“Click Accept”: Your Software License Survival Guide

By CopiaTECH
September 4, 2007

No longer worried about viruses, Trojan horses, worms, identity theft, and phishing scams? Do you feel as if you have gone the distance to protect your company and your network from impending doom? Sleep at night? Well, there is one tiny itty bitty little detail that can be a can of worms that makes a good old virus look quite friendly, the software license agreement. Yes, the EULA or End-User License Agreement. How can something from the people you have given your hard budgeted dollars to possible cause harm? We will tell you…

Reading EULA's is the most boring as well as time-consuming job you can imagine, if done right. Though boring, this is a very necessary task done for the protection of your network. Neglecting it can make all your other measures of IT Security toothless. These agreements contain terms and conditions that you need to follow or agree to, in order to use particular software on your network, desktops, laptops and servers. They are not directly harmful but can lead to disasters, if you neglect them. These agreements actually contain the details of conditions and risks that you may face while using the associated software. Let us discuss the risks that you invite if you neglect the EULAs.

Ok, now it is confession time. All of you out there that click "accept" and move on about the arduous task of installing a bazillion copies of a program on your users computers or risk life itself by installing onto your servers, raise your hand. Go ahead, it is just us, nobody is looking.

Your network security is at stake and now you must be wondering how? One example is when the EULA asks you to allow the software publisher or a third party to track your activities on the net and in return you get to use the software for free. This is how a lot of spyware or adware gets legally loaded onto systems. It may also ask to share your private information or use your network for their interest. This can put your personal security, as well the security of the data stored in your computer, your network and business at a risk.

The publisher or a third party may use the information collected from you like your name, address, credit card number or your passwords etc. in some malicious activities that result in fraud. The only way to stay out of all these risks is to carefully read the EULA and understand it in detail before installing any software and consciously make a decision on sharing your private information, your company's information or access to company assets.

Understanding the term EULA

EULA is actually a legal document that acts as a contract between you and your software publisher. It contains all the terms and conditions that you and your publisher are bound to follow. There can be various points of concern that you need to take care of when reading a EULA. For example, if it says that the software is only for a single computer then there is no problem as long as you only use a single copy on a single machine. However, if it says that all your activities on the internet will be monitored by a third party or the third party will be allowed to collect vital information from your computer, or will be allowed to access your computer, then be alarmed. Accepting such terms will bring risks along with the software.

You should be careful not only while installing the software, but from the time of purchasing it.

You can agree to a EULA in many different ways and the presentation is not always clear. There was a time where a user had to scroll to the end of the terms and conditions prior to being able to accept. It was the publisher's way of trying to make people review the terms, but now it is made quite simple. One of the more obtuse methods is when you enter software keys to activate a program. May licenses are written that to do so is to agree to the terms and conditions, even if you have never read them!

Many of the ways that you agree to a EULA that may not as if they should be binding are:

- When you click the "I accept" button during the installation process
- When you open the shrink wrap of the software
- When you open the seal of the software CD
- When you send your registration card to the publisher, snail mail or electronically
- When you install the software
- When you start using the application

If you do not agree to any of the terms or conditions you can easily refuse it, but then you are not allowed to use the software! Unfortunately, there is not an easy way to disagree with specific line items or accept a EULA partially.

Importance of EULAs

There are a number of factors mentioned in the EULA that you must seriously considered before installing the software, and some of these are mentioned below.

- **Legally binding:** EULA's are very much a legal document that have to be followed and can be challenged only in consumer law courts. Most of the large size EULAs contain so many legal terms and points that they are not easily understood. Concerning these, some of the consumer advocates have also challenged them in court and stated that the size and the language of the EULA are so designed that they discourage the consumer from reading them. In most cases, the verdict was in the favor of the software publisher, so you must always take it seriously.
- **Restrictions on the software use:** The most important clause that most of the EULAs contain is about the usage of the software. They can limit the number of systems on which you can install your software. They can also disable the reverse engineering of the software so that no one can use it to create a compatible or better software to compete with theirs. It may also restrict the users from testing the software and publishing the results.
- **Forced conditions:** Most of the software packages are available as a bundle of multiple software programs. Such bundles may or may not include all the software from the same publisher, as they mostly include third party software. In such cases, the EULA binds you to use either all of them or none. This third party software may ask you to agree on monitoring your activities or sharing your details or computer resources, or worse.
- **Limit your legal rights: M**ost of the EULAs state that the consumer cannot sue the publisher of the software for any damage caused by the software usage, as an example.

What to look for and take into consideration while reading a EULA?

Always read the EULA carefully and then decide what you want to share or exchange for the use of that software. This is critical as agreeing to share your resources and information is just the first step of risking your online security. Always be alert if you find the following clauses in the EULA:

- EULA asks you to allow the publisher or the third party to **monitor your online activity**
- EULA asks you to share your personal information with the publisher or the third party
- EULA asks you to share your computer resources with the publisher or the third party
- EULA binds you to follow the EULA of any other third party software

What measures should we take for our online security?

There are a few steps, if followed, which can help protect against all security and privacy risks that come with EULAs.

Some are discussed below:

- **Read the EULA carefully before the installation of the software**: Though it is quite boring and time consuming, be patient and read the EULA carefully. Know the details before installing the software, , the best way to protect you from EULA related security threats is personal knowledge.
- **Check out the publisher of the software:** Find out about the publisher and his/her reputation. Do a quick Google search on the name if you do not know them, and make sure nothing funny turns up. If you do not know who they are or you have even the slightest doubt about the publisher then take extra care and time to read the EULA.
- **Be mindful of your firewall prompts:** Most of us do not take the firewall alarms and notifications seriously. However, if your **firewall or desktop firewall** asks you before allowing certain data to pass through, then be on alert because it could be a signal of something foul to come. In such a case, read the EULA again and again to find out the reason for this traffic and allow it only if you are satisfied with what you find. Again, Google the name of the program and the publisher and dig deep to know why the program is going out on the net and triggering your firewall.
- **Be wary of software that is free, especially in case of peer-to-peer file sharing software:** Economist Milton Freeman said, "There is no such thing as a free lunch" and that applies to software. The publisher is usually getting something out of letting you have it free. So if your software is free then read the EULA repeatedly to find out what you have to do to use this software.

A Closer Look: EULAs, Security, and Privacy

Now we will discuss the real-life examples of EULAs and the security concerns that arise with them. Most of us just ignore the EULA and accept it without even a scant glance at it, for us detailed reading of it is not even in the cards. Thus, we invite risk to our network and business/employer. It is not that all software publishers want to cheat us or misuse the agreement. Sometime these cases also arise due to mismanagement of the software and partnership between the various parties involved in a bundle of software. Here, the primary publisher take things for granted and does not try to or fails to detect the bugs and loop holes in the attached software or related EULAs. The situation becomes worse when a EULA asks you not only to share your computer and details but also that of others in the network.

Monitoring Software EULAs

This real story is from a major university. In the year 2004, the IT department of the university detected a big trouble in their network. The trouble was actually a software used by most of the users to speed up their internet surfing and downloading speed and protected their emails from viruses. Now there was no problem with the software, but the problem lied in the adware that was attached to it. This adware was designed to collect the sensitive and private information about the user. This adware was also capable of reading information from encrypted files and SSL sessions. Now let us see what its EULA stated:

"…..{this software} monitors all of your Internet behavior, including both the normal web browsing you perform, and also the activity you may have through secure sessions, such as when filling a shopping basket or filling out an application form that may contain personal financial and health information."

After analyzing this threat, the IT department blocked the software and all the connections to it. It also redirected its users to a web page, which contained the detailed explanation on the problems of using this software and also the method to remove this software from the computer. Here the major concern for the department was the security of data traffic during the SSL sessions. Since the monitoring software was also **accessing the SSL encrypted data**, there was a severe security threat to critical university information, personal information, network IDs and passwords and federally regulated data.

With above example, one can easily understand how important it is to evaluate the EULA, and detect those that want to monitor your online activity. Think before giving your personal details and control of your system to a third party, which you never know. Do this for your personal safety and that of the entire network. This is your social responsibility as a good employee.

File-Sharing EULAs

Peer-to-peer (P2P) file-sharing programs are among the most popular and sought after software programs. But, with its popularity it also brings numerous threats for the online security of users. EULA's of such software mostly ask you to allow the publisher or the third party to monitor all your internet activity and share your personal information with its advertisers. It also asks you to share your computer resources with the third party and allow them to open directories on your hard disk. Third parties can use this directory as they want.

As an example: One P2P program had asked its users to install the attached bundle of software. This software converted the users' computers into a distribution channel for third-party software and the publisher's content.
Think seriously and then decide whether you want to give the control of one or more directories of your computer to unknown people and allow them to access these directories every now and then. Moreover, will you allow them to store their contents on your computer? That is clearly a scary thought. Who knows what is taken or left on your system or the network? Also, what is your comfort level about allowing any one to monitor all your online activities. Can you trust them and believe that those unknown people will limit their activity only to the allowed directories and will not try to access other directories or files in your system? Are you sure that they will not upload malicious files and viruses to your computer and then the network? Are you sure that your personal information will not be collected or misused by them? All these factors are discussed in a section below:

- Your system is more vulnerable to **Trojan horses and viruses**.
- Your personal data is on a severe threat.
- Your computer, in totality, is at a risk due to the extended exposure to malicious software.
- If the third party uses your computer in any illegal activity, then any tracing for such activity will lead to you and your computer, and not to the abuser.

Resource Sharing EULAs

In the above sections we have discussed threats due to monitoring and file sharing clauses of a P2P EULA. Now let us discuss a much bigger threat that may arise as a result of resource sharing EULAs.

It is a case in 2001, when a free internet service provider made a big gamble! The ISP expanded into supercomputing and used a very innovative but risky way to do it, of course the risk was all that of the users. The ISP changed the terms and conditions of its EULA to support the new aspirations. The revised EULA had following terms and conditions

- **Users are asked to allow the ISP to install software for this supercomputing venture.**
- **Users must keep their computer on 24 hours a day seven days a week to ensure the availability of resources for the supercomputing venture.**
- **Users where to make the modem available to the ISP servers for connections as needed by the servers for the super computing venture.**
- **Users were prohibited from removing the software or lose use of the ISP**

Just think of the users who had agreed to this revised EULA without knowing they have lost the control over their computer, which can now independently connect to internet. Always take care before giving even the slightest control of your system to a third party. Give an inch and you know they will take a mile, heck maybe even a country mile, which is apparently pretty long. The slightest control can allow the third party of completely reconfigure your computer and create many loopholes in your firewall and through your network. They can easily weaken your security and you did it unknowingly.

Third-Party Software and Cascading EULAs

After all the above discussions, let us discuss a very different case which can be very confusing! Here the EULA of the software states that you need to install or download the attached bundle of software and adware from the third party. It also states that you cannot disable the attached software or make any changes in its settings. Generally, a EULA does not contain the terms related to the attached third party software. The third party software usually has their own EULA. These EULA act as separate terms & conditions which may transfer rights to another third party for monitoring your online activity, etc.

Now understanding such EULAs becomes difficult for the users and they are trapped and locked into these agreements. In such cases you may end up in a situation where you cannot easily find out the risks that you are facing based upon the trail of license agreements.

An incident in 2002 can give you a better picture of the situation. Four popular file-sharing programs were found to be infected with Trojan horses. The Trojan horses were attached to the third party advertising software that was included in the bundle that included the file-sharing program and adware program. This happened due to the negligence of the third party adware, who failed to detect the Trojan that was included in software it bundled further downstream. The virus was in this downstream bogus application which contained W32.Dlder.Trojan. It attracted users in the form of an online contest. The users clicked with the hope of winning prizes, the Trojan horse got installed into their computer, and the rest is misery. The result of this was loop holes in the security system of users. This Trojan horse recorded the list of websites visited by the user and posted it to a website it was in league with.

When contacted, one of the chief technical officers for one of the file-sharing companies involved stated, "We rely on [the advertising partner] to deal with our ad deals and bundled software. We assumed that they did their homework on this package but that does not seem to be the case." And the public relations manager for one of the other file-sharing companies involved just said, "We were unaware of what this program did when we added it to our installs …."

Now with the above example it is quite clear that the software publisher will not always take all the necessary steps for your security. It is you who need to be extra careful when dealing with EULAs that have any clause related to Third party EULA's.

Steps for Protection!

EULAs are boring, but are as important as the anti-virus programs and firewalls for the protection of your network. Now in this section, we will discuss the necessary measures recommended by the experts for the EULA related issues on security and privacy.

Read the EULA

The first and foremost important step in the path of protection of your privacy and resources is carefully reading the EULA before installing any software. You may feel that it consumes a lot of time and is quite boring, but it is very important. I hope we have established that at this point.

If you feel that you don't have enough time to read the lengthy EULA at the time of installation of the software. You can copy it to a text file and abort installation. Later when you have enough time, you can patiently read it and then if you feel like agreeing to it, re-start installation. If you find one or more clauses of EULA confusing or have any doubt, you can anytime contact the publisher's customer service through its website and ask for the clarification.

Now here is one more situation to consider. In some software packets, it states that "**breaking the shrink wrap constitutes agreement**". In such a case how can you read the EULA and agree to its terms and conditions before opening it? The best solution to such a problem is, to have a close look at the package. It will contain the details of the publisher like a customer service number or website for the publisher and also the product details like its product code etc. Visit the website and search for the EULA of the software, as most of the publishers also publish the EULA of their products on their website. If you cannot find the EULA of the product in its website then directly contact the publisher and ask them where it is located or for a copy.

Consider the Software Publisher

Top publishers with popular software are rarely involved in questionable or malicious activities like unusual, misleading, or confusing terms and conditions in the EULA's for their software, because they have too much to lose. But, there is no guarantee without reading the EULA. Never blindly accept the reputation of a company and agree to their terms and conditions without a proper review. Always read the EULA of the software carefully, no matter how good the reputation or highly the popularity of the company may be.

And if you find the publisher of the software to be new, take extra care while reading the EULA of the software. Do a Google search on their name as well as the name of the program to be installed and see if there is any data available on others experience with them. Go through each and every point carefully; especially if it is bundled software.

Beware of Firewall Prompts When Installing Software

The **Firewall is the first application** that gives you a direct warning about a breech in your security system when a program tries to do something your rules do not allow. If the firewall finds any problem with the software, it prompts you at the time of installation by asking you to allow certain inbound or outbound connections. This is the time to ask yourself what this program is doing and why. Check out for what changes your software wants to make to your firewall settings. Proceed only if you don't find any problem in making the required change. Now why does the software want to change your firewall setting?

The answer to this question lies in the EULA of the software most likely. It may have a clause of monitoring your online activity. It may want to access your directories or resources. For any of these requests, the software will have to **create holes in your security system** by changing your firewall settings. Many people find that these things are not mentioned in the EULA of the primary software and even then the firewall asks for the permission to allow data to pass that previously had not been. In such cases check the attached bundle of software from a third party EULA. Sometimes there are also chances that rogue software or a file-sharing Trojan horse is attached to your software or in the attached bundle as discussed above. After this if you feel any doubt about the firewall settings; you should refer to the users manual or the installation guide accompanied with the software. In case of further confusion, or unavailability of the manual, directly contact the publisher of the software for clarification before allowing any changes. Better safe than sorry.

Some firewalls also have the option of one time or case by case connection. Such firewalls can be helpful when you are installing software that needs to connect to the server at the time of installation. If after reading the EULA, you find no harm in it, you can allow the connection once and disable it later.

Beware of "Free" Software

Last but not the least, always remember; nothing in life is free! There will be a **condition for the free software**, you just may not know it. These problems can come in many types of programs; peer-to-peer file sharing programs, games, screen savers, or any other program, it is never free. If they are not asking you for the money, they may be asking you for a non-monetary favor that can cost you much more. This favor is always discussed in their EULA in complete detail, which can be a compromise to your resources, privacy and security.

In the end always be careful when installing any new software, especially when it is free. Read the EULA every time you install any new software even if it takes time. For corporate applications consult someone that deals with that EULA day in and day out, your software reseller.

CopiaTECH has relationships with all the manufacturers it represents and it is our job to know the EULA inside and out and protect your business interests. Licensing software can be very confusing, whether you deal with it daily or it is your annual renewal and time to try to remember, "How do they license that again?"

Glossary

Ad ware: A software application that displays advertising when the program is running. The software may display ads in pop-up windows or a bar in the frame of the application window.

Back door: A back door is a means of access to a computer program that bypasses security mechanisms.
P2P: An internet network in which a group of computer users, each equipped with the same networking program, connect to each other and directly access files from one another's computers.

PGP: (Pretty Good Privacy) is a program used to encrypt and decrypt data, primarily e-mail, over the internet.

SSL: (Secure Sockets Layer) is a method for securing information exchange on the internet. SSL uses data encryption and digital certificate authentication to secure the information exchange.

Spyware: Adware that tracks user activity and passes it to third parties without the user's knowledge or consent.

Super-computing: Computing systems or schemes designed to handle extremely large databases or to perform a great deal of computation. Some supercomputing schemes involve clustering, in which many PC processors and drawn upon to perform the supercomputing tasks.

Trojan horse: A program in which malicious or harmful code is packaged inside apparently harmless software or data.

Zombie: A compromised web server on which an attacker has placed code that, when triggered, will launch with other zombies a denial-of-service attack.

Further Reading:

AusCERT. "File-Sharing Activity Part 1 of 2 - Security implications of using peer-to-peer file sharing software." May 20, 2002. http://www.auscert.org.au/render.html?it=2228&template=1.

Brandt, Andrew. "Click With Caution: User Licenses Get Tough." *PC World*. April 9, 2001. http://www.pcworld.com/news/article/0,aid,46764,00.asp.

Delio, Michelle. "What They Know Could Hurt You." *Wired News*. January 3, 2002. http://www.wired.com/news/privacy/0,1848,49430,00.html.

Garfinkle, Simson. "Software that can spy on you." *Salon.Com*. http://dir.salon.com/tech/col/garf/2000/06/15/brodcast/index.html.

McDowell, Mindi. "Reviewing End-User License Agreements." US-CERT. March 2, 2005. http://www.us-cert.gov/cas/tips/ST05-005.html.

Newitz, Annalee. "A User's Guide to EULAs." Electric Frontier Foundation. http://www.eff.org/wp/eula.php.

Rasch, Mark. "Is Deleting Spyware a Crime?" SecurityFocus. May 24, 2005. http://www.securityfocus.com/columnists/329