White Paper - October 2009

Cookies and Your Privacy

Anyone who uses computers today should be concerned about privacy and security. Any time your computer connects to the outside world, you run the risk of your important data being taken, misused, corrupted or destroyed. That's why it's important to guard against computer attacks with Anti-Virus and Anti-Malware software.

But there's an often overlooked threat from “cookies” and it's getting worse every day. It used to be that cookies were merely little pieces of innocuous information about the web site you visited so that you would have a more interactive experience the next time you visited the site. But, today, they have become much more than that with some predatory information sites. They have become a means by which to track your every move, your purchases, your habits, monitoring you and selling the information to vendors wishing to know how better to get inside your head to convince you to buy their merchandise.

So cookies are good, until they are misused. Which is getting worse lately. How so? Because you no longer even have to visit a site to get cookies from a 3rd party site uploaded to your computer without your express permission. What's more, with the advent of new enhanced multimedia software extensions to your browser, such as Flash and Silverlight technologies, you can now delete certain cookies and these multimedia programs still have the capability within them to put the deleted cookie right back onto your computer. These cookies are even *browser independent*, which means you can switch from one browser to another and the cookie information is still kept. So thinking that you can use, say Mozilla Firefox for sensitive websites, while using Microsoft Internet Explorer for your usual browsing is not a viable, safe method to avoid cookie trouble. Today’s browsers are no longer isolated any more.

To make matters worse, there's so many, literally hundreds, even thousands of cookies per day possible. So why not delete them all? Because some of them are important, because they come from the sites you want, they enhance your site visits. If you delete them all, you may find yourself re-entering your user information every time you visit your favorite sites.

The problem is the keeping the ones you don't frequent that you don't want to have any information about you separate from the ones you want to keep. It would take hours every day to keep up with it all – to keep your information safe and under your control.

That's where MAXA COOKIE MANAGER comes to the rescue. MAXA Cookie Manager is the most advanced and up-to-date method available to handle all known types of cookies, the bad ones, the good ones, even, the new varieties, like the browser independent cookies. And it can keep your information safe, while saving you time and money.

What is a Cookie?

A cookie is a small file with text data, sent by a website server to your web browser that stores information about you and your computer. It used to be and not that long ago that a cookie was less than 256 characters long, but today it can be much larger in size. Today, while HTTP cookies still have the size restriction, new types of cookie technologies allow even more storage.

Cookies are stored by the browser on the hard disk and usually have an expiration date. Some cookies only survive as long as the browser session, others have a lifetime of days, weeks, or even years. When a cookie reaches its expiration date, it is automatically deleted by the browser. Cookie technology allows a web server to leave data on the user's PC. You can consider this as an electronic crumb, left behind by the cookie. Since the web server cannot itself access a user's stable storage, it has to use the browser for this purpose, but can only record data that it holds already (e.g. current address, user PC, user input).

The next time you go to revisit the same web site, the data previously stored in the form of a cookie is automatically passed back to the web site.

What are the disadvantages or dangers from cookies?

Cookies though, are not viruses. They can't access your hard drive or mess up your computer like a virus can, it's just information. But that doesn't mean they're not important or dangerous. You get cookies when you visit web sites, but you can also get them any time an http request to the internet occurs, even from sites you've never explicitly visited and don't want. This also includes content that is loaded when reading an email message or from opening a document. Often, the user does not even notice that it's happening.

Many internet providers use dynamic IP addresses. This means that every new internet connection means a new IP address. This address is essential to identify a PC on the internet. The server only knows the address to which it should send the data requested, not the person who exists behind the address. However a server can now send a cookie to the browser with a unique user identity and give it a long lifespan. After the browser is closed, the cookie is stored and, the next time the user visits that site, he can be identified, regardless of whether he has been given a new IP address.

So the disadvantage of cookies is that they can be used to construct a profile of internet usage of individual users, showing their total internet activity patterns. Cookies become really irritating when personal data is linked to the user's surfing activities – all of this available because the user once entered his name & address, etc., via an input form on a web site. This creates a reusable profile of that user, which can be exploited by others without permission.

Why not just delete all the cookies?

You could delete them all, but then you would have to enter key pieces of information you want to be saved over again, such as login name, password, contact information, etc. That defeats the whole purpose of having cookies in the first place and will waste time, as well as being a big hassle. Some sites won't work at all if you reject all cookies.

What are 'normal' cookies?

Those which are transmitted in a HTTP-Request-Header when accessing a website and managed by the browser itself.

Are there other kinds of cookies?

Naturally, development does not stand still. **"Flash-Cookies"** are the most common b browser independent type at the moment. Their usage is steadily increasing. Almost all current methods of dealing with cookies are ineffective for Flash Cookies – except MAXA Cookie Manager. The Adobe Flash-player present on most PCs controls these "Local Shared Objects. Since the Flash-player is shared by all browsers, and its cookies are still there after normal cookies have been removed, this opens some interesting possibilities for assembling profiles of users.

Silverlight is Microsoft's counterpart to Flash. Here too, each Silverlight application can save and read up to 1 MB of data on the hard disk. This data is browser independent as well.

"Firefox DOM-cookies" first appeared in connection with version 2.0 of Firefox and allow files up to 5MB to be stored.

MS Internet Explorer also allows websites to insert larger files into the **UserData DomStorage** using Javascript.

How can cookies be controlled?

Most of the current browsers offer 'cookie management'. However, this is just not an easy task to do. It can either take too long, or just be too cumbersome to figure out easily. Also, browser independent cookies are not touched when removing standard browser cookies. This is why MAXA Cookie Manager is your best solution for handling the growing threat and irritation of cookies. With MAXA Cookie Manager you can easily manage not only regular cookies, but even the new generation cookies, simply and easily. MAXA Cookie Manager saves time, saves money, and eliminates the hassle of managing cookies.

What exactly is a Web Bug?

In a narrower sense, a Web Bug is a graphics on a Web page, Document or in an Email message, often invisible because only 1-by-1 pixel in size and in the same color of the background. Normally they are loaded from 3rd party servers. In a wider sense a Web Bug is every means of tracking what the user is viewing. MAXA Cookie Manager recognizes web bug cookies as a particular thread and allows to delete and to block them.

What are some of the uses of a Web Bug on a Web page?

Ad networks can use Web Bugs to add information to a personal profile of what sites a person is visiting. The personal profile is identified by the browser cookie of an ad network. At some later time, this personal profile which is stored in a data base server belonging to the ad network, determines what banner ad one is shown.

Another use of Web Bugs is to provide an independent accounting of how many people have visited a particular Web site.

Web Bugs are also used to gather statistics about Web browser usage at different places on the Internet.

They also support “Data Spills” (The accidental transmission or display of private online data to a third-party), when you fill out an online Form. This could create unwanted profile information about YOU and is out of control.

A Web Bug can also be used to log people who are reading messages in particular newsgroup. Such bugs might be used for example by investigators to track illegal activity. Web Bugs might also be used to monitor people in extreme political groups.

What kinds of uses does a Web Bug have in an Email message?

A Web Bug can be used to find out if a particular Email message has been read by someone and if so, when the message was read.

A Web Bug can provide the IP address of the recipient if the recipient is attempting to remain anonymous.

Within an organization, A Web Bug can give an idea how often a message is being forwarded and read.

Why are Web Bugs used in "junk" Email messages?

To measure how many people have viewed the same email message in a marketing campaign.

To detect if someone has viewed a junk email message or not. People who do view a message are added to even more mailings.

To synchronize a web browser cookie to a particular email address. This trick allows a web site to know the identity of people who come to the site at a later date.

Email Web Bugs are represented as 1-by-1 pixel IMG tags. However, because the sender of the message already knows your Email address, they also include the Email address in the Web Bug URL. The Email address can be in plain text or referencing an internal database.

What information is sent to a server when a Web Bug is viewed?

At least the following information is transmitted:

- The IP address of the computer that fetched the Web Bug
- The URL of the page or identity of document that the Web Bug is located on
- The time the Web Bug was viewed
- The type of browser that fetched the Web Bug image
- A previously set cookie value

Do our privacy test to see what information can be inferred from this: http://www.maxa-tools.com/cookie-privacy.php

Especially when previously set cookie values are sent when accessing the web bug, the page or document impression can be linked to the user!

Where can I get more information about MAXA Cookie Manager?

See the product web page at http://www.maxa-tools.com/cookie.php.

The user manual explaining the use of the software can be found here: http://www.maxa-tools.com/MCM-User-Manual-EN.pdf

Whitepaper Information Notice:

Errors & Omissions Excepted

This paper reflects the technical status as of October 2009.