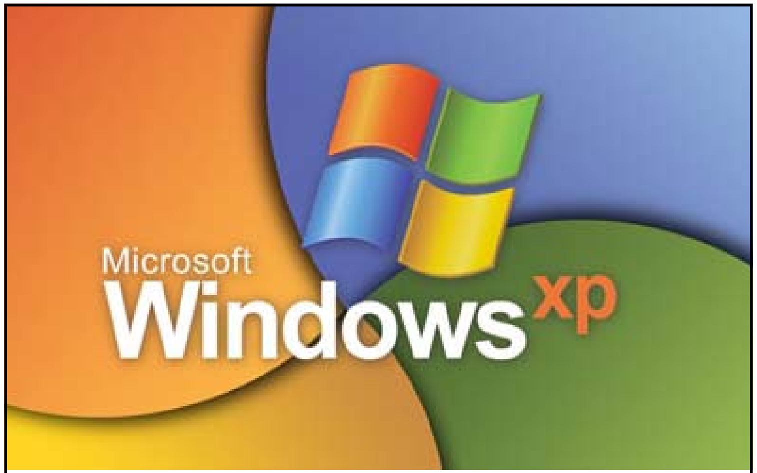


Retirement is Around the Corner

Retirement of Windows XP

- The retirement of Windows XP operating system, for personal and business use.
  - – Lifespan timelines of operating systems.
  - – Hardware recommendations & requirements for personal and business users.
  - – Advice on upgrading options.

Microsoft Windows XP

http://www.microsoft.com/en-us/windows/enterprise/endofsupport.aspx

What is end of support?

After 12 years, support for Windows XP will end on April 8, 2014. There will be no more security updates or technical support for the Windows XP operating system. It is very important that customers and partners migrate to a modern operating system such as Windows 8.1. Customers moving to a modern operating system will benefit from dramatically enhanced security, broad device choice for a mobile workforce, higher user productivity, and a lower total cost of ownership through improved management capabilities.

Support for Office 2003 also ends on April 8, 2014.

What does this mean?

It means you should take action. After April 8, 2014, Microsoft will no longer provide security updates or technical support for Windows XP. Security updates patch vulnerabilities that may be exploited by malware and help keep users and their data safer. PCs running Windows XP after April 8, 2014, should not be considered to be protected, and it is important that you migrate to a current supported operating system – such as Windows 8.1 – so you can receive regular security updates to protect their computer from malicious attacks.

Read the Windows lifecycle fact sheet to learn more.

Potential risks of staying with Windows XP

Running Windows XP SP3 in your environment after April 8, 2104
may expose you to potential risks, such as:

Security:
Without critical Windows XP security updates, your PC may become vulnerable to harmful viruses, spyware, and other malicious software which can steal or damage your business data and information. Anti-virus software will also not be able to fully protect you once Windows XP itself is unsupported.

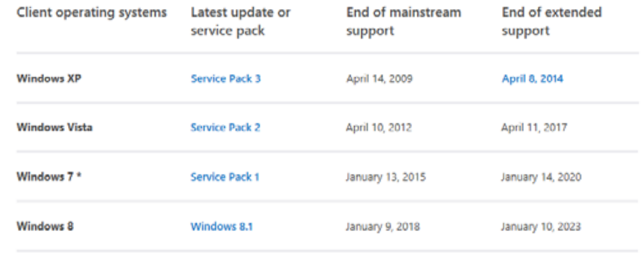
Compliance:
Businesses that are governed by regulatory obligations such as HIPAA may find that they are no longer able to satisfy compliance requirements. More information on HHS's view on the security requirements for information systems that contain electronic protected health information (e-PHI) can be found here (HHS HIPAA FAQ - Security Rule).

Lack of Independent Software Vendor (ISV) Support:
Many software vendors will no longer support their products running on Windows XP as they are unable to receive Windows XP updates. For example, the new Office takes advantage of the modern Windows and will not run on Windows XP.

Hardware Manufacturer support:
Most PC hardware manufacturers will stop supporting Windows XP on existing and new hardware. This will also mean that drivers required to run Windows XP on new hardware may not be available.

Lifecycle Schedule and Fact Sheet

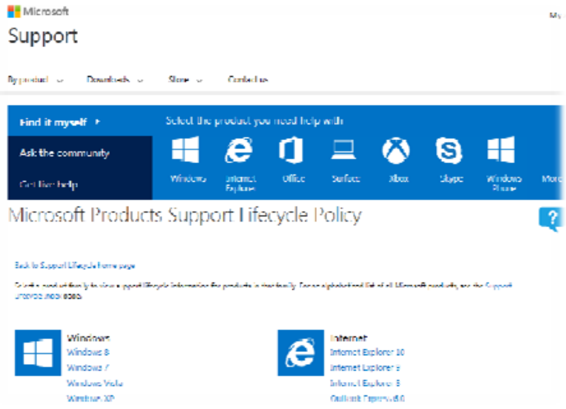
Every Windows product has a lifecycle. The lifecycle begins when a product is released and ends when it's no longer supported. Knowing key dates in this lifecycle helps you make informed decisions about when to upgrade or make other changes to your software. Here are the rights and limits of the Windows lifecycle.



Client operating systems	Latest update or service pack	End of mainstream support	End of extended support
Windows XP	Service Pack 3	April 14, 2009	April 8, 2014
Windows Vista	Service Pack 2	April 10, 2012	April 11, 2017
Windows 7 *	Service Pack 1	January 13, 2015	January 14, 2020
Windows 8	Windows 8.1	January 9, 2018	January 10, 2023

Microsoft Lifecycles

http://support.microsoft.com/gp/lifeselect



Microsoft Products Support Lifecycle Policy

Back to Support Lifecycle home page

Select a product family to view support lifecycle information for products in that family. For an alphabetical list of all Microsoft products, see the Support [illegible]

Windows
Windows 8
Windows 7
Windows Vista
Windows XP

Internet
Internet Explorer 10
Internet Explorer 9
Internet Explorer 8
Outlook Express 6.0

How do I migrate off Windows XP?

Enterprise Customers:
Microsoft offers large organizations (500+ employees) in-depth technical resources, tools, and expert guidance to ease the deployment and management of Windows, Office and Internet Explorer products and technologies. To learn more about migration and deployment programs, please contact your Microsoft sales representative or Certified Microsoft Partner. Learn how to pilot and deploy a modern desktop yourself by visiting the Windows 8.1 Springboard Series.

Small to Medium Business:
There are many options for small and medium businesses considering moving to a modern PC with the latest productivity and collaboration tools. Small to mid-size organizations (<500 employees) should locate a Microsoft Certified Partner to understand the best options to meet their business needs. If your current PC meets the system requirements for Windows 7 or Windows 8.1, you can buy Windows 7 Professional or Windows 8.1 Pro from a local retailer or Microsoft Certified Partner. If your PC does not meet system requirements, consider purchasing a new business PC with Windows 8.1 Pro.

Windows 7 Upgrade Advisor

First Step:

Find out if your PC can run Windows 7
To see if your PC is ready for Windows 7, download the free Windows 7 Upgrade Advisor. It scans your PC for potential issues with your hardware, devices, and installed programs, and recommends what to do before you upgrade. (If you're already running Windows 7, you can add premium features online with a Windows 7 upgrade.)

If your PC can run Windows Vista, it can probably run Windows 7, but it's still a good idea to download and run the Windows 7 Upgrade Advisor before you begin the upgrade process.

Before scanning your PC with the Windows 7 Upgrade Advisor, be sure to plug in and turn on any USB devices or other devices, such as printers, external hard disks, and scanners, that you regularly use with the PC you're checking.
http://windows.microsoft.com/en-us/windows/downloads/upgrade-advisor

Windows 7 System minimum requirements

- If you want to run Windows 7 on your PC, here's what it takes:
- 1 gigahertz (GHz) or faster 32-bit (x86) or 64-bit (x64) processor
- 1 gigabyte (GB) RAM (32-bit) or 2 GB RAM (64-bit)
- 16 GB available hard disk space (32-bit) or 20 GB (64-bit)
- DirectX 9 graphics device with WDDM 1.0 or higher driver

Windows 8 System minimum requirements

- 1 GHz processor or faster with support for PAE, NX, and SSE2
- 1-2 GB RAM / 16-20 GB available hard disk space
- 1024 × 768 screen resolution
- DirectX 9 graphics processor with WDDM driver
- To use touch, you need a PC that supports multitouch
- To install the free update to Windows 8.1 or Windows 8.1 Pro through the Windows Store, your PC must be running Windows 8 or Windows 8 Pro.

Windows 7 Upgrade Advisor

Second Step:

If your PC CAN upgrade to Windows 7
If the Upgrade Advisor finds that your PC is able to run Windows 7, make sure that it is not just barely slipping by. Some PC's will have just enough memory and hard drive space to install Windows 7, but unless you have the recommended amount, your PC will do nothing but boot up and freeze. If you are on the line of possibly being able to upgrade, make sure to choose the 32 bit installation which uses less resources than the 64 bit.
*Remember to keep in mind the lifecycle of Windows 7

If your PC CAN'T upgrade to Windows 7
It may be time to upgrade your hardware. You are able to try an installation of Windows 7, but that means spending money on an operating system that may not come through in the end. When you purchase a new PC, it will come with an upgraded operating system of Windows 7 or 8.
*Remember to keep in mind the lifecycle of the operating system you purchase.

Windows 7 Upgrade Advisor

Third Step:

If your PC CAN upgrade to Windows 7:
You will need to purchase the Operating System license.

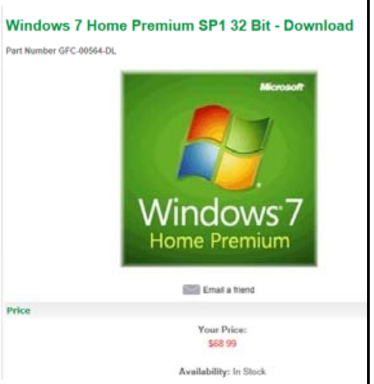
Licenses can be purchased through many vendors, whether they are a retail store or online. The next slide will give you a checklist to ensure you purchase the correct license for you.

If your PC CAN'T upgrade to Windows 7:
You will need to purchase new hardware.

This is the slide that hurts the wallet, but the good news is:
-If you are a non profit, you have options,
-Prices on top-of-the-line technology has come down over the years,
-You will end up with a new computer that will last you through the years, and will bring your business to a new level.

Checklist when Purchasing Windows 7 License and Upgrading

- Check whether you are purchasing 32 Bit or 64 Bit rating
- Home Premium vs. Professional version
- System requirements and your hardware
- Downloading vs. disc
  - *Be careful of scams
- Backup EVERYTHING
- Run Belarc Advisor to retrieve all your pertinent information on your old computer.
- Make sure your peripherals will have drivers available – you may want to download them first and save them to a file.


Windows 7 Home Premium SP1 32 Bit - Download

Part Number GFC-00564-DL

Price

Your Price:
$68.99

Availability: In Stock

Additional Resources and Articles

- http://technet.microsoft.com/en-us/windows/dd671583
- http://www.techrepublic.com/article/deciding-to-ditch-windows-xp-here-are-your-options/#ftag=RSS56d97e7
- http://www.techrepublic.com/article/xp-replacement-179-asus-chromebox-is-most-powerful-chrome-device-to-date/#ftag=RSS56d97e7
- http://www.techrepublic.com/article/microsofts-monumental-task-in-windows-9-win-back-the-base/#ftag=RSS56d97e7
- http://www.techrepublic.com/blog/10-things/dust-off-your-y2k-playbook-10-strategies-to-drive-s-successful-xp-migration/#ftag=RSS56d97e7

Computer Upkeep

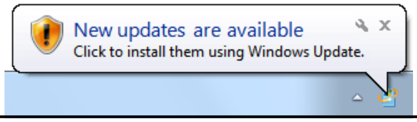
- General computer maintenance.
  - Recommendations for
    - Updates
    - Scans
    - Clean up tools.
  - Internet Security
- How to keep important emails out of SPAM (like the Chamber newsletter!)

7 Basic Windows PC Maintenance Tips

- Lots of small business owners don't know much about basic computer maintenance and as a result, their PCs slow down or crash. The real issue is neglect: failing to update security patches and antivirus software, overloading the system with trial software or running five toolbars at once in Internet Explorer.
- Of course, many small business owners don't know much about cars either, but they know to give it gas, change the oil every so often and to keep an eye out for flat tires. It's the same with PCs. You don't need to be an expert to keep your PC in relatively good condition. You just need to perform a little basic PC maintenance and, more importantly, be observant.

1. Keep Windows Updated with the Latest Patches

- Since Windows 98, Microsoft has provided access to Windows Update. Windows Update scans your system and updates it with the latest security patches and service packs. These are broken down into Critical and Recommended updates.
- A new version of Windows Update, Microsoft Update, is also available. In addition to Windows, Microsoft Update will also patch a wide variety of Microsoft applications, such as Office and Windows Defender. Best of all, you can schedule these updates to run automatically, so there is really no excuse for not having a patched system. To access Windows Update click on the **Start** button, **All Programs** and scroll through the list to find it.
- Updates are scheduled for the Second Tuesday of each month (Patch Tuesday). Make sure to look for this icon in your taskbar area:



New updates are available

Click to install them using Windows Update.

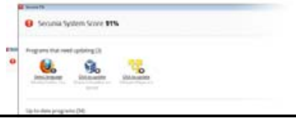
2. Keep Your Spyware and AntiVirus Programs Updated

- No matter how good your spyware and antivirus software is, if it's not updated or, worse, not running at all, then it won't do you any good. Most antivirus applications load an icon in the Windows tray, which lets you verify its status at a glance. Always verify that the application is running after starting Windows.
- In addition, these applications should be configured to perform definition updates everyday and complete system scans should take place at least once a week. Should you need a new antivirus scanner, I suggest using **Avira Antivir**. Not only is it free, but it always performs near to, if not at, the top of most comparison tests. To combat malware, I suggest **A-Squared** and **Malwarebytes' Anti-Malware**. Both are critically renowned for their ease of use and effectiveness; and they're free.

Malwarebytes

3. Keep Your Applications and Utilities Patched

- Believe it or not, all of the applications and utilities on your system are prone to security risks and need to be updated regularly. Programs that you use everyday like Adobe Acrobat Reader, QuickTime, Realplayer, Skype, WinZip and more require both maintenance and security updates from time to time.
- Even applications that run in the background like Flash and Java are at risk. Trying to keep track of each of these individually can be a bit of a handful, but a nifty utility called **Secunia PSI** makes the job much easier. This free utility tracks a massive number of security exploits in applications and will automatically monitor your PC for susceptible apps. When it finds one, it directs you to a site where you can download and install the needed patches. This program is an invaluable resource for keeping your PC secured.



3. Keep Your Applications and Utilities Patched

- BE CAREFUL
  - Updating programs with patches can lead to downloading and installing other software or toolbars.
  - Be careful to "un-check" the installation of these unwanted extras.

4. Remove Unused Applications and Other Junk

- Your PC has a lot of non-essential data (e.g., crud) stored on it, much of which you might not even be aware of. For instance, Internet Explorer stores copies of the Web pages you visit, images and media for faster viewing later. Plus there are temporary files, your Internet history, cookies, and more scattered throughout your system.
- Plus, when your machine was brand new it came pre-loaded with numerous pieces of trial software. This could be games, security suites, even full blown applications like QuickBooks or Microsoft Office. Many people never install these. Others have, but decided not to purchase them at the end of the trial. Yet they remain on the system, wasting space and bloating the Windows Registry. Over time, this can lead to performance problems, causing Windows to become sluggish and unreliable.

4. Remove Unused Applications and Other Junk

- One of the easiest ways to combat this is to use FREE CCleaner, a freeware utility for system optimization, privacy, and cleaning. This tool removes unused files from a hard drive and cleans up online history. But more important, it includes an outstanding registry cleaner. It even has an uninstaller to assists you in removing applications from your system.

CCleaner

.

5. Pay Attention to the Software You Install

- Many applications, especially freeware, often attempt to install additional software on your system. For example, when I install RealPlayer it also gives me the option to install Google Chrome.
- I actually like Google Chrome so, for me, it's a bonus. However, some applications also try to install stuff I don't want, like an additional toolbar in Internet Explorer. In almost all cases you'll be asked whether or not you want this extra software installed.
- The trick is, and I know this can be difficult, is that **YOU MUST PAY ATTENTION DURING THE INSTALLATION** and actually read those screens that popup with the words on them and **NOT** just mindlessly click the "Next" button until the process finishes. If you follow this tip I can guarantee that the amount of junk installed on your system will decrease.
- Some programs may even slip in extra programs without asking you. Make sure to check your program list after installation to make sure you recognize all the programs.
- And should you find something installed without your authorization, uninstall it immediately. If it won't uninstall, use Window's System Restore feature to revert back to an earlier configuration. This brings us to our next tip…

6. Create a System Restore Point

- Before you install any new software on your system, always create a System Restore point. Some software can play havoc to your system causing all sorts of strange problems. System Restore helps you restore your computer's system files to an earlier point in time when your system was working well.
- It's a safe way to undo system changes to your computer without affecting your personal files, such as e-mail, documents or photos. Having a restore point can significantly reduce your downtime. Plus this functionality is built right into Windows so there is really no reason not to do it.
- To create a system restore point go to **Control Panel** and select **Backup and Restore**. Windows 7 users click "**Recover system settings or your computer**". Vista users select "**Create a restore point or change settings**." After you have created a restore point, you can access and use it easily through CCleaner.

7. Defragment and Check Your Hard Drive for Errors Regularly

- In order to help maintain the integrity of your data there are two hard drive tests that you should run at least once a month. The first is to **Defragment** your hard drive. Over the course of regular use, your files get fragmented or spread out all over your hard drive. So while an MP3 or WMV file appears as a single file to you in Windows Explorer, small pieces of the file could literally be spread across the entire hard drive.
- Gathering all of these distant pieces back together into a single contiguous file makes file access faster. Depending on how fragmented the data on your drive is, defragmenting it could make your system noticeably faster.
- The other test we are going to perform is a **Check Disk**. This tool checks hard disk volumes for problems and attempts to repair any that it finds. For example, it can repair problems related to bad sectors, lost clusters, cross-linked files and directory errors. Disk errors are a common source of difficult-to-track problems, and running this test regularly can significantly reduce your risk of problems.

7. Defragment and Check Your Hard Drive for Errors Regularly

- Windows has a built-in defragmenter and check-disk utility. To access either of them just open **Windows Explorer** and right-click on the drive you want to examine. Select **Properties** and then click on the **Tools** tab. To defragment your hard drive go to the **Defragmentation section** and press the **Defragment now** button. To perform a check disk, go to the **Error-checking section** and press the **Check now** button.
- Certain free third-party defragmentation utilities have some significant advantages to the one built into Windows. For instance, both Ultra Defrag and Smart Defrag perform the job much quicker than the built-in version. You can schedule them to run automatically — and transparently — in the background while you work. Try them both for yourself.

Paying Attention

- You don’t need to be a computer expert to keep your computer running well. Resolving these issues doesn’t have anything to do with understanding computers. It has to do with paying attention to what you’re doing and actually reading those messages that popup on screen during an installation. Just follow these basic steps, and I guarantee you’ll computer will be safer and far more reliable.

10 Tips to Protect Your Personal Information and Identity

- When you go online for emailing, instant messaging (IM), shopping, and banking, you often communicate personal information such as addresses, phone numbers, account numbers, usernames, and passwords. Unfortunately, you risk having this personal information and possibly even your identity stolen, or having your PC used as a launching pad for hackers to attack others.
- Follow these top ten tips to protect yourself and your computer:

10 Tips to Protect Your Personal Information and Identity

1. **Invest in trusted, multi-faceted security software.** Look for comprehensive, multi-faceted PC security software that protects you from viruses, spyware, adware, hackers, unwanted emails, phishing scams, and identity theft. Choose a brand that you can trust, like McAfee, Norton, or AVG. Purchasing a license is well worth it compared to free versions.
2. **Always access the Internet from behind a firewall.** A firewall adds a security layer between your PC and the Internet, and helps stop hackers from stealing your identity, destroying your files, or using your PC to attack others.
3. **Use a PC you know is secure.** Hackers can easily retrieve sensitive data that is sent over an unsecured Internet connection. If you need to send sensitive information or make an online transaction, use a PC that you know is secure and remember that there are many flavors of security. Some computers only have the bare minimum while others, have comprehensive security.

10 Tips to Protect Your Personal Information and Identity

4. **Watch out for phishing scams.** Phishing scams use fraudulent emails and web sites, masquerading as legitimate businesses, to lure unsuspecting consumers into revealing private account or login information. Even if you have PC security, you still might visit a malicious web site without knowing it. Legitimate businesses will never ask you to update your personal information via email. Always verify web addresses before submitting your personal information.
5. **Secure your wireless network.** You are at risk if you access the Internet from a Wi-Fi network. Since your wireless network’s radio waves travel through walls, a hacker with a simple antenna could attack you from miles away to steal your information and use your wireless network for their own communication. Always use additional Wi-Fi security protection (which starts with a password!).
6. **Never install potentially unwanted programs (PUPs) like spyware or adware on your PC.** Many free programs that you download via the Internet, while appearing to be harmless, are specifically designed to be malicious and monitor your keystrokes, track your Internet logins, transmit your confidential information, or redirect your browser to fake sites. Some of these programs can also be installed on your machine simply by clicking on an advertisement link on the Internet.
   With security software, you can stop these programs from installing. Never willingly install programs unless you are familiar with the web site and program and have read the end-user license agreement thoroughly.

10 Tips to Protect Your Personal Information and Identity

7. **Do not answer chain email.** Even with PC security, some chain email forwarded by your friends might ask for personal information. Do not download files from friends and family unless you know the content of the file and know that it is secure.
8. **Monitor your credit reports and be aware.** At least once a year, check your credit history. This is one of the best ways to find out if someone is using your personal finance information without your knowledge.
9. **Monitor your children's online activity.** Limit your children's time spent online. Install and use parental controls software that allows you to monitor your children's online activity as well as prevent them from accessing undesirable web sites and sharing personal information via online communications.
10. **Make regular backups of critical data.** Keep a copy of important files on removable media such as Zip disks, recordable CD-ROM disks (CD-R or CD-RW disks), or external hard drives. Use software backup tools if available, and store the backup disks in case of an emergency.

Keep Important Emails out of SPAM – Senders and Recipients

Keep Important Emails out of SPAM - Sender

1. Be Compliant with the CAN-SPAM Act

- If you are sending "any electronic mail message, the primary purpose of which is the commercial advertisement or promotion of a commercial product or service," then you must comply with the following 7 main requirements (or face penalties up to $16,000) [5]:
- Don't use false or misleading header information
- Don't use deceptive subject lines
- Identify the message as an ad
- Tell recipients where you're located
- Tell recipients how to opt-out of receiving future email from you
- Honor opt-out requests promptly
- Monitor what others are doing on your behalf
- If your email contains only transactional emails or relationship content, then you are exempt from these rules; however, you must still not include false or misleading routing information.

2. Avoid Spam Trigger Words and Phishing Phrases

- Unfortunately, there is no complete list of spam trigger words. Further, it is not always the case that your email will end up in the spam filter simply by using a so-called trigger word.
- The key thing to remember, is that a spam filter is trying to remove commercial advertisements and promotions. So generally, words that are common in such emails should be avoided or used sparingly. That said, take a look at these 100 Spam Trigger Words & Phrases to Avoid.
- Phishing emails are designed to steal your identity by getting you to click on a fraudulent link. The most common method is for the email to be disguised as a legitimate email from a service you trust, such as your bank or a website you frequent. Thus, you want to avoid using phrases that are common to phishing attacks. At 24HourSupport.com you will find a short list of common phishing phrases along with references for further investigation.

3. Include a Text Version of Your Email if You Are Sending HTML Emails

- This is a common, and easily preventable, cause for landing in the spam folder. Not only is this a good practice for avoiding a spam filter, but it also covers you in the case where the recipient can not view HTML emails.

4. Use Permission Marketing Techniques

- Seth Godin coined the phrase "Permission Marketing," and offers his thoughts here. There you will find sound advice on the ideas behind getting your customers or potential customers to give you the permission to email. Take it a step further at the point of subscription and ask to be placed on their white list.

5. Use Spam Checkers Before Sending Your Emails

- Before sending emails out to your entire list, its worth the time to utilize a spam checking service.
- MailingCheck.com offers a free downloadable tool for Windows that uses SpamAssassin to check. If you prefer to avoid downloading any software, you can send email to the IsNotSpam.com service and they will also check a few other items important to email deliverability. Alternatively, ProgrammersHeaven.com uses a form-based solution to test your emails.

Keep Important Emails out of SPAM - Sender

6. Get Off Blacklists

- If your email server is on a blacklist, it becomes extremely difficult to reliably send email, especially to new people on your lists.
- The first step is to check if your email server is on a blacklist, following are a few free services:
- Free Email Blacklist Lookup
- Email Blacklist Check
- Spam Database Lookup
- If you find that you are on a blacklist, you will need to follow up with the website that has added you to their blacklist. That information is provided by the tools listed above.

7. Maintain a Good Text to Image Ratio

- It is usually best to not include images at all; however, if you must include images, here are some tips:
- Do not send any image-only emails
- We suggest that for every graphic, include at least two lines of text
- Optimize your images the best you can
- Use well formed HTML for email

8. Avoid Spam Traps

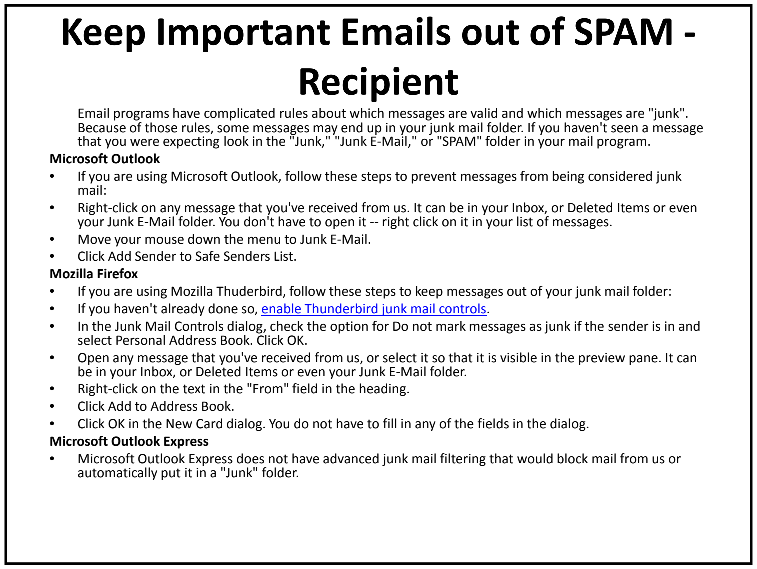
- Spam Traps are email addresses that are flagged by ISPs as being no longer used by a human, so it then stands to reason that there could have been no opt-in. To avoid including a Spam Trap email in your mailing list, use a opt-in process and do not buy lists from email brokers.

9. Avoid Large Attachments and Certain Attachment Types

- In general, .jpg, .gif, .png and .pdf attachments are safe to send, provided you include some content in the email as well. However, executable attachments such as .exe, .zip, .swf, etc. should be avoided entirely. Generally, you should not send attachments to people on your list that are not expecting them.
- If you need to email a large attachment or an attachment type that usually can be flagged as spam or trigger virus scanners, we recommend a service such as DropBox.com. If the attachment contains sensitive data, you may consider using your company's secure FTP server.

10. Make Sure Your DKIM, SPF, Sender-ID and Domain Keys Are Setup Properly

- You will want to make sure your email server supports these protocols (DKIM, SPF, Sender-ID and Domain Keys) and that they are properly implemented.
- This alphabet soup helps ISPs determine the authenticity of your email from a technical perspective. To make sure yours are setup properly try using IsNotSpam.com's checking service.
- If you want to dig deeper, here are the definitions:
- DomainKeys Identified Mail (DKIM)
- Sender Policy Framework (SPF)
- Sender-ID
- Domain Keys
- **Bonus Tip: Use a Email Delivery Service**



Keep Important Emails out of SPAM - Recipient

Email programs have complicated rules about which messages are valid and which messages are "junk". Because of those rules, some messages may end up in your junk mail folder. If you haven't seen a message that you were expecting look in the "Junk," "Junk E-Mail," or "SPAM" folder in your mail program.

Microsoft Outlook

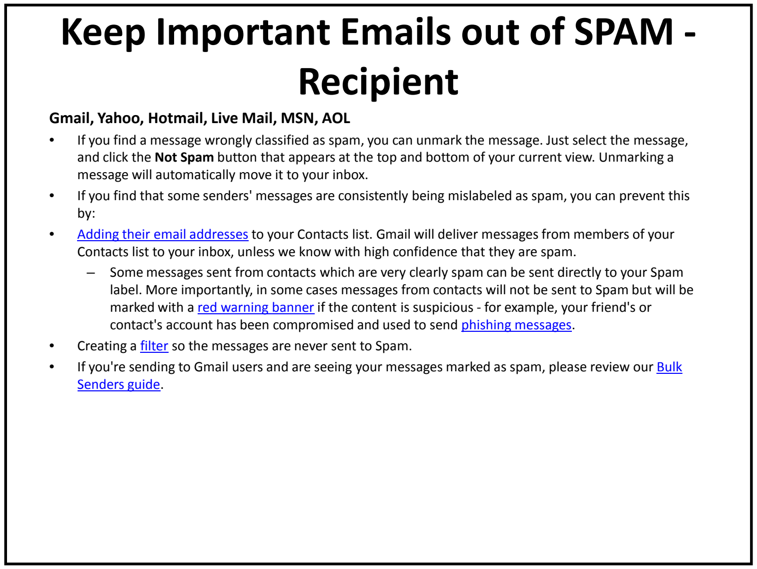
- If you are using Microsoft Outlook, follow these steps to prevent messages from being considered junk mail:
- Right-click on any message that you've received from us. It can be in your Inbox, or Deleted Items or even your Junk E-Mail folder. You don't have to open it -- right click on it in your list of messages.
- Move your mouse down the menu to Junk E-Mail.
- Click Add Sender to Safe Senders List.

Mozilla Firefox

- If you are using Mozilla Thuderbird, follow these steps to keep messages out of your junk mail folder:
- If you haven't already done so, enable Thunderbird junk mail controls.
- In the Junk Mail Controls dialog, check the option for Do not mark messages as junk if the sender is in and select Personal Address Book. Click OK.
- Open any message that you've received from us, or select it so that it is visible in the preview pane. It can be in your Inbox, or Deleted Items or even your Junk E-Mail folder.
- Right-click on the text in the "From" field in the heading.
- Click Add to Address Book.
- Click OK in the New Card dialog. You do not have to fill in any of the fields in the dialog.

Microsoft Outlook Express

- Microsoft Outlook Express does not have advanced junk mail filtering that would block mail from us or automatically put it in a "Junk" folder.



Keep Important Emails out of SPAM - Recipient

Gmail, Yahoo, Hotmail, Live Mail, MSN, AOL

- If you find a message wrongly classified as spam, you can unmark the message. Just select the message, and click the **Not Spam** button that appears at the top and bottom of your current view. Unmarking a message will automatically move it to your inbox.
- If you find that some senders' messages are consistently being mislabeled as spam, you can prevent this by:
- Adding their email addresses to your Contacts list. Gmail will deliver messages from members of your Contacts list to your inbox, unless we know with high confidence that they are spam.
  - Some messages sent from contacts which are very clearly spam can be sent directly to your Spam label. More importantly, in some cases messages from contacts will not be sent to Spam but will be marked with a red warning banner if the content is suspicious - for example, your friend's or contact's account has been compromised and used to send phishing messages.
- Creating a filter so the messages are never sent to Spam.
- If you're sending to Gmail users and are seeing your messages marked as spam, please review our Bulk Senders guide.