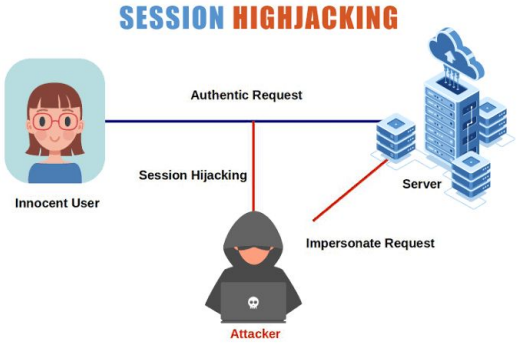
GUARDSIGHT

https://www.guardsight.com

Cybersecurity Tips For Session Security

YOUR AWARENESS IS THE BEST DEFENSE

A session can be considered as all the sites you visit during one sit down at your computer. During a session, websites store cookies on your computer as a benign way in identifying you in future sessions. Attackers can steal your cookies and use them to log in to your personally or professionally sensitive areas such as social media accounts, bank account, and work environments. This known as Session Hijacking.



SESSION SECURITY

1 **Verify That Sites Use SSL or HTTPS**
This provides end to end encryption so there is no unauthorized access to your cookies and other information at least while they are being transmitted.

2 **Use a VPN**
A VPN further encrypts traffic and is an added level of security while your information is being transmitted. Don't use free VPNs.

3 **Delete Cookies**
Deleting your cookies every so often forces sites to reestablish your identity.

4 **Update Your Antivirus**
Antivirus software programs are becoming better at detecting session hijacking. Make sure yours is up to date.

5 **Avoid Clicking Suspicious Links**
When in doubt, use free services like VirusTotal.com to see if a link is malicious or not.

For additional advice or to learn more contact us: info@guardsight.com