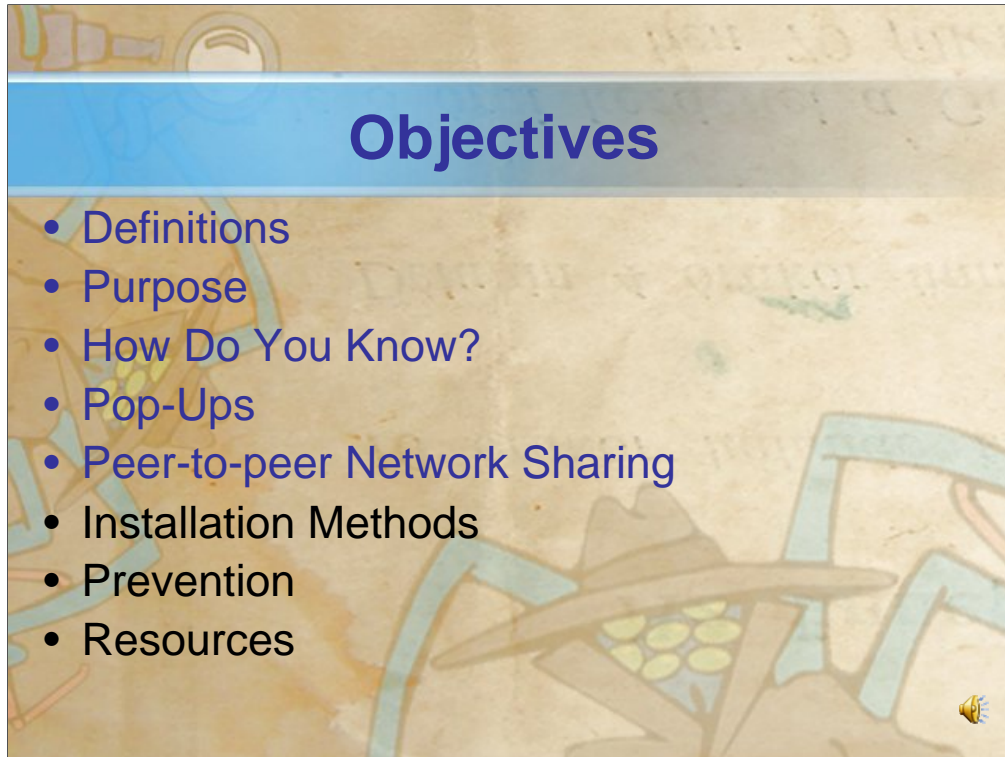


Welcome to Part 1 of the online course, Spyware and Adware – What's in your computer?

Are you being bombarded by advertisements on your computer, has your browser home page changed on it's own, is your operating system loading very slowly, are there programs loading you haven't seen before, are you constantly receiving error messages and registry errors? If you answered yes to any of these questions – you, along with 88% of consumer computer users, are most likely the victim of adware or spyware.

Disclaimer

- This course is designed for **Windows** operating system clients
- This course is not relevant for Mac OS clients



This course is the first of a two-part series on Spyware and Adware. We have created this course to help you better understand spyware and adware so that you can protect yourself from this parasite. All of the objectives listed will be covered in the complete course. In part 1, the following topics will be discussed:

- Spyware and adware will be defined.
- We'll discuss the malicious intent of spyware and adware
- Symptoms of spyware and adware will be explained so you will know if you are infected
- And we will explore the hidden dangers of pop-ups and peer to peer networking

“State of Spyware” Report

- Nine out of 10 PCs connected to the Internet are infected with spyware or adware
- 88% of consumer computers had some form of unwanted program (Trojan, system monitor, cookie or adware)
- 87% of corporate PCs had some form of spyware

A state of spyware report was conducted and the results indicated that 9 out of 10 pcs connected to the Internet are infected with spyware or adware.

88% of consumer computers contained some form of an unwanted program and the results weren't much better for corporate PCs – 87% of those had some form of spyware on them!

Clearly, these numbers are alarming and demonstrate the need to educate every computer user on the dangers of spyware and adware.

Definition - Spyware

Any software that covertly gathers user information through the user's Internet connection without his or her knowledge, usually for advertising purposes.

Spyware is any software that covertly gathers user information through the user's Internet connection without his or her knowledge, usually for advertising purposes. Spyware applications are typically bundled as a hidden component of freeware or shareware programs that can be downloaded from the Internet. Once installed, the spyware monitors user activity on the Internet and transmits that information in the background to someone else.

Spyware – What Is Its Purpose?

- Tracks your computer usage
- Collects personal information
- Reports on web sites visited
 - Builds a marketing profile for the user to sell “targeted” advertisements
 - Results in targeted e-mails sent to the user
- Installs components that affect your system performance or take up bandwidth
- Violates your privacy

As we said, spyware operates without the consent of the user, therefore, it's important to be aware of the effects of spyware and what specific behaviors to look for.

First, spyware will track your computer use and collect personal information. It will report back on web sites you have visited in order to build a marketing profile on you. This profile is then used to sell targeted advertisements. Have you ever wondered why you get advertisements for specific products which are related to your hobbies – well, it isn't just a coincidence. The ads are based upon a marketing profile that was created for you.

Spyware will also install software and other components that affect your system performance. You may notice that your computer appears to be very sluggish and it takes forever to perform certain operations that previously only took a few seconds. This is an indication that spyware could be running on your computer.

In short, spyware violates your privacy by tracking your browsing activity and possibly even capturing every keystroke you type on your computer! It can use your PC to dispatch spam, exploit your e-mail address book for spam, shop illegally online using your credit cards, access your bank account, be used for the purpose of identity theft, and so on - the list is almost endless.

Symptoms of Spyware – How Do You Know if You Have It?

- Computer crashes
- Home page has changed
- New toolbar installed automatically
- Browser settings have changed
- Large number of pop-up ads display – even when not in the browser
- Decreased system performance
- Something “new” on system
- Unidentified toll charges on phone bill

It is very important to be able to identify the symptoms of spyware in order to determine if your computer has been compromised. We have already touched upon some of the symptoms, but let's review the list of what to look for:

First, if your computer keeps crashing that is a good sign that you may have a spyware infection. Another good indicator is if your home page has changed on its own or if a new toolbar has been installed automatically. You will find this new toolbar in your Internet browser. Frequently, people are not even aware of this new toolbar so it's important to take a good look at your Internet browser and check for anything unusual.

In addition, your browser settings may have changed without any action on your part. One of the most annoying and obvious signs of spyware is a constant bombardment of pop-up ads. These ads will appear to multiply like bunnies! Sometimes, the pop-up ads may appear even when you are NOT in the browser. We will discuss pop-ups in greater detail in a few minutes.

As mentioned earlier, decreased system performance is another good indicator that you have become the victim of spyware. You may also notice something “new” on your computer. Perhaps when you click on Start-Programs you notice a new program is present that you didn't install.

If using a phone line connection and you notice unidentified toll charges on your phone bill, that could be an indication that the spyware is using a stealth dialer to call overseas.

Spyware Example: Bonzi Buddy



Here's an example of a popular spyware program, Bonzi Buddy. Users are invited to install Bonzi Buddy on their computer – he seems harmless enough as depicted in this description from the Bonzi website:

He will explore the Internet with you as your very own friend and sidekick! He can talk, walk, joke, browse, search, e-mail, and download like no other friend you've ever had! He even has the ability to compare prices on the products you love and help you save money! Best of all, he's FREE!

Most people would think this is a great add-in to download – and besides, it is FREE. Well, free does come with a price tag – and trust me, it can be a pretty high price tag at that!

Spyware Example: Bonzi Buddy

- Spyware program targeted at children
 - Children often install the software – looks like a fun toy
- Computer speed, privacy, ease of use all adversely affected by installing

Note: The Bonzi Buddy site was discontinued in 2004

As you might imagine from the description, Bonzi Buddy is targeted at children. Children often install software that looks like a fun toy – and what parent would have a problem with their son or daughter installing free software. Well, that's just what these companies are counting on!

In reality, computer speed, privacy, and ease of use are all adversely affected by installing Bonzi Buddy. Sure, you didn't have to pay in order to install Bonzi Buddy, but you will pay a price in terms of your computer performance and privacy!

In addition, Bonzi buddy automatically sets your home page to www.bonzi.com

Please keep in mind that this example is for educational purposes – **Warning: Bonzi Buddy site contains spyware and may not be safe to visit !**

Definition - Adware

Software that goes beyond the reasonable advertising that one might expect from freeware or shareware.

Adware is software that goes beyond the reasonable advertising that one might expect from freeware or shareware. Typically, adware is a separate program that is installed at the same time as a shareware or similar program. Adware will usually continue to generate advertising even when the user is not running the originally desired program.

Adware – What Is Its Purpose?

- Advertising-supported software
- Frequently “free” software comes with adware
 - Alternative to paying registration fees
 - Bombarded with advertisement pop-ups
- Runs in the background
 - Acts as a “mole”
 - Information is logged and used to create a user profile

Adware is basically advertising-supported software.

Some companies provide "free" software in exchange for advertising on your computer. It's how they make their money. In other words, as an alternative to paying registration fees for downloading a product you will be bombarded by advertisement pop-ups – it's the trade-off for the “free” software.

Adware runs in the background and will act as a mole. Your browsing habits are tracked and logged - then used to create a profile. Once again, this profile is used to direct targeted advertising.

End User License Agreement

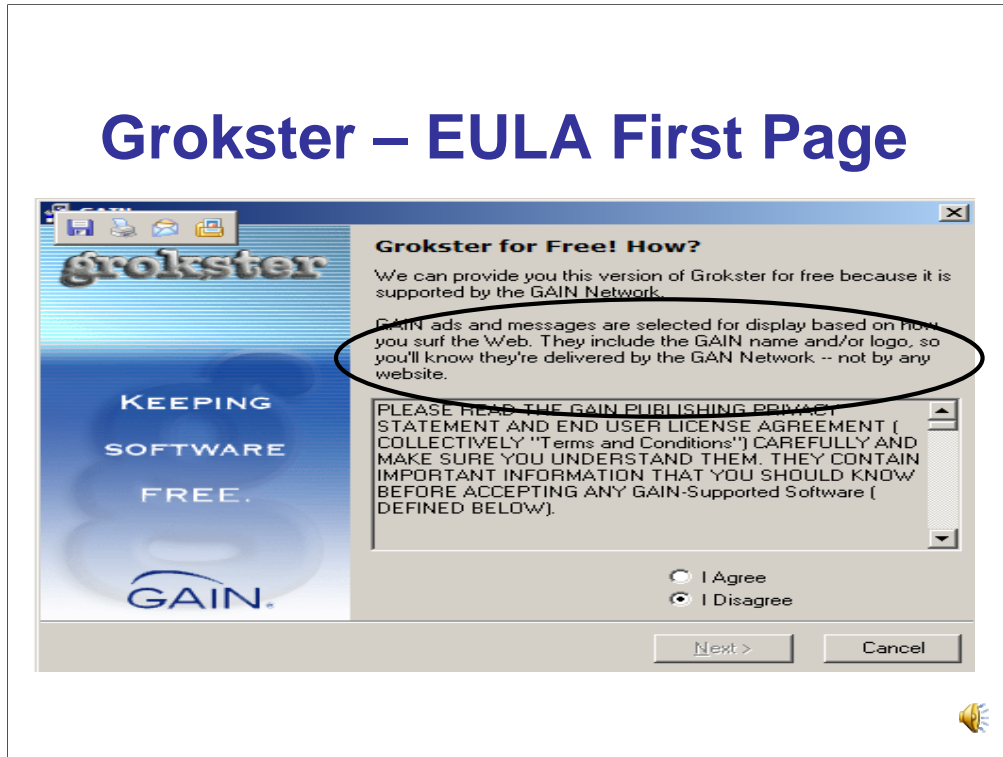
- EULA = End User License agreement
- Read the license agreement!
- Examples:
 - Claria's Gator EULA when installing as part of a bundle with Kazaa:
 - 56 on-screen pages
 - 5,541 words
 - WhenU (Bear Share)
 - 45 on-screen pages

EULA stands for End User License agreement and is the type of license used for most software. The EULA specifies the details of how the software can and cannot be used and any restrictions imposed by the manufacturer. It is very important that before installing any piece of software you thoroughly read and understand the license agreement. Now these companies are aware of that, which is why the license agreement will be quite lengthy, confusing, and possibly unintelligible – they are hoping you won't take the time to read it in its entirety – and even if you do read it, you won't be able to understand what it really says. Therefore, if you don't fully understand the license agreement (or if you don't want to take the time to read it) – you should not be installing FREE software! Remember, free does come with strings attached!

Let's look at some of these license agreements. The EULA for Gator when installed as part of a bundle with Kazaa is 56 pages long and consists of 5,541 words. To put that into perspective, the US Constitution is 4,616 words in length.

As another example, When U has a 45 page EULA. Certainly, they aren't planning on anyone reading all those pages!

Grokster – EULA First Page



Here is an example of the first page of the Grokster EULA. Notice it does state that the gain ads and messages displayed are based upon the individual's surfing habits!

Adware – How Do You Know?

- Disrupts browsing
 - Pops up context-related promotions
- Decreased system performance
 - Computer slows down
- Pop-up advertisements multiply

The adware will also result in disrupted browsing as context-related pop-ups are displayed.

In addition, you may notice a decrease in your system performance. For example, your computer may take twice as long to boot.

Pop up Advertisements may also continue to multiply – interrupting your browsing and becoming a nuisance.



ShopAtHome is an example of adware. The following is a screen shot taken from their web page.

ShopAtHome - Adware Example

- Can silently download, install and run new software
 - Includes updates of its software
- Monitors Internet usage and displays pop-up advertisements
- Modifies browser settings

ShopATHome can be silently downloaded and installed on your computer. In addition, as software updates are available – these are also downloaded without the user's knowledge.

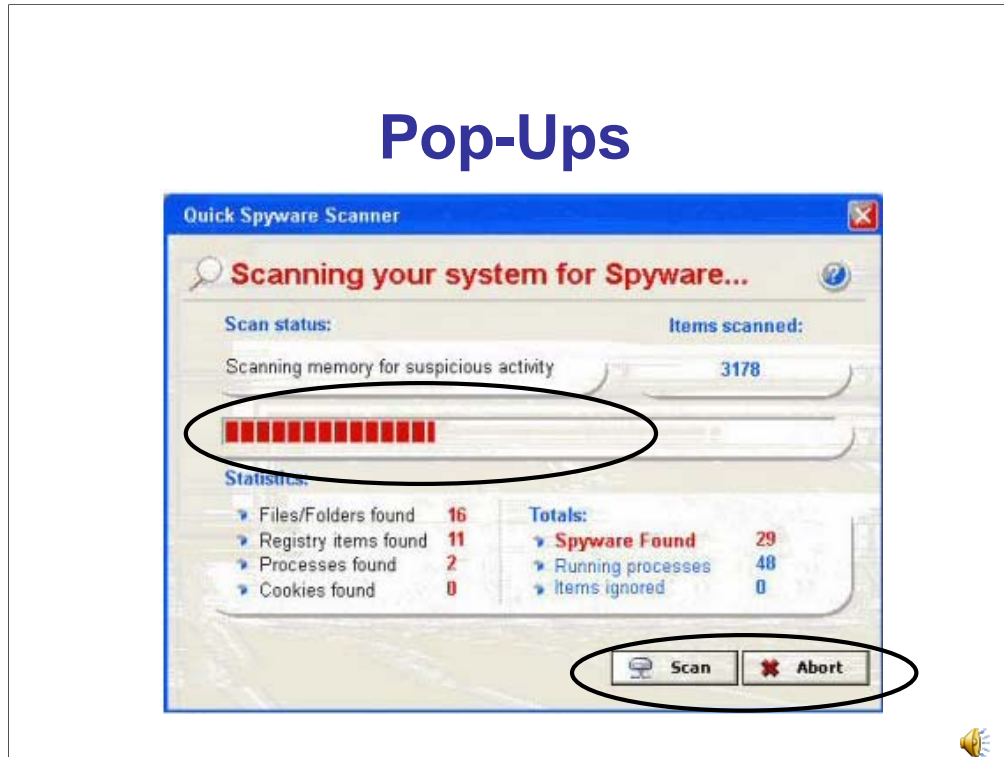
This software monitors Internet usage and will display pop-up advertisements. In addition, it can modify browser settings.

Pop-Ups

- Ads – want to sell something
- Clicking anywhere on pop-up may trigger installation of spyware
 - Program downloaded without your consent or knowledge

I'm sure everyone has seen a pop-up. They frequently come in the form of advertisements or games enticing you to hit the bullseye. Some pop-ups are disguised to look like system messages or warnings that your privacy may have been violated. To many people pop-ups are just a nuisance. However, those innocent-looking pop-ups can also install spyware programs on your computer without your knowledge.

Pop-Ups

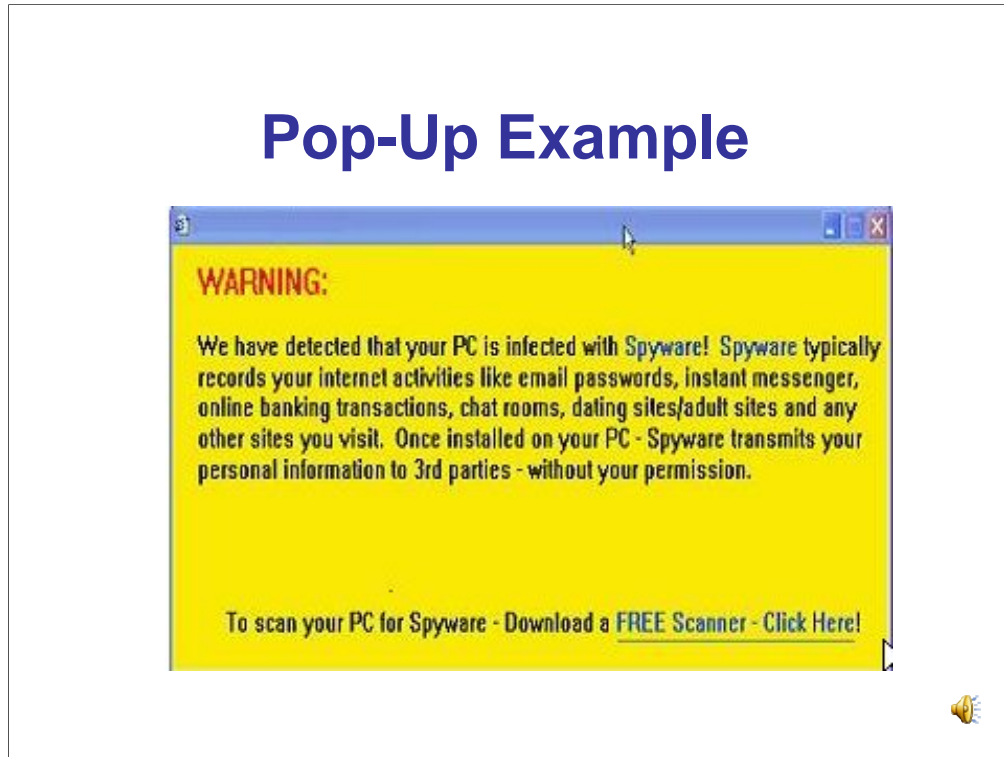


Pop-ups frequently have buttons to click on – such as OK, Cancel, Abort, or Continue. What you don't know, is the wording on those buttons may have nothing to do with what really happens when you click on them. In many cases, clicking on one of those buttons will cause a program to begin downloading onto your computer – without your knowledge or consent. Therefore, NEVER click on any button you see in a pop-up. The only button you should click is the standard close button (the X) in the upper right hand corner.

In this example, the pop-up advertisement is pretending to scan your computer and check for spyware. Notice the use of animated graphics with the status bar and the Scan and Abort buttons – these graphics are used to convince you that this is a legitimate system scan, when in fact, it is NOT.

Be warned – pop-ups are dangerous!

Pop-Up Example



Here's a picture of a pop-up telling the user their pc is infected with Spyware. They are hoping to scare them into clicking on the Free Scanner link. Even if they didn't have spyware installed on their computer- they will, as soon as they click on that link!

Beware – the creators of these pop-ups are very good at tricking you into clicking the links on their pages – don't fall for it!

Peer-to-Peer Networking

- File-sharing software available freely on the Internet
- Allows computers to connect with each other and directly access files from one another's hard drive
 - Exchange files from one another
 - Allows for sharing of music files **as well as personal files**



Peer-to-peer network sharing is also worth discussing. Such file-sharing is freely available on the Internet. This type of software allows computers to connect with each other and directly access files from one another's hard drive. In this manner, users exchange files with one another.

Although the purpose is primarily for the sharing of music files, peer-to-peer file sharing allows for the sharing of personal files as well. That's right, don't think that by opening up your computer to anyone on the peer-to-peer network that you are strictly limiting them to music files. Have a credit application saved on your hard drive, download some work to take home that includes student social security numbers or other personal information? Well, you may have just made those files freely available to anyone who uses the peer-to-peer file network.

File Sharing Scenario 1

- Mary downloads free version of file-sharing program (i.e. Kazaa, Limewire, Morpheus)
 - Mary uses her new file-sharing program to download music files
 - The music file that Mary downloads also contains key logging spyware which installs itself on her computer and captures her every keystroke

To better clarify peer-to-peer networking, let's take a look at a couple of scenarios. In both scenarios, our victims, have installed a free file-sharing program - such as Kazaa, LimeWire, or Morpheus.

In our first scenario, Mary searches for and downloads music files using her new file-sharing application. However, when Mary downloads a music file she also unknowingly installs keylogging spyware which captures her every keystroke.

This scenario demonstrates one of the dangers of using Peer to Peer applications - it is difficult, if not impossible, to verify that the source of the files is trustworthy. These applications are often used by attackers to transmit malicious code. Attackers may incorporate spyware, viruses, Trojan horses, or worms into the files. When you download the files, your computer becomes infected.

File Sharing Scenario 2

- John unknowingly saves a copy of his recent loan application to the “shared folder” on his computer
 - Now, John’s personal information is available to anyone on the file-sharing network via his loan application
 - Once the information has been exposed, it's difficult to know how many people have accessed it

The second scenario has John unknowingly saving a loan application to the shared folder on his computer. This makes his personal information available to anyone on the file-sharing network.

This demonstrates another danger of Peer to Peer applications - you may be giving other users access to personal information. Whether it's because certain directories are accessible or because you provide personal information to what you believe to be a trusted person or organization, unauthorized people may be able to access your financial or medical data, personal documents, sensitive corporate information, or other personal information.

Peer-to-Peer Networking Risks identified by US-CERT

- Installation of malicious code
- Exposure of sensitive/personal information
- Susceptibility to attack
- Denial of service
- Prosecution

US-CERT – the National Cyber Alert System has listed the security risks posed by sharing files using peer-to-peer networks. These risks include:

The installation of malicious code. This risk was identified in our first scenario. As we saw from this example, it is difficult, if not impossible, to verify that the source of the files you are sharing are trustworthy. Frequently, attackers use these applications in order to transmit malicious code. Spyware, viruses, worms, or Trojan horses can be incorporated into the files so that anyone who downloads them will be infected.

The second major security risk is the exposure of sensitive or personal information. If you remember, this risk was identified in the second scenario. Just by using a peer to peer application you may be giving others access to your personal information. This means others may be able to access your financial or medical information, personal documents, work-related information and documents, etc. In addition, it's difficult to know who has accessed this private information – making the security risk even greater. In summary, the easy availability of your personal information to others on the peer-to-peer network increases your risk of identity theft.


Third, using peer to peer applications increases your susceptibility to attack. Some of the applications may ask you to open certain ports on your firewall in order to transmit the files. This in turn, can give attackers access to your computer by taking advantage of vulnerabilities that exist in the peer-to-peer application. The end result – your computer is attacked!

Denial of service is the fourth security risk. Downloading files causes significant network traffic and relies on certain processes on your computer. This can reduce the availability of certain programs on your computer and may limit your access to the Internet.

Finally, files that are shared via peer-to-peer applications may include pirated software, copyrighted software, or pornography. Even if you download these files unknowingly, you could be faced with fines or other legal action.

Popular Adware/Spyware Programs

- Weatherbug
- Gator
- iMesh
- BargainBuddy
- eDonkey
- Morpheus
- Grokster
- Comet Cursor
- Kazaa (paid version free of adware)
- Limewire (paid version free of adware)
- Complete list:
http://www.spywareguide.com/creator_list_full.php



In this part of the course, we have provided you with some examples of adware and spyware.

Keep in mind that adware and spyware may be bundled or hidden in various types of programs – such as screen savers, games, utilities, weather updates, etc. Therefore, it is important to exercise extreme caution before downloading free software.

We have listed some of the popular adware/spyware programs such as Weatherbug, Gator, iMesh, Bargain Buddy, EDonkey, Morpheus, Grokster, and Comet Cursor. Some of the software vendors do offer an adware-free version that is available if you purchase the product, rather than downloading the free version. These include Kazaa and Limewire.

This list is changing as companies respond to pressure to remove the spyware and adware from their products.

For a complete list, you may wish to visit the web address referenced on this slide. This list is updated constantly, providing a good resource to check software against prior to downloading and installing on your computer.

Record Course Completion

- Click the following link to have this course added to your training record:

<http://survey.uakron.edu:2929/2wV3GFE/Link.html>

NOTE: Failure to click the link and complete the necessary information will result in your course completion being unrecorded!



Part 1 Conclusion

To advance to Part 2 click the link below:

<http://video.uakron.edu:82/train/Security/Spyware/SpywarePart2.htm>

Questions?

pstrain@uakron.edu



This concludes Part 1 of Spyware and, Adware – What's in Your computer!

Please – don't forget to watch Part 2 of this course. Part 2 will explore the methods used to install adware and spyware and provide some best practices in order to prevent this software from being installed on your computer. In addition, many valuable resources are provided.

Should you have any questions, you may direct them to pstrain@uakron.edu