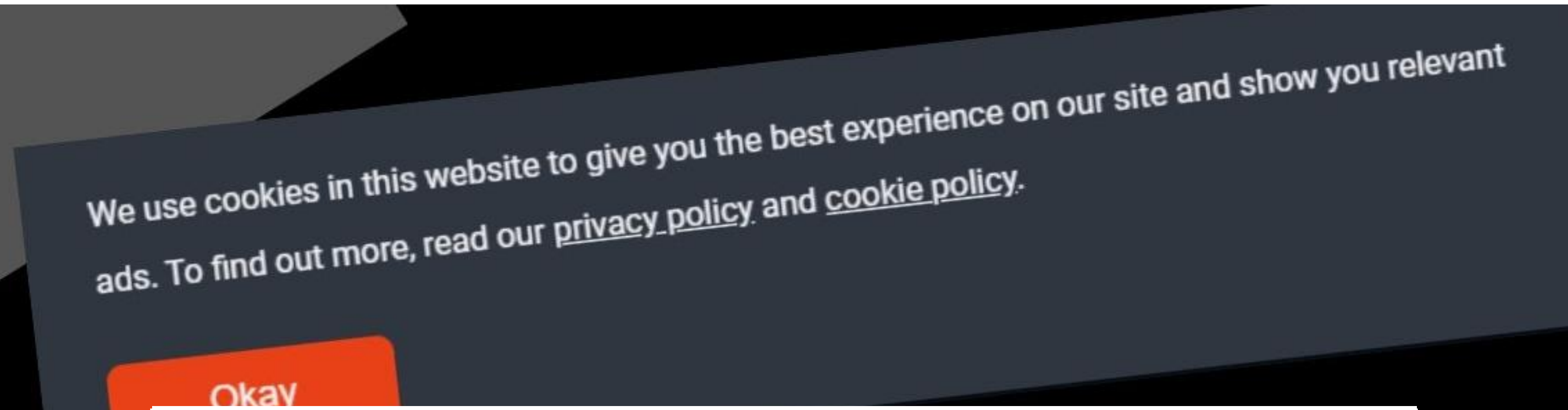


We use cookies in this website to give you the best experience on our site and show you relevant ads. To find out more, read our privacy policy and cookie policy.

Cookies ;)

Have these (internet cookies) – with care.

Awareness, Careful consent, Good practices – will enable productive and safe Internet experience.

Cyber security awareness Series | 23F09
Exclusively for members of ARIA by Sanjay Kadel, Infosec Partner

The cookies are *sweeter things* in life, but like a dentist/doctor would warn to be careful about it, so are the 'internet cookies' or 'browser cookies' or 'website cookies'. (Just different names!) – just be aware and careful about it.

Let's understand the concept of these internet cookies, their intended purpose (as a technology); what cyber security issues / threats emerge from this tech-concept ***(like tracking cookies, cookie hijacking, cookie poisoning, Session fixation, Cross-site request forgery, Zombie cookie, etc.)***; and what best practices can be adopted to have a productive and safe internet experience.

I. A small Introduction on Cookies

Most modern-day websites (or internet servers) use cookies. In-fact in our regular browsing over internet, use of cookies happens in background (without our knowledge) and nowadays some websites could give pop-up or alert about the use of cookies and may sometimes, give ***option*** to accept cookies completely or partially.

Whenever, you visit these websites, they place ***tiny text files*** on your computer through the browsers you use (like Google chrome or Internet explorer or Safari). Such ***tiny text files***, contain certain important / private / system / website data to serve useful and sometimes essential functions of that website.

Cookies can be of certain types – categorized on the basis of longevity of its usage:

(a). Session cookies (Temporary cookies) – These cookies help the websites / servers to know that all your website activity (within a period of time) came from the ***same source*** and should be treated as a ***single session***. These cookies extinguish once you close your browser, as they are usually kept in active memory.

(b). Persistent cookies (Permanent cookies) – These cookies help websites / servers to identify you for a longer period and help in authentication and tracking. These cookies will not be deleted automatically.

Based on which website / server / party installs the cookies in your computer, cookies can be of the following types:

(a). First-party cookies – These cookies are created by the website you are visiting.

(b). Third-party cookies – These cookies are created by a website you are not even visiting, also known as marketing or advertising cookies, and are used for tracking a user and gathering information over different websites.

As third-party cookies gather more and more information, they are used to provide a so-called "personalized experience." This means you will be receiving targeted and custom ads based on information (accessed through these cookies) such as previous user queries, user behavior, geographic location, interests and more.

Now, based on the declared-intended purpose / the use-case of cookies are generally, the following:

- Session management
- User authentication
- Authorized use / access of sensitive / protected website resources
- Auto fill personal / routine information on web forms
- Saving user preferences like language, country, categories, etc.
- Personalized user experience over internet
- Speed up transactions – for example, on banking or e-commerce websites
- Compile & Tracking user behavior / browsing activity / habits
- Enabling targeted advertising / marketing / remarketing
- Assess website performance and analytics / track web traffic
- Ascertain audience use patterns and feedbacks
- Improve security
- Provide content, services, recommendations

Therefore, usually the cookies are used for functional / statistical / marketing purposes by the website / servers.

II. So, what's the issue with Cookies?

Cookies are, in general, good for the productive use of internet and having a great personalized experience online. Well, as with any good tech and tool, misuse is the other side of coin.

So, let's understand what potential ***cyber security issues / threats*** emerge from this every-day tech-concept (cookies), while browsing internet and accessing websites / servers.

1. Issue: Loss of Confidentiality / Loss of Privacy / Unauthorized access to website

Remember – Authentication cookies. Depending on the issuing website and the user's web browser, such cookie data may be encrypted or plain text.
Security vulnerabilities may allow an attacker (security hacker) to read the cookie's data (user's information), and also gain access (with the user's credentials) to the website to which the cookie belongs.

2. Issue: Collection of excess information by websites / servers & User profiling for targeted marketing / Ad campaigns / Any other targeted communication or agenda

Tracking cookies, especially Third-party cookies gather and store considerable amount of data — a ***potential privacy concern***. In-fact this prompted regulatory and government agencies to mandate these websites to obtain - "***informed consent***" from users before storing non-essential cookies on their device.

It was observed that top websites, had installed an average of 64 pieces of tracking technology (including cookies) onto computers, resulting in a total of 3,180 tracking files. This data can then be collected and sold further to bidders (many a times these land in wrong hands).

3. Issue: Cookie theft – eavesdropping / cross-site scripting

Also known as ***eavesdropping attack***, sniffing attack, or snooping attack, it is a method that retrieves user information through the unencrypted internet transmission or open Wi-Fi.
If the cookies don't have 'Secure flag' then the cookies are exposed to '***Cookie theft***' via eavesdropping, as they can be transmitted even over an un-encrypted connection (http) or unsecured Wi-Fi.

An attacker could use intercepted cookies to impersonate a user and perform a malicious task, such as transferring money out of the victim's bank account.

Cookies can also be stolen using a technique called ***cross-site scripting***. This occurs when an attacker takes advantage of a website that allows its users to post unfiltered HTML and JavaScript content.

4. Issue: Cookie poisoning

It happens when unauthorized persons (attackers) can manipulate cookies due to the poor security infrastructure of a website. By editing or manipulating the cookie, the attacker can gain access to the user data stored in the cookie.

5. Issue: Cross-site request forgery / CSRF / XSRF

Also known as one-click attack or session riding and abbreviated as CSRF or XSRF is a type of malicious exploit of a website or web application where unauthorized commands are submitted from a user that the web application trusts.

An innocent end user is tricked by an attacker into submitting a web request that they did not intend. This may cause actions to be performed on the website that can include inadvertent client-side or server-side ***data leakage***, change of session state, or ***manipulation*** of an end user's account.

There are many ways in which a malicious website can ***transmit such commands***; ***specially-crafted image tags***, ***hidden forms***, and ***JavaScript fetch*** or ***XML HTTP Requests.*** These can act without the user's interaction or even worse - without the user's knowledge!

Attacks were launched by placing malicious, automatic-action HTML image elements on ***forums*** and ***email spam***, so that browsers visiting these pages would open them automatically, without much user action.

6. Issue: Zombie cookies

It is a cookie with data and code that has been placed on the device, in a ***hidden location***, and that automatically recreates a HTTP cookie as a regular cookie after the original cookie had been deleted.
When absence of such zombie cookie is detected in certain location, the missing instance is recreated by the JavaScript code using the data stored in other locations.

7. Issue: Session Hijacking

When a legitimate user is logged in to a website, attackers use their knowledge of the current session cookie to ***take over the user's session***.

8. Issue: Session spoofing

Attackers use stolen or forged session tokens to start a new session and impersonate the legitimate user. This type of attack requires no user interaction and can be initiated even when the user is not logged in to the website.

9. Issue: Session fixation

Attackers send a known session identifier via a phishing email or other means and fool a legitimate user into using this identifier to log in to a vulnerable or malicious site. The attacker then hijacks the user session.

These and many other vulnerabilities exist and emerge from careless use of cookies and cookie-handling mechanisms.
Ranging from severe risk to privacy, to several types of frauds and cyberattacks can be based on exploiting cookies vulnerabilities, and that may lead to severe security incidents.

III. Let's discuss Safeguard Options!

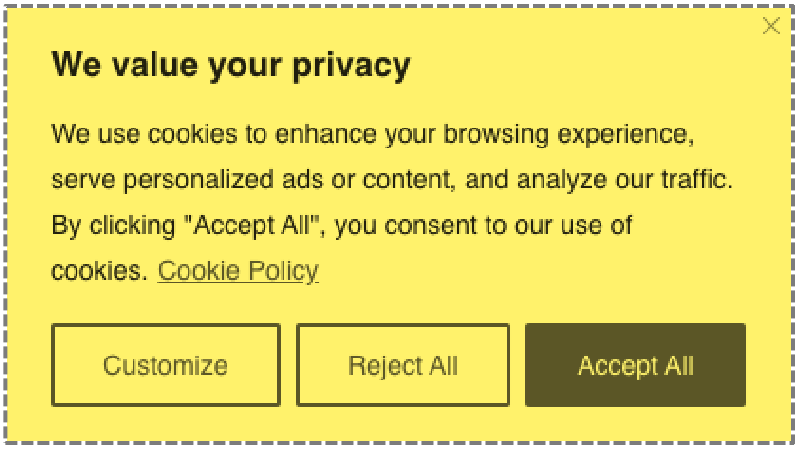
While doing away with the use of cookies is currently not possible due its wide-use and functionality it provides to the users and more-so to the companies / websites / servers – cookies can surely be used in a secure and responsible manner.

> Do we have a choice to safeguard ourselves from the risks / issues / threats arising from use of cookies? The answer is yes, we do have *to certain extent* certain safeguard options.

1. Cookies Consent Banner

Safeguards in hands of User, Service provider, Regulators

Many "ethical" and "compliant" ;) websites / servers have banners (top / bottom of screen) or pop-ups or alerts displayed on their website, which provides the users who land on such websites with certain safeguard controls.



We value your privacy

We use cookies to enhance your browsing experience, serve personalized ads or content, and analyze our traffic. By clicking "Accept All", you consent to our use of cookies. Cookie Policy

A typical example of a cookies consent banner.

Live sample websites
URL1, URL2

You should look into / check whether the websites provide the following safeguard controls and carefully make use of them.

- Information (Transparency) on the cookies which website uses; cookies policy; privacy policy and regulatory requirement / compliance like GDPR
- Choice to ***accept all*** cookies
- Choice to ***deny all*** cookies
- Choice to ***accept essential*** cookies only

2. Training / Awareness

Safeguards in hands of User, Service provider, Regulators

A reasonable amount of awareness on the 'cookies' concept and emerging risks / issues / threats arising from improper / careless use of cookies is critical among the users, service providers, regulators, and other stakeholders. This will ensure that the cookies are used in a secure and responsible manner.

More-over good amount of training offered to developers / seeking help of competent tech-professionals will help in ensuring that the websites / servers – use / configure cookies in a secure and responsible manner.

3. Hygienic internet usage

Safeguards in hands of User

Users should avoid visiting suspicious / un-necessary websites either voluntarily or based on social engineering inducement.

Whenever visiting websites, ensure https on the URL-address, which ensures that the transmission between the particular website and the user – will be encrypted.

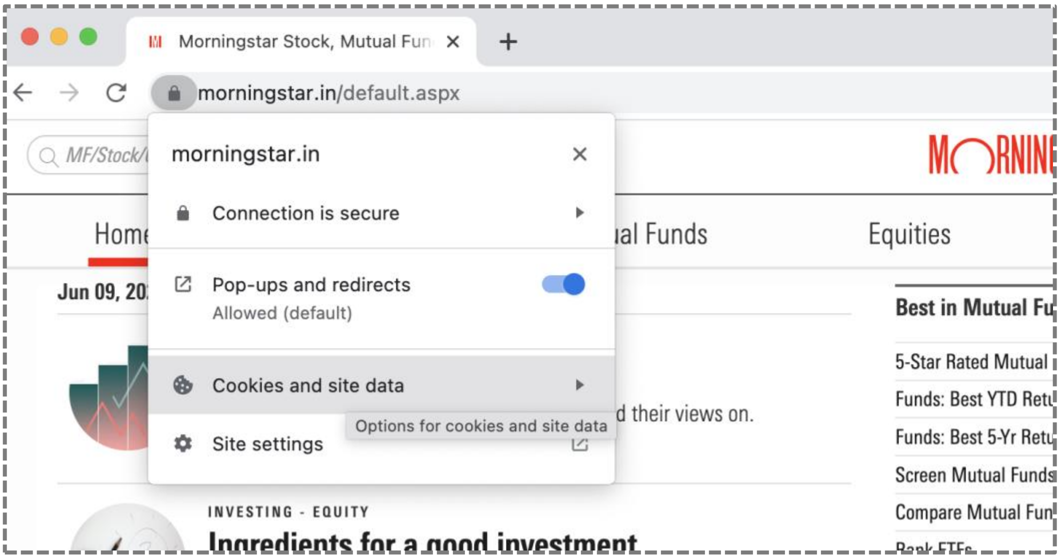
Users should visit the necessary website always through ***specified URL-address*** of the website found in official email of that company or official business correspondence of that company – so that you don't land up on suspicious / malicious / un-necessary websites.

Remember – Google is only a search engine and will throw up all possible matching results – it does not necessarily provide authentic / genuine website address of the company you are searching for.

4. Review Website's cookies settings

Safeguards in hands of User

You can click the small lock symbol on the URL address bar (like the one shown in following image) and '***view site information***' about a particular website to review the website's cookies settings and other security information.



Morningstar Stock, Mutual Fun

morningstar.in/default.aspx

morningstar.in

Connection is secure

Pop-ups and redirects
Allowed (default)

Cookies and site data

Options for cookies and site data

Site settings

5. Review Browser's cookies settings

Safeguards in hands of User

You should review and configure your browser settings for the cookies, according to your privacy and cyber security risk tolerance.

For instance, in the google chrome browser, the cookies settings can be accessed by going to the following URL:

```
chrome://settings/cookies
```

You should look into / check the browser's cookies settings which provide the following safeguard controls and carefully make use of them.

- Choice to 'Allow all cookies'
- Choice to 'Block third-party cookies'
- Choice to 'Block all cookies' (not recommended)

Further you also have following choice of general actions / configurations:

- Choice to enable 'Clear cookies and site data when you close all windows'
- Choice to enable 'Send a 'Do not track' request with your browsing traffic.

You can also specifically white-list or black-list certain websites related to cookies usage, as follows:

- Choice to white-list websites that are allowed to 'always use cookies'
- Choice to list websites wherein 'Always clear cookies when windows are closed'
- Choice to black-list website that are 'Never allowed to use cookies'

You could periodically or in case, necessary – delete the cookies in your browser history. For instance, in the google chrome browser, you head to following URL:

```
chrome://settings/clearBrowserData
```

6. Install security applications and patches

Safeguards in hands of User

You could install an ad-blocker or anti-tracking browser extension. Some of the anti-virus / firewall applications could also help to hide your internet activity from tracking cookies.

Installing a VPN (Virtual private network) – with features like changing your IP address in every session, makes your profile much harder to reconcile and track.

The browsers do release patches / updated versions which fixes bugs and known / exposed vulnerabilities. So, do keep your browser version updated.

7. Development safeguards

Safeguards in hands of Service provider

Like any other technology, cookies also form a critical element of websites / servers to provide functionality / services / content / performance / security and analytics.

The Service providers / Companies should ensure that the ***website developers*** provide robust configuration and handling of cookies along with appropriate / compliant disclosures and options to the users for using cookies at user's consent and user's cyber security and privacy safeguard perception / requirement.

8. Policy compliance

Safeguards in hands of Service provider

To ensure the secure and ethical practices related to data collection, storage, and usage through the use of cookies, there needs to be a top-down policy and commitment from governance, management, and security forums internally, lest excess-use and misuse of private data will be rampant and affect one and all negatively.

The Service providers should conduct compliance audits of their cookies policy, settings, and usage, including operating effectiveness in terms of data protection and privacy safeguards.

9. Technology alternatives

Safeguards in hands of Technology

Some of the operations that can be done using cookies can also be done using other / alternative mechanisms. For instance,

▪	To achieve authentication and session management	Instead of cookies – technology concepts like JSON Web Tokens, HTTP authentication, URL (query string), Hidden form fields, and others can be used alternatively.
▪	To achieve tracking data (for website functionality)	Instead of tracking cookies – technology concepts like IP address, E-Tag, Browser cache, Browser fingerprint and others can be used alternatively.

10. Regulatory compliance

Safeguards in hands of Regulators

As cyber security and data privacy landscape evolves, and more countries address the emerging issues, ***cookies*** are almost always included in the narrative.

For instance, the popular legislation - ***General Data Protection Regulation (GDPR)*** – on data protection and privacy, meant for the European Union (EU) regions - treat ***cookies as "personal data"*** making them subject to regulation. It mandates the Website / Servers to ***collect consent from users*** before serving any non-essential cookies to the user's device.

It has had a huge positive impact on the disclosure, transparency, and safe handling of user data by the websites / services using cookies to collect the user data. In-fact, use of third-party cookies fell 22% on average immediately after the GDPR's implementation.

India is currently working on similar data privacy laws. However, till then GDPR is anyway being followed as an industry standard by Information security professionals, along with other standards like ISO 27001 and related series, SOC2 Trust service principles, HIPAA, HiTrust, NIST guidelines, PCI DSS, and many others.

Wishing you <secured> digital star! In work and life.

Caveat – The design of controls and extent of cyber security best practices, to be adopted for the organization / user, should be based on business requirements (nature and size), risk assessment and feasibility (technical, financial, and operational), and compliance requirements! Arising from policies, contractual obligations, legal & regulatory mandates.

Disclaimer – Information contained in the cyber security awareness campaign, and related notes / documents / guidelines / interpretations / publication provided in connection to such awareness campaign, for RIA's compliance to cyber security awareness campaign, are intended for use, primarily by the relevant members of ARIA only, to the extent suitable to their situation / case. If you are not the intended audience of these publication or artefacts, an agent of the intended audience or a person responsible for delivering the information to the named entities, you are notified that any use, distribution, transmission, printing, copying or dissemination of this information in any way or in any manner is strictly prohibited.

Every effort has been made to avoid errors or omissions in these publications and artefacts. In spite of this, errors may creep in. Any mistake, error or discrepancy noted may be brought to our notice at membership@aria.org.in (more contact details at https://aria.org.in) which shall be taken care of in the next update and release.

Though, we may provide, to the best extent possible, a reasonably proper publication or artefact, there may be, alternative approaches / interpretations / improvisation possible.

It is notified that neither ARIA nor the authors, including, members of Sanjay Kadel & Co. Chartered Accountants, or anyone connected herewith will be responsible for any damage or loss of action to anyone, of any kind, in any manner, therefrom. It is suggested that to avoid any doubt the reader, receiver, or user of the information contained in these publications or artefacts, should cross-check all the facts, law, and contents of the publication with original source, publication, or notifications.