off your computer.

When you are not actively using your computer, shut down or disconnect from the Internet. If your computer is on-line less frequently, the chance of access by a malicious source decreases.

11. Lock your computer if you step away.

If you take a break from your computer for only a few minutes, it's enough time for a hacker to destroy or steal your information. Locking your computer password-protects your session until you return and prevents anyone else from physically or remotely accessing your information.

12. Be careful with public computers.

Avoid banking or conducting other personal business on public computers at libraries, hotels and airports. Not only could the on-line activity be intercepted, but strangers in the area could watch your activity and remember passwords and other personal details.

13. Consider Apple computers.

Since Windows personal computers are much more prevalent in the marketplace, most viruses and spyware is designed to penetrate Windows software. Mac owners still deal with spam and phishing issues, but the odds of virus attack is much less likely.

14. Be wary of downloads.

Free downloads are plentiful on the Internet, and the thousands of games, software and utility programs are very useful. Unfortunately, many of these freebies include malware and spyware. Try to download programs only from well-known manufacturers and trusted sites.

15. Consider a security suite.

If your operating system doesn't include security features or you want extra protection, a security software suite will include all the products required to keep your computer safe.

16. Run your antivirus software.

Simply having antivirus software installed will not help your computer from being attacked. Scan for viruses on a regular basis, or set the software to do automatic scans at a certain time daily.

17. Double your spyware protection.

Spyware can be difficult to detect, so it can be worth your while to use two different programs to search for spyware. Set the stronger program for constant monitoring, and use the second for occasional scans to verify that nothing was missed by the first program.

18. Try disposable e-mail addresses.

Create separate free e-mail addresses for different purposes. Use this ìdisposableî e-mail account to register for sites or complete surveys that may result in increased spam. If the spam becomes overwhelming, close the account and create another. This will keep the junk mail from your regular e-mail account, as you continue to use your regular e-mail address for business or personal communication.

19. Use credit cards.

When shopping on-line, credit cards offer higher protection than debit cards or other payment options. Credit card issuing banks offer protection against fraud that debit cards and checking accounts do not.

20. Devote a single credit card to online purchases.

If only one card is used for all online transactions, misuse or identity theft will be easier to detect than if multiple cards were used. Using a single card will also minimize the damage you experience if the card number is stolen.

21. Avoid saved passwords.

Although saved passwords and saved site default settings can be convenient, if your computer is hacked into any saved account information becomes available to the attacker. Limit the use of saved credit card numbers and addresses.

22. Look for evidence of secure sites.

Only enter personal information on sites that have the https:// prefix or a padlock icon in your browser window. This means that the Web site is secured and any information transmitted is encrypted and can not be read easily by humans.

23. Don't assume that secure and honest are the same thing.

The https:// prefix and padlock symbol are good indicators of transmission security, but not of reputation. Ensure that you shop from or do business with reputable companies by looking for the Better Business Bureau logo or other positive affiliations. Also read reviews on-line to find out what other users have experienced with the company.

24. Guard your personal information.

Do not respond to emails requesting personal information, like passwords, Social Security numbers and birthdates unless you know the sender or are expecting the email. If an email requests that you contact a telephone number, verify the number first.

25. Avoid clicking on hyperlinks.

Hyperlinks in email messages can be misleading, as the text shows one address but the link may take you to another. Before clicking on links in e-mails or Web pages, hold the cursor over the link and verify that the address that appears at the bottom of your browser window is the same one that you intend to visit.

26. Type with care.

On-line criminals often create Web sites that look similar to another site and use common misspellings of the original site as the URL. Be sure that you are typing accurately, or use a bookmark to visit favorite sites.

27. Report phishing.

Emails that appear to be legitimate and ask for information are forms of phishing. If you receive a phishing e-mail, forward it to the appropriate bureaus, including the Anti-Phishing Working Group (reportphishing@antiphishing.org) and the Federal Trade Commission (spam@uce.gov).

28. Review your accounts.

Look at your bank and credit card statements for suspicious or unknown transactions. These are often a signal of identity theft. Report these situations to your bank as soon as possible.

29. Practice the golden rule.

The Internet is a global community with many positive benefits. Just as in the real world, be responsible, safe and respectful towards others. Also respect any rules or laws that apply to your on-line activity.

30. Do not open unknown e-mails.

Delete any e-mails from unknown senders. Also be aware of email attachments and do not download attachments that you are unsure about, even if you recognize the sender. Do not forward unknown attachments to others.

31. Create strong, private passwords.

Choose password that would be hard for others to guess. Do not use obvious passwords like a name or birth date. Use a combination of letters, numbers and symbols in your password and do not share your password with anyone.

32. Use firewall protection.

Install firewalls to prevent hackers from gaining access to your computer. This will prevent theft of any personal information stored on the computer. You may choose an external or software firewall depending on your network needs.

33. Do not file share with strangers.

Sharing files can allow a stranger to look at files stored on your computer or plant a virus to infect the computer. Learn about the risks of file sharing, and learn how to disable file sharing on your operating system to prevent these risks. If a file sharing program is installed on your computer, be sure that it does not run automatically when you boot up your computer.

34. Back up your files regularly.

Make a back up of your hard drive onto an external media device. The act of making a back up copy does not offer protection, but it is insurance that nothing will be lost should a computer security disaster occur.

35. Protect your from power outages.

Use power strips and surge protectors to protect your computer against sudden power outages. During a storm when a power surge is likely, shut your computer down and unplug it to prevent any loss of information.

36. Evaluate your computer's security.

Review the security features and programs on your computer twice annually to be sure that everything is working as it is supposed to. Update or replace any programs as necessary. Do this process for all computers in your home.

37. Delete unused software programs.

Programs that you do not use take up valuable space in your computer's memory. In addition to wasting resources, rarely-used programs are usually not updated and may not have the security patches that could stop a hacker from accessing your computer.

38. Be wary of e-mail attachments.

Do not open email attachments from strangers unless the security and anti-virus software on your computer verifies that they are safe. Always delete any spam or junk email that contains an attachment.

39. Never open certain attachments.

Viruses are often sent as email attachments. Avoid opening any file with an extension that is .exe, .pif, .com or .bat, regardless of who they are from. These are almost always harmful files.

40. Don't click on pop-ups.

Many malicious sites use pop-ups that look very similar to the ones that your operating system may use to tell you that there is a security risk for your computer. These are ploys to get you to click on the ad; if you do click, the site usually installs spyware or malware on your computer. Close these ads by clicking on the X in the top right corner.

41. Be sure that your anti-spyware program is authentic.

Stick with anti-spyware products from reputable manufacturers. Unfortunately, some products marketed as free spyware detectors actually install spyware on your computer.

42. Read the license agreement.

Before installing any downloaded software, review its license agreement. Many free downloads come with spyware and programs that you would not want installed on your computer. Careful reading of the agreement can help you to find them.

43. Avoid pornographic Web sites.

The majority of spyware is distributed through pop-ups from pornographic sites. On-line gambling sites are also popular locations for adware and spyware.

44. Do not use unlicensed software.

Pirated software is illegal, and the sites that distribute it are often loaded with malware. This admonition goes beyond software, including crack key generators, and pirated music or movies. Unlicensed software is sometimes incompatible with patches and can be more susceptible to viruses. It may even come with viruses previously installed.

45. Run on-line virus scans.

In addition to running the anti-virus scan scheduled on your computer, occasionally run a free on-line scan to make sure you're your computer is not infected with something that your installed software is not aware of. Each program may find something that the other does not.

46. Visit Windows Update.

If you use Windows, visit Windows Update on a regular basis. The site will scan your computer for any updates or patches that are not installed on your computer. Then it will create a list of the items recommended to update your computer. Download anything marked as a critical update to keep your computer secure.

47. Password protect and encrypt sensitive files.

In addition to protecting the entire computer, you may want to encrypt or use passwords for certain files or folders that contain confidential information.

48. Visit Apple Security Updates.

If you are a Mac user, check the Apple Security Site for new updates and download them if they are available.

49. Protect your identity:

Personal information is all that an on-line criminal needs to begin stealing your identity. Be sure to keep your social security number, birth date, credit card numbers and address protected by limiting how you share the information on-line.

50. Protect your kids.

Children face many unique risks with Internet activity. Monitor your children's on-line activity and use parental filters or other tools to protect them from threats and security risks.

51. Disable scripts and active content.

Set your browser to prompt you when Javascript, Java or ActiveX controls are executed on a Web site. Malicious code is sometimes hidden in these features. Be sure that the site is trustworthy before enabling the content.

52. Be mindful of the information kept on portable USB drives.

Portable USB drives are a convenient way to store information, but their small size makes them easy to lose. Consider encrypting the data stored on these drives, in case of loss or theft. If you find someone else's USB drive, do not plug it into your computer. Hand it over to authorities instead.

53. Keep a log of sites visited.

Have children keep a list of any sites that they visit so you can review for potential spyware and other risks. Do not let children register with Web sites without permission.

54. Use a spam filter.

If your e-mail program separates spam and junk mail, use these features. This will filter away the scams and malicious messages so that there is no chance of accidental response or infection.

55. Be wary of strange messages.

Hackers and e-mail viruses can come in e-mails from recognized senders, so be aware of any strange e-mails, even if the sender's name is familiar. Examples of strange messages include attachments with odd file extensions or incoherent words in the message body. Treat these messages as you would ones from unknown senders and delete them immediately.

56. Change passwords regularly.

Changing passwords on a regular basis can help prevent criminals from accessing your personal information. Get in the habit of changing passwords every 90 days. Also change your password if you feel that there has been any type of security breach.

57. Stay informed. Subscribe to the National Cyber Alert System at www.us-cert.gov.

These updates will give you timely information about current Internet security issues. Knowing the risks is important to effectively protect your home and business computers.

58. Be cautious with chat and instant messaging.

Before divulging any personal information in a chat or IM message, be sure that you are communicating with who you expect to communicate with. To ensure that friends are not confused with strangers, you may want to create a password to help you recognize an on-line friend.

59. Forward spoof e-mails to verify.

Phising e-mails often claim to be from eBay, PayPal, or a familiar company name. If you are unsure of the e-mail's validity, forward it to the customer service department at the actual company the email claims to be from. They can confirm whether or not it is real.

60. Limit information given when registering for a Web site.

Although name and e-mail address are usually standard requirements for any site registration, some require more information, like address and phone number. Be cautious of which sites you give the information to. When possible only complete the required fields, often marked with an asterisk.

61. Be safe about meeting on-line friends in person.

If you decide to meet an on-line only friend in person, meet at a public place and tell other friends and family about your plans.

62. Protect friends' e-mail addresses.

To avoid sharing e-mail addresses of friends and family with spyware distributors and spammers, avoid using a site's ìrecommend to friendsî feature unless you are sure that the Web site is reputable.

63. Mark spam messages.

An e-mail spam filter will catch most spam and junk mail messages, but some may still get through. Train your e-mail service to recognize junk by marking junk mail messages in your inbox as spam. The e-mail service will know to direct similar messages to the spam folder in the future.

64. Read the fine print.

Review the terms and conditions for any site you register with. Most have a checkbox for whether you would like to receive updates and offers from sponsors. Be sure that this box is left unchecked, or you could end up receiving lots of junk mail and spam. Most reputable sites include a statement explaining that they do not sell or share your e-mail address with other companies.

65. Be careful about what you share with others.

Don't say anything on-line that you would not tell anyone you never met. This is especially important for social networking sites, like Twitter or Facebook. Be sure not to divulge addresses of where you are or full names of who you are with. Too much information can be an invitation for a stranger to show up at your location.

66. Practice caution with Out-Of-Office responses.

An automated response explaining that you are unable to check emails on vacation can be helpful, but it also acts as an advertisement that you are away from your computer and/or your home. If possible, modify the Out-Of-Office response settings so the response is only sent to existing members of your e-mail address book. Don't be too specific about the details of where you are and why you won't check your e-mail; leave the message simple and secure.

67. Know who is watching you.

Be careful about your e-mail and Internet activity at work. In most of the United States, any activity conducted on a work computer is property of the employer. Not only could inappropriate activity result in work-related disciplinary action, but you could end up divulging personal information to strangers at your place of business.

68. Beware of public Wi-Fi access.

Don't send or view confidential information when using public wireless connections. Other wireless users in the same location could monitor network activity and see what you are doing.

69. Minimize chances of mobile device theft.

Don't advertise that you have a laptop by using it in public. Consider using a non-traditional laptop carrying case and an alarm or lock to add additional security.

70. Always log off of secured sites.

When using on-line banking or other password protected sites, be sure to log off when finished and close the browser window. This ensures that the session is closed and information can not be viewed by others. This is especially important if you are using a public computer.

71. Clear your cookies frequently.

Cookies are the way that Web sites store personal information. Not all cookies are bad, but some companies sell this information to other companies for marketing purposes. You can delete unnecessary cookies through the Internet options section of your browser.

72. Secure mobile connections.

When using Wi-Fi, hot spots or Internet cafes, be sure that webmail is secured with the https:// prefix. Also be aware of those around you who may watch you type passwords or other personal details.

73. Secure your home wireless connection.

Make sure that your home WiFi connection is password-protected so no one can access your connection, even if they are in signal range.

74. Remember physical security.

All the security precautions in the world will not protect your computer if it is physically vulnerable to theft. Always keep your laptop in sight when travelling. If a private computer is kept in a home with roomates or family members, consider locking the door to the computer room when you are not around.

75. Watch for security cues.

Secured sites should change from the http:// prefix to https:// or shttp:// at the moment when you are prompted to type in a user name and password.

76. Review your credit reports.

Each consumer is entitled to a free copy of his or her credit report each year. Order copies of credit reports from the three reporting bureaus annually, and review for incorrect information or unfamiliar accounts. Dispute any errors immediately.

77. Use separate computers for leisure and personal business.

If possible, stop Web surfing on the computer that you use for on-line banking or shopping. This will limit the amount of cookies, spyware and monitoring and can reduce the incidence of identity theft.

78. Be aware of cyberstalking.

Cyberstalking is on-line harrassment, including threatening e-mails, identity assumption and on-line defamation of character. If you believe you are a victim of cyberstalking, your Internet service provider should be able to assist you in finding the perpetrator.

79. Be safe on social networking sites.

Use the privacy settings on social networking sites to keep your personal details secure. Make information like your last name, e-mail address and phone number invisible to anyone except for people you know and approve. Do not allow the site to automatically accept friend requests. Instead, approve each request personally.

80. Keep sensitive information out of chat rooms.

Even if you are talking with someone in a private chat room, chat services often archive conversations on a server. You have no control over what happens to archived conversations. Even if you feel that everything is secure on your end, remember that you don't know if the person you are chatting with has someone watching his or her interactions with you.

81. Browse with care.

Be cautious about the Web sites that you visit, and if a site seems suspicious, close your browser and leave the site. Most Web sites are able to track bits of information from your computer, like IP address and the software that you use, for marketing purposes. While this information collection is not necessarially harmful from trustworthy sites, Web sites that seem less legitimate can use this information for malicious activity.

82. Change Wi-Fi administrator passwords.

Most Wifi routers come with a generic username and password for equipment setup. Although password-protected, this information is not specific to the individual and therefore well known to hackers. Change the username and password as soon as your wireless network is set up.

83. Enable WPA/WEP encryption.

All WiFi equipment supports encryption to protect information sent over wireless networks. Choose the strongest encryption option that works with your network. It may require synchronizing the encryption settings on all Wi-Fi devices that you and your family use.

84. Change the default SSID name.

Wi-Fi access points and routers use a network name called the SSID, and routers often have a default SSID of the manufacturer name. Using the generic SSID does not make your wireless network more susceptible to threats, but it is a sign to others that the network is poorly configured, making it more of a target. Shange the default SSID name immediately when configuring your wireless security.

85. Allow MAC address filtering.

Each Wi-Fi component has a unique identifier called the MAC address, and access points and routers keep tabs on all the MAC addresses of devices that connect to them. Many products allow the owner to type in the MAC addresses of his or her equipment, so the etwork will only allow connection from those approved devices.

86. Disable SSID broadcast.

Access points and routers usually broadcast the SSID name at regular intervals. This function was originally intended for roaming, but it is unnecessary when a wireless network is used in the home. Disable the broadcast so others will not be able to see your network.

87. Disable Wi-Fi auto-connect.

Most computers have a setting to allow the computer to connect to any open wireless network. Disable this setting and always connect directly to your home network. Use the auto-connect if necessary during temporary situations, like when travelling.

88. Assign fixed IP addresses to wireless devices.

Turn off DHCP and assign a static IP address to your computer. Although DHCP is easier to onfigure, it is also easier for hackers to find IP addresses and intercept. Use a private range for the IP address so the computer is not vulnerable to being reached from the Web.

89. Enable the firewalls on your router.

In addition to a firewall on your computer, make sure that your wireless router's firewall is turned on. This will offer an additional level of protection for your home wireless network.

90. Position the router appropriately.

Home Wi-Fi signals are intended to be used in the home. While some signal may leak outdoors, keep an eye on how far the signal reaches. The position of the router determines how far the signal will reach, so try to place the router in the center of the home to prevent the signal passing across streets or into different neighborhoods.

91. Shut down your network when it is not being used.

While it isn't practical to turn off a wireless network daily, be sure that it is disconnected if you plan to be gone on vacation or extended off-line periods.

92. Use third-party payment services.

When shopping online, use a third-party service to pay. These services, like PayPal and Amazon Payments, seamlessly transfer money from a bank account to the vendor without the need to expose your bank or credit card information to the seller.

93. Watch out for e-mail hoaxes.

If it's too good to be true, it probably isn't. Be cautious of any easy money scams, like promises of lottery winnings or requests to move money from a foreign country. These scams usually ask that you send money or personal information to sign up for the opportunity. Steer clear of these hoaxes.

94. Beware of virus hoaxes.

Sometimes e-mails that inform of a security risk are malicious or intended to create panic. Always verify before you act or share the information. Check with McAfee or F-Secure to see if the virus described is a hoax before you take any action.

95. Avoid Bots.

Not everyone in a chat room is an actual person behind a keyboard. Chat robots, or bots, are often used to moderate chat rooms and provide news or weather updates. Malicious bots can be set up to infiltrate your computer.

96. Take precautious with smartphones.

Use the same precautions accessing your smartphone in public as you would any other public computer. Avoid on-line banking in busy public spaces because strangers could shoulder-surf to watch what you type. Also consider disabling the feature that allows the phone to automatically connect to any open wireless network.

97. Encrypt Internet phones.

Voice over IP (VOIP) is a way of communicating by voice over public internet connections, so a risk of eavesdropping is always present. Choose a VOIP provider that offers secure encryption services.

98. Erase data from unwanted computers.

Before tossing out an old computer, copy all the data tha you need to keep and erase the hard disk. Simply deleting files is not enough. Use a program to erase all traces of personal data from the computer before recycling or donating.

99. Assume permanence.

The Internet does not have a delete button. If you post or publish any information and then delete it, you maintain no control over how it is copied, stored or archived. Think before you post anything that you may regret later.

100. Be cautious of links or attachments from chat messages.

Although you may feel comfortable with a person that you share conversations with in a chat room, if you do not really know the person, you can not be sure of his or her intentions. Avoid clicking on any links or opening attachments from a chat buddy that you do not know very well. This is a common method for hackers to distribute malicious material directly.

101. Know what to do if something is wrong.

If you suspect that malware is affecting your computer, stop any on-line activities that involve usernames, passwords or other personal information. Scan your computer with an anti-virus software, and delete anything that the program finds to be suspicious. If the problem is not resolved call for professional technical help from a repair shop or manufacturer.