Internet Security Tips

This guide is intended to assist Heartland Owners in understanding and protecting against internet security threats.

Note that due to the rapidly-changing security landscape on the internet and with computer software, it's impossible to ever be up-to-date in a document like this. Nevertheless, the tips here should prove helpful in protecting you. Please check the date of the document in the footnote. If the document is more than 1 year old, the advice may be dated and some links may not work.

Important Notices

Who created this document?

This document has been created by Heartland Owners independently of the Heartland RV Company, and is posted to the Heartland Owners Forum as a service to the owner community.

Errors and Omissions

Because the authors are Heartland owners, not engineers or service technicians, it's possible that this document could contain errors or omissions. Readers are advised to also review the manufacturers' product documentation for more complete information and guidance.

Limitations on Using this Document

- This document may not be modified or sold.
- It may not be posted on the internet without permission.
- Other websites may link to the page from which the document may be downloaded, but may not link directly to the document without permission (search engines excluded).

Contact Information

Questions and comments may be directed to manuals@heartlandowners.org

Internet Security Tips

Table of Contents

Internet Security Tips

As soon as you connect your computer to the internet, you're exposed to significant threats to the health of your computer, your stored data files, your privacy, and even your finances.

Types of Threats

Most of us are generally concerned with viruses infecting our computers, degrading normal operation, or worse. Many people think that as long as you run an Antivirus program and don't open executable files from people you don't know, you'll be protected. But other types of threats exist.

Common Threats

1. Opening files from people you know can be dangerous. A common malware tactic is to use the infected computer's email address book to target and infect others. Your defenses may be lowered because the file came from someone close to you. If you think it's legitimate, scan the file for viruses before opening.
2. Visiting any website can be dangerous. Elements on any webpage may contain malware that tries to exploit security weaknesses in your software. The favorite containers for malware are Java, Flash, and PDF files. While we'd like to believe that only "those kinds" of websites could possibly have malware, it's possible to embed malware into files that get posted on well-known websites. We may incorrectly assume that well-known sites scan posted content for malware in order to protect us. Maybe they do, maybe they don't. Protective measures are discussed on following pages.
3. Similar to opening a file, clicking on a link that arrived via email is dangerous. It may very well take you to a website with malware, with intent to infect your computer. This is particularly true if the link is prefaced with a generic or impersonal message. If your brother clicked on the link, and was infected, the infected software used your brother's address book to find and infect you. Verify before clicking by contacting the sender.
4. Installing downloaded software. Unfortunately, even software that looks legitimate can be compromised. Always do a virus scan of the file before installing.
5. Pfishing and Spoofing. This is a very common technique to try and steal your userid and password. An email arrives informing you that you need to log into your account to do something. A link is conveniently included. Instead of taking you to the real site, it takes you to a site masquerading as the real site, but designed to capture your log in information. It may even then transfer you to the real site and log you in so as to not arouse your suspicions. If you think the email is legitimate, type the URL by hand. Never use the conveniently provided links.
6. Open Port Attacks. Your operating system opens certain "ports" or software addresses on your computer for remote programs to do their work. For example, your Internet Browser users a port that must be open in order to communicate with websites. When you connect to the internet, within a very short time, your computer will be probed to find open ports and attacks will begin, trying to exploit weaknesses. Firewalls protect against most of these attacks.

Why Do These Threats Exist?

There are multiple reasons for people to create viruses and other attacks.

Some are created by people who think it might be intellectually challenging, or fun to create a virus, a worm, or some other attack. They gain satisfaction when they succeed.

Some are created by people who dislike a software vendor. Microsoft software is often a target. They may think that by hurting you, they hurt Microsoft.

Some are a concerted attempt to steal your private information, your financial records, or even your identity. Many celebrities have had their private photos stolen and posted on the internet.

Some attacks are intended to compromise as many computers as possible so that they can be used in coordinated attacks against major websites. If millions of computers suddenly all begin accessing the same website at the same time, it can deny service to legitimate visitors. This is known as a "Denial of Service" attack.

There are nations now working on Cyber warfare with intent to disable or damage another nation's computer infrastructure. It's believed that Russia used Cyber warfare with devastating success against Georgia in their conflict a few years ago. Such attacks could easily target private users along with Government, Business, and Infrastructure sites.

Security Improvements to Clean Up Infections and Protect You

This is a multi-step approach to cleaning your computer and helping to protect against future infections.

1. Download and run Malwarebytes. There are Free and Fee versions. You can work with the free version. You may have to select the free version several times and decline trials in the course of downloading and installing.

   The application will likely download an update to its definitions after the install. This is expected and desired.

2. Download Microsoft's "Windows Defender Offline"
   If your computer is already infected, it's possible that the infected code could be partially or entirely disabling the normal antivirus software, or hiding from it. Running the cleanup program from a bootable disk eliminates the possibility that the cleanup program you normally use might have been compromised.

   Before downloading, you'll need to know whether you have a **32bit** version of Windows installed, or a **64bit** version. You can determine this by right-clicking on "Computer" or "My Computer", and then click on Properties. Look for a notation regarding 32bit or 64bit.

   Download the matching 32bit or 64bit version of Windows Defender Offline.

   When you run the downloaded program, it will prompt you to **install on a Bootable disk** (either CD, DVD, or USB Thumb Drive).

   Once the program has been installed on the bootable disk, **shutdown the computer** and with the new disk in the drive or USB slot, **restart the computer**. Note: you will likely have to press a key during the boot process for the computer to boot from the CD/DVD/USB Thumb Drive. You may have to interrupt the normal boot process by pressing Escape, F10, F12, or F2.

   If you see the normal Windows boot logo, the machine did not boot from the new disk and you'll have to try restarting.

   After booting, select the "Full Scan" option of Windows Defender Offline to ensure the deepest cleaning.
3. If you have previously installed Antivirus/Firewall software from Norton/Symantec, McAfee, TrendMicro, etc, consider replacing it with Microsoft Security Essentials. Microsoft's program is lighter weight and makes fewer changes to your computer as part of its routine installation. It is free and like other Microsoft programs, is updated via the Windows Update Tool.
   a. Download Microsoft Security Essentials.
   b. Uninstall your current AntiVirus software. In most cases, you can do this from the Windows Control Panel - Programs and Features or Add/Remove Programs. In some cases, you may have to visit the vendor's website to get an uninstall program.
   c. Immediately install Microsoft Security Essentials.
   d. Run another "Full Scan" with Security Essentials.
4. In the Windows Control Panel, open the Security Center to make sure the **Firewall is ON**.
5. If you followed all of these steps, and the programs report that any infections have successfully been dealt with, you should be in good shape. You'll still need to be diligent to prevent introduction of viruses by way of downloaded software and similar mechanisms.

What if My Computer is Still Infected?

This guide doesn't cover all possible scenarios, and some infections are simply too deeply embedded for the techniques and programs listed earlier. In cases like this, your computer cannot be trusted again until it's been completely re-formatted and re-loaded.

At this point, you may want to get professional assistance.

If you want to continue on your own:

1. Save all the data files you care about to an external drive.
2. Install Windows from scratch – including formatting the drive completely.
3. Install the Microsoft Security Essentials.
4. Install all Windows updates. You usually have to install and then re-check because there are usually updates to the updates. Keep doing this until there are no more updates.
5. Install all Device Drivers for your hardware from newly downloaded copies from the original manufacturer's website.
6. Re-install your other software and reinstall the files you saved.
7. Consider using "Foxit " instead of Adobe Acrobat for PDF viewing.

Protecting Your Computer from Malware

Most of today's malware threats to the PC come in via one of 3 attack vectors:

Java, Flash, Acrobat PDF files.

All three file types are commonly used on websites and are pretty much unavoidable. Since you have no way of knowing if a website has malware hiding in one of these file types, you'll have to take a multi-faceted approach to protect your computer.

1) Don't click through to unknown websites. If you get an email that says "This is really funny" or "Take a look at this" or any similar enticement, with a link to click on, just don't go there. Even if the email is from someone you trust, just don't go there. If you think it might be legitimate, before clicking, reply to your friend and ask if they intended to send you this link.
2) Make yourself a smaller target. More attacks are aimed at Internet Explorer than at Firefox or Chrome browsers. Install Firefox and/or Chrome and make one of them your primary browser.
3) Uninstall Java unless you know that you need it. Some employers may use Java programs, so if you use the computer for work, you might need it. If you goof by uninstalling it, you can always reinstall it later. Use the Windows Control Panel - Programs and Features or Add/Remove Software to locate it and uninstall. The entry will say something like "Java™ 6 Update 37"
4) Disable the browser plug-in for Java. If you know that you need the plug-in for browsing, perhaps on a banking website, you might leave it in one browser. You could leave it on Internet Explorer for example, but disable it from Firefox and Chrome. Then do your routine internet browsing from Firefox or Chrome. Only switch to Internet Explorer when you need the Java plug-in to run.

5) Add extensions to your browsers to block Ads and to block Flash objects from routinely launching. Note that the menus change as versions are updated, so the wording shown here may have changed.
   a) Changes to Firefox
      i) **Disable Java.** Go to the main menu and select **Add-ons**. Then select the **Plug-ins tab**. Find Java and press the Disable button.
      ii) **Install Adblock**. Select the **Get Add-ons** tab. Search for AdBlock and install it to block unwanted ads that may contain malware.
      iii) **Install Flashblock**. Search for and install the FlashBlock add-on and install it. This will prevent Flash files from opening, eliminating a major source of malware. You'll still be able to click on an icon to view the flash file if you are comfortable that it's not infected.
   b) **Changes to Chrome**
      i) **Disable Java.** In the address bar, type **chrome://plugins/** Find Java and disable unless you know you need to use it.
      ii) On the main menu, go to **Tools/Extensions** and **Install Adblock**.
      iii) On the main menu, go to **Tools/Extensions** and **Install Flashblock**
   c) **Changes to Internet Explorer**
      i) On the main menu, go to **Tools/Manage Add-ons** and **Disable Java**.
      ii) **Blocking Ads**. Use this link to install Simple Adblock.
      iii) **Blocking Flash**. Go to **Tools/Manage Add-ons**. Find Shockwave Flash Object and double-click on it. Then select **Remove All Sites**. After doing so, when you browse a Flash Object, you'll be prompted on whether to enable Flash on that site.
6. **Ensure your Windows Updates are current.** This is important because security patches are constantly being released. Down level software is extremely vulnerable because the security attacks have been perfected against the weaknesses in down level releases.
7. **Ensure your Adobe Acrobat is up-to-date**. Acrobat (reader for PDF files) is a major target because PDF files are so pervasive. New attacks are constantly being developed and software updates are released on a frequent basis to patch the code.
8. Consider using "Foxit " instead of Adobe Acrobat for PDF viewing.

Am I Safe Now?

Maintaining security is a constant battle and requires constant care. The good guys are working hard to defend you. The bad guys are working hard to develop new attacks that get through the defenses. Stay alert. Avoid bad practices like clicking on email links. Keep your software updated. Disable plug-ins that you don't need.

In short, make yourself a smaller target by following the recommendations above.

Then enjoy the internet.