The Cookie Monster is Coming for You

Types of digital cookies and how to protect yourself from poisoned cookies

White Paper

CRA™
Transform IT
Computer Resources of America

The Cookie monster is coming for you

Talk of the Cookie monster and the image that instantly pops in our head is that of the lovable Sesame Street Muppet who is eternally hungry and devours just about anything. But, the Cookie monster we are talking about is anything but lovable and can devour your personal data, online privacy, identity, finances and more! Sounds scary, doesn't it? We tell you how you can beat the Cookie monster, in this whitepaper.

Let's start with Cookie alerts

When you visit a site, probably for the first time or from a new device or browser, you will see an alert that mentions the site "uses Cookies to offer you a more personalized experience" and asks you if you are okay with it. Let's admit it. A lot of us don't even bother to read what the notification says before we click "Accept" and move on with our browsing.

So, what are these cookies anyway?

Cookies are tiny information packets that store data related to your interaction and behavior on websites. It is like walking into your favorite local diner and having them serve up the "usual" instantly. Cookies Track your digital footprint on a website and allow the site to offer you a more personalized browsing experience. For example, let's say you visited Amazon.com and looked at some cameras; perhaps, you put one into your cart as well, but never checked out, or added one to your wishlist on the site. The next time the camera is on a sale, the Amazon app sends you a notification about the price reduction. That happens with the help of cookies. And, that's just one example. Cookies are not necessarily limited to shopping sites.You know how sometimes you can save your password for some sites, so you don't have to type it or log in every time you visit the website? You are able to do that because of cookies. Any site can have cookies, though shopping and banking sites can't function without them.

Types of Cookies-Not your average chocolate chip and mint

There are 3 kinds of cookies, each having different functions. One of them is session cookies. If it weren't for session cookies, you wouldn't be able to do any online shopping, banking, social media posting or any other activity that requires you to be logged in/identified. These session cookies are temporary cookies and they disappear once you log out of the website, thereby ending your session. It is the session cookies that enable the website to identify you and your actions and react accordingly. Without them, every click you make on the site will be treated as a new one, unrelated to the previous action. For example, you logged into your bank account to transfer money to a friend. If you click on "Money Transfer", without a session cookie, the bank's website won't recognize you from your log-in and you just won't be able to proceed further. You will be stuck in an endless loop of log-ins.

The second kind of cookies are called persistent cookies.These cookies are stored in the hard drive of your computer. Unlike the session cookies, they are not temporary and don't disappear until you clear them proactively. Persistent cookies are used by websites to offer you a customized browsing experience. For example, when you visit the website of a company that has a global presence, you may be given the option to choose your preferred language and country, so the site displays relevant information. Unless you clear the cookies from your computer manually, the next time you visit the site, you will automatically be taken to the version of it that you chose last time--probably English, US.

The third kind of cookies are called third-party cookies and are typically used to retarget customers as a part of online advertising campaigns. You might have noticed that sometimes after you visit online shopping sites, ads related to the items you viewed on the shopping site shows up as you browse other websites too. That is a situation where third party cookes have been deployed.

The poisoned cookie-How cookies become a security threat?

So, now we know that cookies inherently are not dangerous. Some cookies like the session cookies are absolutely indispensable, while some like persistent cookies make your web browsing experience more pleasant and the third party cookies, while not very pleasant, are used basically to facilitate online advertising. How do cookies become a security threat, then? Cookies become a security threat when hackers get access to them. If hackers hijack your cookies, they can get access to your session, your passwords and other related online activities. Hackers sometimes create “Super Cookies” and “Zombie cookies” to steal information from authentic cookies. Such cookies are difficult to identify and delete and sometimes work like worms replicating themselves, thus making it more difficult to get rid of them. Hackers can also steal your cookies if they get access to your network or to the server of the website you are visiting. For example, if your bank’s or shopping website’s server was hacked into, chances are, the hacker has access to your cookies and thereby all your account details.

Managing cookies effectively

Now we know that while cookies by themselves are harmless, cybercriminals can use them as a medium to attack you virtually. But, as we discussed before, you just cannot make do without cookies. So, how do you manage cookies effectively to stay safe? Here are a few tips.

1. **Avoid third-party cookies:** Third-party cookies are primarily used for online advertising and retargeting, so you won’t miss anything significant by avoiding these cookies. So, whenever you see a cookie alert on any site, first, check if it is for third-party cookies and if yes, it’s best to ‘Not accept cookies’ **As a business, don’t allow third-party cookies on your site.**

2. **Secure sites:** Make sure the sites you visit are secure (HTTPS) and have a valid SSL(Secure Socket Layer) certificate. The SSL certificate ensures that any data that’s exchanged is encrypted, meaning even if the hackers get access to the cookies, the information will be garbled eliminating any data leakage. **As a business, make sure your site is secure and has a valid SSL certificate.**

3. **Anti-malware software and security patches:** Install antimalware software programs on your computers and make sure they are up-to-date. Install security plug-ins and patches as soon as they are available, without delay. Do not use outdated software or operating systems for which support and security upgrades have been discontinued. Cybercrime modus operandi evolves at a rapidly:, an outdated cybersecurity setup will do you no good.

4. **Invest in a good password manager tool:** One of the reasons people tend to store passwords and other sensitive information online--which involves use of cookies, is because they have a tough time remembering passwords. A good password management system provides you with a safe and secure alternative.

5. **Educate your staff:** Train your staff to identify and steer clear of basic cybersecurity risks such as

   a. Phishing links
   b. Clone websites
   c. Using public Wi-Fi
   d. Poor password hygienee.
   e. Unverified app downloads, etc. ,

6. **IT Policy:** Establish a solid IT policy that spells out the dos and don’ts for your staff to follow in the office and also when accessing work data remotely.

   If all of this feels overwhelming on top of running a business, it makes good sense to bring an MSP onboard who can take care of not just the Cookie monster but also of your entire IT security setup.

For more information please contact,

Computer Resources of America Phone:
2123764040 | Email: hello@consultcra.com