US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Ten Ways to Improve the Security of a New Computer

Jennifer Kent and Katie Steiner

Why Should I Care About Computer Security?

Our computers help us stay connected to the modern world. We use them for banking and bill paying, shopping, connecting with our friends and family through email and social networking sites, surfing the internet, and so much more. We rely so heavily on our computers to provide these services that we sometimes overlook their security. Because our computers have such critical roles in our lives and we trust them with so much personal information, it's important to improve their security so we can continue to rely on them and keep our information safe.

Attackers can infect your computer with malicious software, or malware, in many different ways. They can take advantage of unsafe user practices and flaws in your computer's programs (flaws including vulnerabilities and unsecured services and features) and use social engineering (in which an attacker convinces someone to perform an action such as opening a malicious email attachment or following a malicious link). Once your computer is infected, intruders can use the malware to access your computer without your knowledge to perform unwanted actions. They can steal your personal information, change computer configurations, cause your computer to perform unreliably, and install even more malware they can use to leverage attacks or spread malware to others.

One of the most well-known attacks was the Conficker malware detected in late 2008. This malware grew to become one of the largest malware infections, affecting millions of computers and causing billions of dollars in damage across the world. The Conficker malware had the ability to steal and relay personal information to attackers, disable existing security measures like Windows Automatic Updates and antivirus software, and block internet access to popular security websites. Attackers could use infected computers as part of a botnet, or a collection of compromised computers connected to the internet, to leverage additional attacks against other computers. The Conficker malware took advantage of three separate security flaws on Microsoft Windows computers: the enabled file sharing service, the default AutoRun setting, and a vulnerability in the Windows Server network service. If people had used the following ten practices, the risk of infection of Conficker would have been significantly reduced.

How Do I Improve the Security of My Home Computer?

Following are ten important things you can do to make your home computer more secure. While no individual step will completely eliminate your risk, together these practices will make your home computer's defense strong and minimize the threat of malicious activity.

1. Connect to a Secure Network

Once your computer is connected to the internet, it's also connected to millions of other connected computers, which could, in turn, allow attackers to connect to your computer. Information flows from the internet to your home network by first coming into your modem, then to your router, which most people have, and finally to your computer. Because your modem doesn't have security settings, it's crucial to secure your router—the first securable device that receives information from the internet. Be sure to secure it *before* you connect to the internet to improve your computer's security. If you don't have a router, contact your service provider to learn how you can best secure your network.

The default configurations of most home routers offer little security. Though it may seem cumbersome to spend time configuring your router's settings, it's well worth it because a secure router is one of the best initial lines of defense. To secure your router, consult its user's guide, which will direct you to a predefined URL or IP address where you can do the following:

- Configure the wireless network to use WPA2-AES encryption for data confidentiality.
- Change the default login username, if permitted (refer to the user's guide), and password. (The default passwords are published in manufacturer's publications and are readily accessible.)
- Conduct MAC address filtering (a form of whitelisting, or identifying wirelessly connected computers you trust).
- Change the default wireless SSID.

Learn more about each of these configurations and others in the document "Small Office/Home Office Router Security" (http://www.us-cert.gov/reading_room/HomeRouterSecurity2011.pdf).

2. Enable and Configure a Firewall

A firewall is a device that controls the flow of information between your computer and the internet, similar to a router. Most modern operating systems include a software firewall. In addition to the operating system's firewall, the majority of home routers have a firewall built in. Refer to your user's guide for instructions on how to enable your firewall. Once your firewall is enabled, consult the user's guide to learn how to configure the security settings and set a strong password to protect it against unwanted changes.

3. Install and Use Antivirus and Antispyware Software

Installing an antivirus and antispyware software program and keeping it up to date is a critical step in protecting your computer. Many types of antivirus and antispyware software can detect the possible presence of malware by looking for patterns in the files or memory of your computer. This software uses virus signatures provided by software vendors to look for malware. New malware is discovered daily, and vendors frequently make new signatures available, so

antivirus software will be most effective if the signatures are up to date. Many antivirus and antispyware programs offer automatic updating. Enable that feature so your software always has the most current signatures. If automatic updates aren't offered, be sure to install the software from a reputable source, like the vendor's website or a CD from the vendor.

4. Remove Unnecessary Software

Intruders can attack your computer by exploiting software vulnerabilities (that is, flaws or weaknesses), so the less software you have installed, the fewer avenues for potential attack. Check the software installed on your computer. If you don't know what a software program does and don't use it, research it to determine whether it's necessary. Remove any software you feel isn't necessary after confirming the software is safe to be removed.

Back up important files and data before removing unnecessary software in case you accidentally remove software essential to the operating system. If possible, locate the installation media for the software in case you need to reinstall it.

5. Disable Nonessential Services

Like unnecessary software, nonessential services increase the opportunities for attack. Two services to look for are file sharing and print sharing, which enable you to share files, such as photos and music, with other computer users and print to other computers on your network. The Conficker malware used file sharing to infect computers and spread the infection to others. Disabling file sharing would have eliminated one of the ways Conficker infected computers at the time of the Conficker malware infection.

If those services are enabled in your operating system, disable them if you only have one computer connected to your network or don't use them. Because services differ depending on your operating system and many of them are critical to your computer's operation, research any services you aren't sure about or don't use before disabling them.

6. Modify Unnecessary Default Features

Like removing unnecessary software and disabling nonessential services, modifying unnecessary default features eliminates opportunities for attack. Review the features that came enabled by default on your computer and disable or customize those you don't need or plan on using. As with nonessential services, be sure to research these features before disabling or modifying them.

The AutoRun feature in Microsoft Windows systems was a default feature at the time of the Conficker malware and was one of the three ways computers became infected. When the AutoRun feature is enabled on Windows computers, Windows detects when removable media, such as CDs and USB storage devices, are inserted into the computer and automatically executes the media's contents.

7. Operate Under the Principle of Least Privilege

In most instances of a malware infection, the malware can operate only under the rights of the logged-in user. To minimize the impact the malware can have if it successfully infects a computer, consider using a standard or restricted user account for day-to-day activities and only

logging in with the administrator account (which has full operating privileges on the system) when you need to install or remove software or change system settings from the computer.

8. Secure Your Web Browser

Web browsers installed on new computers usually don't have secure default settings. Securing your browser is another critical step in improving your computer's security because an increasing number of attacks take advantage of web browsers. Before you start surfing the internet, secure your browser by doing the following:

- Disable mobile code (that is, Java, JavaScript, Flash, and ActiveX) on websites you're not familiar with or don't trust. While disabling these types of code on all sites will significantly reduce your risk of being attacked, the websites you visit may not function as they normally do.
- Disable options to always set cookies. A cookie is a file placed on your computer that stores website data. Attackers may be able to log onto a site you've visited (like a banking site) by accessing the cookie with your login information. To prevent that, configure the browser to ask for permission before setting a cookie, allow cookies for sessions only, and disable features that keep you logged in to a site or that retain information you've entered, such as text you type into forms and the search bar.
- If you're using Internet Explorer, set the security levels for trusted sites (websites you most often visit and trust) to the second highest level. At the highest level, websites may not function properly.

Learn how to adjust these and other critical settings for the three most common browsers—Internet Explorer, Mozilla Firefox, and Apple Safari—in the document "Securing Your Web Browser" (http://www.us-cert.gov/reading_room/securing_browser/).

9. Apply Software Updates and Enable Future Automatic Updates

Most software vendors release updates to patch or fix vulnerabilities, flaws, and weaknesses (bugs) in their software. Because intruders can exploit these bugs to attack your computer, keeping your software updated is important to help prevent infection.

The third way Conficker attacked computers was by exploiting a vulnerability in Windows systems. Microsoft provided an update for this vulnerability. If people would have applied the update in a timely manner, they would have eliminated the opportunity for Conficker to infect their computers through this software vulnerability and helped reduce the spread of further Conficker infections across the internet.

When you set up a new computer (and after you have completed the previous practices), go to your software vendors' websites and check for and install all available updates. Enable automatic updates if your vendors offer it; that will ensure your software is always updated, and you won't have to remember to do it yourself. Many operating systems and software have options for automatic updates. As you're setting up your new computer, be sure to enable these options if offered. Be cautious, however, because intruders can set up malicious websites that look nearly identical to legitimate sites. Only download software updates directly from a vendor's website, from a reputable source, or through automatic updating.

10. Use Good Security Practices

You can do some simple things to improve your computer's security. Some of the most important are

- **Use caution with email attachments and untrusted links.** Malware is commonly spread by people clicking on an email attachment or a link that launches the malware. Don't open attachments or click on links unless you're certain they're safe, even if they come from a person you know. Some malware sends itself through an infected computer. While the email may appear to come from someone you know, it really came from a compromised computer. Be especially wary of attachments with sensational names, emails that contain misspellings, or emails that try to entice you into clicking on a link or attachment (for example, an email with a subject like that reads, "Hey, you won't believe this picture of you I saw on the internet!").
- **Use caution when providing sensitive information.** Some email or web pages that appear to come from a legitimate source may actually be the work of an attacker. An example is an email claiming to be sent from a system administrator requesting your password or other sensitive information or directing you to a website requesting that information. While internet service providers may request that you change your password, they will never specify what you should change it to or ask you what it is.
- **Create strong passwords.** Passwords that have eight or more characters, use a variety of uppercase and lowercase letters, and contain at least one symbol and number are best. Don't use passwords that people can easily guess like your birthday or your child's name. Password detection software can conduct dictionary attacks to try common words that may be used as passwords or conduct brute-force attacks where the login screen is pummeled with random attempts until it succeeds. The longer and more complex a password is, the harder these tools have to work to crack it. Also, when setting security verification questions, choose questions for which it is unlikely that an internet search would yield the correct answer.

Where Can I Learn More?

Implementing the practices in this paper will significantly improve your computer's security. The more you can implement, the more secure your computer will be. Even after implementing all ten of these practices, you still may not be protected from all of the risks you and your computer may encounter. It's important to continue investigating and implementing new ways to secure your computer because new risks will arise and old risks evolve. Learn more from these US-CERT resources:

- "Small Office/Home Office Router Security" (http://www.us-cert.gov/reading_room/HomeRouterSecurity2011.pdf)
- "Socializing Securely: Using Social Networking Services" (http://www.us-cert.gov/reading_room/safe_social_networking.pdf)
- "Securing Your Web Browser" (http://www.us-cert.gov/reading_room/securing_browser/)