

1. I received a notice saying that my Internet connection was used to download infringing material. What should I do now?

The notice contains the name of the infringing file(s) accessed using your Internet connection. Please search for and remove the infringing file(s) from your computer(s). Also, if you or another member of your household used a P2P (peer-to-peer) software client to download and/or share the file(s), be sure to remove the infringing file(s) from that software client as well.

For more information about copyright infringement and places you can go to purchase access to legitimate downloadable copies of video games, please visit <http://www.theesa.com/public-policy/intellectual-property/content-protection/>.

2. I did not download the infringing content described in this notice. Why did I receive this notice?

When you access the Internet, your Internet Service Provider (“ISP”) assigns a unique Internet Protocol or “IP” address to your computer. That IP address can be used to identify the computer you are using to access their services. You received this infringement notice because an IP address assigned to a computer used your Internet account to upload or download infringing material on the date described in the notice.

If you have checked all of your computers/devices and cannot find the infringing content, then the following may explain why you received the notice:

1. Do other members of your household or people who visit your home use your Internet connection? If so, these individuals may have downloaded the infringing file(s). Check (or ask them to check) their computers/devices to find out whether they have downloaded the infringing file(s), and if they have, ask them to delete the file(s). It may be helpful to show the notice to anyone who uses your Internet connection often, and tell them they should not download illegal copies of copyrighted material (videogames, movies, music, etc.) when they are using your Internet connection.
2. If you have a wireless Internet connection, someone outside your home may be using your network without your knowledge. Securing your wireless router using WPA/WPA-2 encryption is one important step to take if you want to prevent people from using your Internet connection without permission. If you have any questions about how to secure your router, contact the router manufacturer or your Internet Service Provider and let them know that you need help setting up a WPA/WPA-2 password for your router.

3. What if I didn’t know I was uploading copyrighted files?

You – or someone else who uses your computer – may have installed Peer to Peer, or “P2P,” software on your computer to exchange files with other Internet users. When files are placed in the “shared” folder of the P2P software, they are available for other users to download from your computer. Unless you have been authorized by the copyright holder to distribute those files, each time someone

downloads a copyrighted file from that “shared” folder, your Internet account is being used to illegally distribute those files. If you have P2P software on your computer, you should either remove the software completely, or delete any files from the “shared” folder that you have not been authorized to share.

If you want to search for P2P software on your devices, but do not know how to do it, you might start by typing the phrase “is there P2P software on my computer” into a search engine, and then use the search results to find instructions for determining whether P2P software has been installed on your computer.

4. My wireless router uses WEP encryption, shouldn't that prevent others from using my connection?

WEP encryption has inherent flaws that can allow a person to gain unauthorized access to your network. WPA and WPA2 are newer standards less vulnerable to intrusion. If your router does not support the WPA /WPA2 encryption standard, replacing it with one that does will help you prevent people you don't know from using your Internet connection. For more information about improving the security of your computer, you can refer to the United States Computer Emergency Readiness Team (US-CERT) website at www.us-cert.gov/. Information about securing your home router is available at: <http://www.us-cert.gov/security-publications/small-officehome-office-router-security>

5. The IP address on the notice does not match my current IP address. Have I received this notice in error?

Your ISP assigns a unique IP address to your account, which can be used to identify activity related to your account on their network. These IP addresses have a “lease time,” which means that the IP address may expire when that lease time ends. Depending on your ISP, you may be assigned the same IP address after the original lease has expired, or you may get a different IP address. The IP address referenced in the notice you received from your ISP is the IP address they assigned to your account on the date and time when your account was used to upload or download infringing files.

6. My ISP disabled my Internet connection because of these notices. What should I do?

Your ISP, not the ESA, sent this notice to you. You should read that notice carefully and decide whether you need to contact your ISP directly.

You should also follow the instructions for searching for and deleting the infringing content referenced in the notice (see FAQ # 1 and # 3, above). If you have a wireless Internet connection, make sure your wireless router is secure (see FAQ # 2, above). Once you have taken both of these steps, contact your ISP.

7. I have removed the game listed in the notice I received. Why do I keep receiving notices on that same title?

The infringing game might have been removed from the folder where you store game files on your computer, but your P2P software client may have stored a copy of the file, making it accessible to other P2P users. Make sure to remove the file from the P2P software client to prevent future notices from being sent.

8. Am I being sued?

No, the notice you received from your ISP is not notice that you are being sued. Instead, it serves as a warning that your computer has been used to unlawfully download or share copyrighted materials. It is intended to advise you that this activity is occurring, inform you that it is illegal, and provide you with the opportunity to stop the infringing activity from happening.