2003 CERT Tech Tips: Before You Connect a New Computer to the Internet

Original publication date: December 15, 2003

This Tech Tip provides guidance for users connecting a new (or newly upgraded) computer to the Internet for the first time. It is intended for home users, students, small businesses, or any site with broadband (cable modem, DSL) or dial-up connectivity and limited Information Technology (IT) support. Although the information in this document may be applicable to users with formal IT support as well, organizational IT policies should be followed.

I. Motivating Factors

The CERT/CC has composed this Tech Tip to address a growing risk to Internet users without dedicated IT support. In recent months, we have observed a trend toward exploitation of new or otherwise unprotected computers in increasingly shorter periods of time. This problem is exacerbated by a number of issues, including:

- Many computers' default configurations are insecure.
- New security vulnerabilities may have been discovered between the time the computer was built and configured by the manufacturer and the user setting up the computer for the first time.
- When upgrading software from commercially packaged media (e.g., CD-ROM, DVD-ROM), new vulnerabilities may have been discovered since the disc was manufactured.
- Attackers know the common broadband and dial-up IP address ranges, and scan them regularly.
- Numerous worms are already circulating on the Internet continuously scanning for new computers to exploit.

As a result, the average time-to-exploitation on some networks for an unprotected computer is measured in minutes. This is especially true in the address ranges used by cable modem, DSL, and dial-up providers.

Standard advice to home users has been to download and install software patches as soon as possible after connecting a new computer to the Internet. However, since the background intruder scanning activity is pervasive, it may not be possible for the user to complete the download and installation of software patches before the vulnerabilities they are trying to fix are exploited. This Tech Tip offers advice on how to protect computers **before** connecting them to the Internet so that users can complete the patching process without incident.

II. Recommendations

The remainder of this document is divided into two major sections: General Guidance and Operating-System-specific steps.

1. General Guidance

    The goal of this document is to provide sufficient protection to a new computer so a user can complete the download and installation of any software patches that have been released since the computer was built or the software media (e.g., CD-ROM or DVD-ROM) being installed was manufactured. Note that these steps are not intended to be a complete guide to securely maintaining a computer once the initial download and installation of patches is completed. Additional tips and references about securely maintaining a computer are at the end of this document.

    Notes:
    - We recommend following the steps below when upgrading to a new operating system from disc(s) as well as when connecting a new computer to the Internet for the first time.
    - Perform these steps **before** connecting to the Internet for the first time.

    Following are the general steps we recommend:

    a. If possible, connect the new computer behind a network (hardware-based) firewall or firewall router.
    A network firewall or firewall router is a hardware device that users can install between the computers on their Local Area Network (LAN) and their broadband device (cable/DSL modem). By blocking inbound access to the computers on the LAN from the Internet at large (yet still allowing the LAN computers' outbound access), a hardware-based firewall can often provide sufficient protection for a user to complete the downloading and installation of necessary software patches. A hardware-based firewall provides a high degree of protection for new computers being brought online.

If you are connecting your computer behind a firewall or router that provides Network Address Translation (NAT), and if either of the following are true: (a) the new machine is the only computer connected to the LAN behind the firewall, or (b) all other machines connected to the LAN behind the firewall are up to date on patches and are known to be free of viruses, worms, or other malicious code, you may not need to additionally enable a software firewall.

b. Turn on the software firewall included with the computer, if available.
   If your operating system includes a built-in software firewall, we recommend that you enable it in order to block incoming connections from other computers on the Internet.

   As mentioned above, if your computer is going to be connected to a local network behind a hardware-based firewall and all other computers (if any) on that local network are known to be fully patched and free of malicious code, this step is optional. However, as part of a "defense-in-depth" strategy, we recommend enabling the built-in firewall software included with your operating system regardless.

   If your operating system does not include a built-in software firewall, you may wish to install a third-party firewall application. Many such applications are available at relatively little (or sometimes no) cost. However, given that the issue we're trying to address is the relatively short lifespan of an unprotected computer on the open Internet, we recommend that any third-party firewall application be installed from media (CD-ROM, DVD-ROM, or floppy disc) before connecting to a network rather than downloaded directly to the unprotected computer. Otherwise, it may be possible for the computer to be exploited before the download and installation of such software is complete.
c. Disable nonessential services, such as file and print sharing.
   Most operating systems are not configured with file and print sharing enabled by default, so this shouldn't be an issue for most users. However, if you are upgrading a computer to a new operating system and that computer had file or print-sharing enabled, it is likely that the new operating system will have file and print sharing enabled as well. Since the new operating system may have vulnerabilities that were not present in the older version being upgraded, disable file and print sharing in the older version before beginning the upgrade process. After the upgrade is complete and all relevant patches have been installed, file sharing can be re-enabled if needed.
d. Download and install software patches as needed.
   Once the computer has been protected from imminent attack through the use of either a hardware or software-based firewall and the disabling of file and print sharing, it should be relatively safe to connect to the network in order to download and install any software patches necessary. It is important not to skip this step since otherwise the computer could be exposed to exploitation if the firewall were to be disabled or file/print sharing turned back on at some later date.

   Download software patches from known, trusted sites (i.e., the software vendors' own sites), in order to minimize the possibility of an intruder gaining access through the use of Trojan horse software.

1. Operating System-Specific Guidance

   The previous section outlined the CERT/CC's general guidance for installing new computers. However, the specific implementation of those recommendations depends on the operating system in use. This section contains specific guidance for users of Microsoft Windows XP and Apple Macintosh OSX, as well as some pointers for other operating system users.

   a. Microsoft Windows XP

      In order to complete these steps, you will need to be logged into an account with local administrator privileges.

      i. Review General Guidance above.
      ii. Connect behind a hardware-based firewall if available.

          This step is covered in the General Guidance section above.

      iii. Enable the Internet Connection Firewall.

          Microsoft has provided both detailed and summarized instructions for enabling the built-in Internet Connection Firewall on Windows XP.

      iv. Disable shares if enabled.
          1. Go to Start -> Control Panel.
          2. Open "Network and Internet Connections".
          3. Open "Network Connections".
          4. Right-click on the network connection you wish to change (e.g., "Local Area Connection").
          5. Select "Properties".
          6. Make sure "File and Printer Sharing for Microsoft Networking" is unchecked.
      v. Connect to the network.
      vi. Go to http://windowsupdate.microsoft.com.
      vii. Follow the instructions there to install all Critical Updates.
      viii. Review Staying Secure below.

      Additional Windows References can be found at the end of this document.

   a. Apple Macintosh OSX
      i. Review General Guidance above.
      ii. Connect behind a hardware-based firewall if available.
      iii. Enable the software firewall.
          1. Open "System Preferences".
          2. Select "Sharing".
          3. Select the "Firewall" Tab.
          4. Click "Start".
          5. Select the "Services" Tab.
          6. Verify that all services are unchecked (default).
      iv. Connect to the network (plug in or dial-up).
      v. Update installed software.

1. Open "System Preferences".
2. Select "Software Updates".
3. Turn on automatic updates (checkbox: "Automatically check for updates when you have a network connection".)
4. Select an appropriate update frequency (daily is recommended).
5. Click "Check Now".
6. Install any recommended updates.

vi. Review Staying Secure below.

Additional OSX References can be found at the end of this document.

a. Other Operating Systems

Users of other operating systems should review the General Guidance above, then consult their respective software vendors' sites for specific instructions (where available).

Additional Linux References can be found at the end of this document.

III. Staying Secure

1. Read our Home Network Security document.

1. Install and use antivirus software

While an up-to-date antivirus software package cannot protect against all malicious code, for most users it remains the best first-line of defense against malicious code attacks. Many antivirus packages support automatic updates of virus definitions. The CERT/CC recommends using these automatic updates when available.

1. Enable automatic software updates if available

Vendors will usually release patches for their software when a vulnerability has been discovered. Most product documentation offers a method to get updates and patches. You should be able to obtain updates from the vendor's web site. Read the manuals or browse the vendor's web site for more information.

Some applications will automatically check for available updates, and many vendors offer automatic notification of updates via a mailing list. Look on your vendor's web site for information about automatic notification. If no mailing list or other automated notification mechanism is offered you may need to check the vendor's website periodically for updates.

1. Avoid unsafe behavior

Additional information on this topic can be found in our Home Network Security Tech Tip.

- Use caution when opening email attachments or when using peer-to-peer file sharing, instant messaging, or chatrooms.
- Don't enable file sharing on network interfaces exposed directly to the Internet.

1. Follow the principle of least privilege — don't enable it if you don't need it.

Consider using an account with only 'user' privileges instead of an 'administrator' or 'root' level account for everyday tasks. Depending on the OS, you only need to use administrator level access when installing new software, changing system configurations, and the like. Many vulnerability exploits (e.g., viruses, Trojan horses) are executed with the privileges of the user that runs them — making it far more risky to be logged in as an administrator all the time.

References

1. CERT/CC References
   - Home Network Security -- http://www.cert.org/tech_tips/home_networks.html
   - IN-2003-01 Malicious Code Propagation and Antivirus Software Updates -- http://www.cert.org/incident_notes/IN-2003-01.html

1. Microsoft Windows XP References
   - Protect Your PC -- http://www.microsoft.com/security/protect/default.asp
   - Using the Internet Connection Firewall -- http://www.microsoft.com/windowsxp/home/using/howto/homenet/icf.asp
   - How to Enable Internet Connection Firewall (ICF) on Windows XP -- http://www.microsoft.com/security/incident/icf.asp
   - Microsoft Windows XP Baseline Security Checklist -- http://www.microsoft.com/technet/security/chklist/xpcl.asp

1. Apple Macintosh OSX References
   - How to Keep Network Computers Secure -- http://docs.info.apple.com/article.html?artnum=61534
   - Apple Product Security -- http://www.info.apple.com/usen/security/index.html
   - OSX Security Features Overview -- http://www.apple.com/macosx/features/security/
   - Apple Security Updates -- http://docs.info.apple.com/article.html?artnum=61798

1. Linux References
   - Debian Security Information -- http://www.debian.org/security/
   - Lindows.com -- http://www.lindows.com/
   - MandrakeSecure -- http://www.mandrakesecure.net/en/index.php
   - RedHat Security Resource Center -- http://www.redhat.com/solutions/security/

- RedHat Security and Errata -- http://www.redhat.com/apps/support/errata/
- Slackware Security Advisories -- http://www.slackware.com/security/
- SUSE Security (US/Canada) -- http://www.suse.com/us/private/support/security/

Revision History
December 15, 2003 Initial Release