Protect Yourself: Computer Security

How to Protect Your PC from Identity Theft

Making sure your computer is protected is a crucial step to protecting your identity. The best place for a thief to look is in through a computer where personal information is stored. If you set up as many safeguards as possible, making it more difficult for an imposter to access your personal data, then it will be more likely that they will simply give up.

1. **Get an Antivirus Program:**
   
   a. An antivirus program is designed to search for, prevent, detect and remove software viruses. You can purchase different antivirus software that can:

      - Schedule scans to automatically run for you
      - Initiate scans of specific files, flash drives or CDs at any given time
      - Scan certain directories or files for known malware patterns
      - Display the “health” of your computer
      - Remove malicious codes that were found

2. **Use a Firewall:**
   
   a. A firewall is a piece of hardware or a software program that helps keep out viruses, worms and hackers from your computer from over the Internet. Microsoft recommends protecting every computer if you have more than one connected at home or in an office network.

   b. Consumers should have a hardwire firewall to protect your network (e.g. a router) and a software firewall for each computer. Both forms of protection help stop a spread of a virus to your whole network if one of the computers becomes infected.

3. **Keep Windows Operating System (OS) Updated:**
   
   a. Updates from Microsoft are important and used to fix any security holes that could be present in the OS. Using updates keeps your system up to date and installs the latest security functions.

   b. If you let your operating system, web browser, or security software get out-of-date, criminals could sneak their bad programs – malware – onto your computer and use it to secretly break into other computers, send spam, or spy on your online activities.

   c. Don’t buy security software in response to unexpected pop-up messages or emails, especially messages that claim to have scanned your computer and found malware. Scammers
send messages like these to try to get you to buy worthless software, or worse, to “break and enter” your computer. You can check to see if your computer is up to date by:

- Clicking Start and then All Programs and selecting Windows Update
- On the left side, select Check for Updates
- If any updates pop up, click Install Updates
- Proceed to enter in the appropriate password if asked

(1) Steps to set up automatic updates for Windows:

- Open Microsoft Internet Explorer internet browser
- On the right side of the page, Internet Explorer will display the current status of the update if it is already set up
- If it is not already set up, click Turn on Automatic Updates
- In the window, select OK

4. **Password-Protect Guest Accounts**:

   a. PC’s generally allow you to have accounts, one for the main administrator and one as a guest account. Set up a password for all accounts, even the guest one. You don’t want someone to log onto the guest account and set a password so you no longer have access to it. This can easily provide extra precautions to your PC.

5. **Encrypt Sensitive Information**:

   a. Encrypting your information makes it harder for hackers to access, gain and copy data. Ensure you give personal information over encrypted websites only.

   (1) If you’re shopping or banking online, stick to sites that use encryption to protect your information as it travels from your computer to their server. To determine if a website is encrypted, look for https at the beginning of the web address (the “s” is for secure).

   (2) Some websites use encryption only on the sign-in page, but if any part of your session isn’t encrypted, the entire account could be vulnerable. Look for https on every page of the site you’re on, not just where you sign in.

   (3) Windows allows you to encrypt or decrypt folders or files by:

   - Right-clicking the desired file or folder to encrypt
   - Select Properties
   - Click on the General tab and select Advanced
   - Check the box that is labeled Encrypt contents to secure data
   - To decrypt, uncheck this same box
   - Select OK
6. **Back Up Your Files:**

   a. No system is completely secure. Copy important files onto a removable disc or an external hard drive, and store it in a safe place. If your computer is compromised, you’ll still have access to your files.

7. **Use Strong Passwords and Change Them Regularly:**

   a. Strong passwords are necessary for any type of electronic devices, not only PCs.

   b. Here are a few principles for creating strong passwords and keeping them safe:

      (1) The longer the password, the tougher it is to crack. Use at least 10 characters; 12 is ideal for most home users.

      (2) Mix letters, numbers, and special characters. Try to be unpredictable – don’t use your name, birthdate, or common words.

      (3) Don’t use the same password for many accounts. If it’s stolen from you – or from one of the companies with which you do business – it can be used to take over all your accounts.

      (4) Don’t share passwords on the phone, in texts or by email. Legitimate companies will not send you messages asking for your password. If you get such a message, it’s probably a scam.

      (5) Keep your passwords in a secure place, out of plain sight.

---

**Cookies: Leaving a Trail on the Web**

*Understanding Cookies*

1. **What is a cookie?**

   a. A cookie is information that a site saves to your computer using your web browser. A cookie allows sites to record your browsing activities – like what pages and content you’ve looked at, when you visited, what you searched for, and whether you clicked on an ad.

   b. Data collected by cookies can be combined to create a profile of your online activities.

2. **Who places cookies on the web?**

   a. **First-party cookies** are placed by a site when you visit it. They can make your experience on the web more efficient. For example, they help sites remember:
- items in your shopping cart
- your log-in name
- your preferences, like always showing the weather in your home town
- your high game scores.

b. **Third-party cookies** are placed by someone other than the site you are on. These may include an advertising network or a company that helps deliver the ads you see. They may be used to deliver ads tailored to your interests.

---

**Controlling Cookies**

1. **Controlling Cookies:**

   a. Various browsers have different ways to let you delete cookies or limit the kinds of cookies that can be placed on your computer. When you choose your browser, you may want to consider which suits your privacy preferences best.

   b. To check out the settings in a browser, use the ‘Help’ tab or look under ‘Tools’ for settings like ‘Options’ or ‘Privacy.’ From there, you may be able to delete cookies, or control when they can be placed. Some browsers allow add-on software tools to block, delete, or control cookies. And security software often includes options to make cookie control easier.

   c. If you disable cookies entirely, you may limit your browsing experience. For example, you may need to enter information repeatedly, or you might not get personalized content or ads that are meaningful to you. However, most browsers’ settings will allow you to block third-party cookies without also disabling first-party cookies.

2. **Keep your Browser Up-to-Date:**

   a. No matter which browser you use, it’s important to keep it updated. An out-of-date browser can leave your computer vulnerable to attack by malware, which could intercept sensitive data like your log-ins, passwords, or financial information. Most browsers update automatically, or prompt you to update to the latest version.

3. **“Opt-Out” Cookies:**

   a. Some websites and advertising networks have cookies that tell them not to use information about what sites you visit to target ads to you.

   b. There are a couple of ways to opt out of certain types of data collection or certain kinds of targeted advertising:

   c. You can download software – an “add-on” to your browser – that controls whether and how cookies – including opt-out cookies – are stored or deleted. You can find add-ons on sites sponsored by the browser. Look through the settings or “Help” function. Browser companies
review most add-ons for security and functionality before making them available for download, but as with any software, don’t download an add-on unless you have checked it out and trust the source.

d. Programs from the online advertising industry, including The Network Advertising Initiative and the Digital Advertising Alliance, offer tools for opting out of targeted advertising – often by placing opt-out cookies – offered by their members. You also can opt out by visiting advertising networks and advertiser websites one by one.

e. Deleting all your cookies will erase any opt-out cookies you’ve downloaded. To restore opt-out cookies, you will have to go through the opt-out procedure again.

“Private Browsing”

1. “Private Browsing”:

   a. Many browsers offer private browsing settings that are meant to let you keep your web activities hidden from other people who use the same computer.

   b. With private browsing turned on, your browser won’t retain cookies, your browsing history, search records, or the files you downloaded. Privacy modes aren’t uniform, though; it’s a good idea to check your browser to see what types of data it stores. Although it won’t keep cookies after the private browsing session ends, cookies used during the private browsing session can communicate information about your browsing behavior to third parties.

Flash Cookies

1. **What are Flash Cookies?:**

   a. A Flash cookie is a small file stored on your computer by a website that uses Adobe’s Flash player technology.

   b. Flash cookies use Adobe’s Flash player to store information about your online browsing activities. Flash cookies can be used to replace cookies used for tracking and advertising, because they also can store your settings and preferences. When you delete or clear cookies from your browser, you won’t necessarily delete the Flash cookies stored on your computer.

2. **Controlling Flash Cookies:**

   a. The latest versions of Google Chrome, Mozilla Firefox, and Microsoft Internet Explorer let you control or delete Flash cookies through the browser’s settings. If you use an older version of one of these browsers, upgrade to the most recent version, and set it to update automatically.
b. If you use a browser that doesn’t support deleting Flash cookies, look at Adobe’s Website Storage Settings panel. There, you can view and delete Flash cookies, and control whether you’ll allow them on your computer.

c. Like regular cookies, deleting Flash cookies gets rid of the ones on your computer at that moment. Flash cookies can be placed on your computer the next time you visit a website or view an ad unless you block Flash cookies altogether.