INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed JournalMulti Disciplinary
Peer Reviewed Edition :

www.ijlra.com

 ISSN: 2582-6433

DISCLAIMER

ISSN: 2582-6433

EDITORIAL TEAM

EDITORS

Megha Middha

Megha Middha, Assistant Professor of Law in Mody University of Science and Technology, Lakshmangarh, Sikar

Megha Middha, is working as an Assistant Professor of Law in Mody University of Science and Technology, Lakshmangarh, Sikar (Rajasthan). She has an experience in the teaching of almost 3 years. She has completed her graduation in BBA LL.B (H) from Amity University, Rajasthan (Gold Medalist) and did her post-graduation (LL.M in Business Laws) from NLSIU, Bengaluru. Currently, she is enrolled in a Ph.D. course in the Department of Law at Mohanlal Sukhadia University, Udaipur (Rajasthan). She wishes to excel in academics and research and contribute as much as she can to society. Through her interactions with the students, she tries to inculcate a sense of deep thinking power in her students and enlighten and guide them to the fact how they can bring a change to the society

Dr. Samrat Datta

Dr. Samrat Datta Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Samrat Datta is currently associated with Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Datta has completed his graduation i.e., B.A.LL.B. from Law College Dehradun, Hemvati Nandan Bahuguna Garhwal University, Srinagar, Uttarakhand. He is an alumnus of KIIT University, Bhubaneswar where he pursued his post-graduation (LL.M.) in Criminal Law and subsequently completed his Ph.D. in Police Law and Information Technology from the Pacific Academy of Higher Education and Research University, Udaipur in 2020. His area of interest and research is Criminal and Police Law. Dr. Datta has a teaching experience of 7 years in various law schools across North India and has held administrative positions like Academic Coordinator, Centre Superintendent for Examinations, Deputy Controller of Examinations, Member of the Proctorial Board

ISSN: 2582-6433

Dr. Namita Jain

Head & Associate Professor

School of Law, JECRC University, Jaipur Ph.D. (Commercial Law) LL.M., UGC -NET Post Graduation Diploma in Taxation law and Practice, Bachelor of Commerce.

Teaching Experience: 12 years, AWARDS AND RECOGNITION of Dr. Namita Jain are - ICF Global Excellence Award 2020 in the category of educationalist by I Can Foundation, India.India Women Empowerment Award in the category of "Emerging Excellence in Academics by Prime Time & Utkrisht Bharat Foundation, New Delhi.(2020). Conferred in FL Book of Top 21 Record Holders in the category of education by Fashion Lifestyle Magazine, New Delhi. (2020).Certificate of Appreciation for organizing and managing the Professional Development Training Program on IPR in Collaboration with Trade Innovations Services, Jaipur on March 14th, 2019

Mrs.S.Kalpana

Assistant professor of Law

Mrs.S.Kalpana, presently Assistant professor of Law, VelTech Rangarajan Dr. Sagunthala R & D Institute of Science and Technology, Avadi.Formerly Assistant professor of Law,Vels University in the year 2019 to 2020, Worked as Guest Faculty, Chennai Dr.Ambedkar Law College, Pudupakkam. Published one book. Published 8Articles in various reputed Law Journals. Conducted 1Moot court competition and participated in nearly 80 National and International seminars and webinars conducted on various subjects of Law. Did ML in Criminal Law and Criminal Justice Administration.10 paper presentations in various National and International seminars. Attended more than 10 FDP programs. Ph.D. in Law pursuing.

Avinash Kumar

Avinash Kumar has completed his Ph.D. in International Investment Law from the Dept. of Law & Governance, Central University of South Bihar. His research work is on "International Investment Agreement and State's right to regulate Foreign Investment." He qualified UGC-NET and has been selected for the prestigious ICSSR Doctoral Fellowship.He is an alumnus of the Facultyof Law, University of Delhi. Formerly he has been elected as Students Union President of Law Centre-1, University of Delhi.Moreover, he completed his LL.M. from the University of Delhi (2014-16), dissertation on "Cross-border Merger & Acquisition"; LL.B. from the University of Delhi (2011-14), and B.A. (Hons.) from Maharaja Agrasen College, University of Delhi. He has also obtained P.G. Diploma in IPR from the Indian Society of International Law, New Delhi.He has qualified UGC – NET examination and has been awarded ICSSR – Doctoral Fellowship. He has published six-plus articles and presented 9 plus papers in national and international seminars/conferences. He participated in several workshops on research methodology and teaching and learning.

ISSN: 2582-6433

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANLAYSIS ISSN

2582-6433 is an Online Journal is Monthly, Peer Review, Academic Journal, Published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essay in the field of Law & Multidisciplinary issue. Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

www.ijlra.com
Volume 2 Issue 7 | Jan 2024

ISSN: 2582-6433

EXPLORING THE RISKS AND DANGERS OF PUBLIC WI-FI NETWORKS

AUTHORED BY - PRIYANSHU ABHINAV

ABSTRACT

Public Wi-Fi networks are now widely used and offer simple internet access in a variety of public situations. The simplicity of use is accompanied by serious security threats, though, such as malevolent assaults, invasions of privacy, and the interception of private information. Vulnerabilities in public Wi-Fi networks can be exploited by hackers, potentially putting users' sensitive and personal data at risk. Users must take proactive steps to protect their data and be aware of potential hazards in order to mitigate these risks.

There are a number of important suggestions that can reduce the risks related to using public Wi-Fi. These include establishing robust encryption standards, using Virtual Private Networks (VPNs) to secure internet data, and adopting self-protective practices. Furthermore, implementing WPA3 and other upgraded security protocols can greatly improve Wi-Fi network security, lowering the risks connected to using public Wi-Fi.

In order to mitigate these threats, policy measures and technological advancements targeted at enhancing the security of public Wi-Fi networks are also essential. The study is to increase awareness of the possible risks connected with utilizing public Wi-Fi networks by enabling users to make educated decisions and adopt actions to protect their sensitive and personal data. It is feasible to reduce security threats and provide a safer environment for people and companies using public Wi-Fi networks by combining user attentiveness, technology breakthroughs, and legislative improvements.

KEYWORDS:- Public Wi-Fi networks, security risks, cyber threats, privacy breaches, data interception, mitigation strategies.

ISSN: 2582-6433

INTRODUCTION

Public Wi-Fi networks have become much more common in recent years, providing extensive connectivity but also giving rise to worries about privacy and security hazards. The number of public Wi-Fi hotspots worldwide as of 2022 was 549 million, indicating people's growing dependence on technology and ongoing need for connectivity. [1]Public Wi-Fi networks are becoming more widely available and are a global phenomenon, found in both large cities and tiny communities. However, a number of variables, including governmental regulations, economic growth, technological infrastructure, and urbanization, affect the standard and accessibility of public Wi-Fi. Public Wi-Fi networks are expanding quickly, which has led to a number of security and privacy concerns. Users of public Wi-Fi networks who connect insecurely and without encryption are more susceptible to malware, man-in-the-middle attacks, data theft, and other online dangers. Therefore, while utilizing public Wi-Fi, users must adopt self-protective behaviors and security precautions, such as restricting access to sensitive information, utilizing a Virtual Private Network (VPN), and exercising caution. Network managers and users must continue to be watchful and proactive in safeguarding their networks due to the rising number of cyber-attacks and the evolving threat landscape for wireless networks. It's critical to put strong security measures in place to reduce the hazards connected with public Wi-Fi networks. Some examples of these precautions include employing strong passwords, updating firmware, and leveraging encryption technologies. Wi-Fi and other wireless networking technologies are widely available, which has made it easier to set up public Wi-Fi networks. Wi-Fi networks are now more suited for public usage thanks to the development of Wi-Fi protocols like IEEE 802.11n, 802.11ac, and 802.11ax (Wi-Fi 6), which have allowed for faster speeds, more dependability, and larger coverage regions. IoT devices are becoming more common in homes, offices, and public areas, which increases the demand for seamless connectivity and interoperability. Applications including environmental sensing, public safety monitoring, and smart home automation are made possible by public Wi-Fi networks, which act as the foundation for connecting and controlling IoT devices.

[1] Antonio Coreas Uson , Transformation in wireless connectivity, 2022 [accessed 26 January, 2024]/ https://nap.nationalacademies.org/catalog/27064/transformation-in-wireless-connectivity-guide-to-prepare-airports

ISSN: 2582-6433

SECURITY THREATS IN PUBLIC WI-FI NETWORKS

1. **Man-in-the-middle(MitM)attacks**

   One frequent risk connected to public Wi-Fi networks is the man-in-the-middle (MITM) attack. A third party intercepts two systems' communications in a Man-in-the-Middle (MITM) attack, giving the attacker access to all messages sent between the unwary victims. Attackers have the ability to create their own Wi-Fi hotspot and allow gullible users to connect to it rather than the official network. With a laptop carrying two Wi-Fi adapters, they can link one of them to the authorized public hotspot and configure the other adapter to act as a second Wi-Fi hotspot with the same SSID as the authorized one. Additionally, they would design a phony login screen that perfectly mimics the real one. Attackers can install malware, move data files, steal credentials, and even spy on the user if they have access to the device. Users can utilize a Virtual Private Network (VPN), restrict access to critical information, and refrain from visiting unsafe websites in order to prevent Man-in-the-Middle (MITM) attacks. By hiding the IP address and encrypting data, a VPN makes it more difficult for hackers to intercept communications. Before joining to a Wi-Fi network, users should also verify its security settings. They should also stay away from unprotected networks.

2. **Rogue hotspots and evil twin attacks**

   Unauthorized access points such as evil twin attacks and rogue hotspots can present significant security threats. They are frequently used to obtain illegal access to a victim's network or device, which enables hackers to take advantage of login passwords, private data, financial information, and other sensitive information. Unauthorized wireless access points that are installed to a network without the owner's knowledge or consent are known as rogue hotspots. Hackers may install them in order to intercept data or obtain unauthorized access to a victim's network or device. A sort of rogue hotspot known as a "evil twin attack" occurs when a hacker constructs a phony Wi-Fi network that mimics an authentic one. Users may find it challenging to differentiate between the two when the attacker installs a new hotspot (evil twin) with the same name (SSID) as the legitimate

ISSN: 2582-6433

access point. [2]Once a user establishes a connection with the evil twin, the attacker is able to track their online activities, obtain sensitive personal data, and take advantage of it. Take into consideration the following safety measures to shield yourself against evil twin attacks and rogue hotspots:

i. Use your own hotspot: You can be better protected from evil twin attacks by using your own personal hotspot rather than public Wi-Fi networks.
ii. Verify the security configurations: A public network should only be connected to when the security settings have been updated and activated.
iii. Avoid using unprotected networks: Stay away from networks that are labeled as "unsecured," as evil twin attacks are more likely to occur on them.
iv. Exercise caution: Recognize the dangers of using public Wi-Fi networks and take the appropriate safety measures to safeguard your personal data.

3. Packet sniffing and data interception

One technique for capturing and examining packet data conveyed over a network is called packet sniffing. Network administrators can use it for monitoring and troubleshooting, but hackers can use it to snoop on or steal private information. Tools for packet sniffing can gather a variety of network communications, including IP addresses, passwords, and login information. Software packet sniffing, which utilizes a program to record and examine network data, and hardware packet sniffing, which employs a physical device that plugs straight into a network interface, is the two primary forms of packet sniffing. Packet sniffing exploits provide hackers the ability to read emails, examine passwords, and record online activity. Hackers collect network packets in order to intercept or steal potentially unprotected data during a packet sniffing attack. Data thefts known as sniffing attacks are carried out by using packet sniffers, which are designed to intercept and read unencrypted network traffic.

The unapproved or covert interception of data while it is being transferred over a network or communication channel is referred to as data interception. It entails intercepting and

[2] M. Vanhoef, Célestin Matte, M. Cunche, L. Cardoso, Frank Piessens , Why MAC Address Randomization is not Enough: An Analysis of Wi-Fi Network Discovery Mechanisms, 2016

ISSN: 2582-6433

occasionally manipulating data transmitted between two parties without those parties' knowledge or agreement. Wireless communications, phone systems, and computer networks are just a few of the settings where data interception can happen. Data interception includes eavesdropping, packet sniffing, man-in-the-middle (MitM) attacks, email and message interception, and radio signal interception. Data interception can result in identity theft, business espionage, and nation-state espionage, among other types of criminality. Organizations can deploy encryption technology, identify and categorize sensitive data, train employees to spot phishing scams, and establish password procedures to avoid data interception.

4. **Malware Distribution and Drive-By Downloads**

The techniques employed by hackers to distribute malware to target computers are referred to as malware distribution. Malware can spread via a number of channels, including as links in phishing emails or malicious websites, advertising, corrupted storage devices, and email attachments. Malware may also be concealed in other files, such software or pictures. Social engineering, which is duping people into downloading, installing, and using malware on their computers or other devices, is a major factor in the spread of malware. Users should be trained to spot warning indications of questionable messages and to steer clear of attachments and links from senders they don't recognize in order to stop the spread of malware. Additionally, businesses can employ antivirus software, update their software, and periodically perform data backups.

When malicious malware is accidentally downloaded into a computer or mobile device, it's known as a "drive-by download" and exposes users to a variety of risks. Drive-by downloads are a common tool used by cybercriminals to infect endpoints with malware, introduce exploit kits, or steal and gather personal information. Drive-by downloads can happen even when a user doesn't click anything or go to a particular website. They frequently exploit security holes in outdated or non-updated software, operating systems, or web browsers. Drive-by download attacks frequently involve the distribution of files that are malware, spyware, or computer infections. Drive-by downloads may occur as a result of opening an email attachment, clicking a link, going to a website, or clicking on a

ISSN: 2582-6433

false pop-up window. Users should routinely update or patch their systems with the most recent versions of programs, software, browsers, and operating systems to guard against drive-by download. Avoiding unreliable or perhaps dangerous websites is also advised. Endpoints can be protected with the aid of a dependable and proactive security solution that actively analyzes websites.

5. Session Hijacking and Side jacking

A cyber-attack known as "session hijacking" occurs when an attacker gains unauthorized access to a web server by either stealing or correctly guessing a valid session token, thus taking control of a user's internet session. [3]Session sniffing, predictable session token ID, man-in-the-browser, cross-site scripting, session side jacking, and session fixation are some of the techniques that might lead to session hijacking. After obtaining the session ID, the attacker can assume the identity of the authorized user and use it to carry out any network operation that person is permitted to carry out. By putting security measures in place at both the application and network levels, such as encrypting session data, employing secure session management techniques, and keeping an eye out for unusual activities on the network, session hijacking attempts can be avoided.

Side jacking is a sort of cyber-attack in which an attacker intercepts and takes a user's session cookie in order to obtain unauthorized access to online accounts or services. It is also referred to as session hijacking or cookie hijacking. Sidejacking is a type of interception where the primary goal is to capture session identifiers, which are often saved in browser cookies, as opposed to traditional methods that target data carried over a network.

This is how side jacking usually operates:

i. Session Cookies: The server gives the user's browser a special session identifier (session cookie) when the user connects into a website or online service. The user

[3] Elira Hoxha, Igli Tafa, Kristi Ndoni, Session hijacking vulnerabilities and prevention algorithms, 2022.

ISSN: 2582-6433

can access their account without having to enter their credentials again by using this session cookie, which serves as a temporary authentication token.[4]

ii. Unencrypted connections: A lot of websites use unencrypted HTTP connections to send session cookies, which leaves them open to being intercepted by nefarious parties. Even if HTTPS encryption might be used to secure the login process, later requests might fall back to plain HTTP, leaving session cookies vulnerable to interception.

iii. Cookie Theft: An attacker can utilize side jacking to obtain a user's session cookie, which they can then exploit to assume the user's identity and access their account without authorization. This gives hackers the ability to carry out a variety of harmful tasks, including accessing private data, conducting illicit transactions, and taking control of user sessions.

Strategies for Mitigation against Sidejacking:

i. Use of HTTPS Everywhere: All web traffic not simply that which occurs during login should be encrypted using HTTPS, according to websites and online services. All connections between the user's browser and the server are encrypted via HTTPS, which helps prevent hackers from intercepting session cookies and other private information.

ii. Secure Cookies: To improve the security of session cookies, web developers can use secure cookie properties such the "Secure" and "HttpOnly" flags. The "HttpOnly" flag lowers the possibility of cross-site scripting (XSS) attacks by preventing client-side scripts from accessing cookies, while the "Secure" flag guarantees that cookies are only transferred over secure HTTPS connections.

iii. Using Virtual Private Networks (VPNs): By encrypting their internet traffic and hiding their IP addresses, VPN users may safeguard their online security and privacy. Through the creation of a secure tunnel between the user's device and the VPN server, attackers are prevented from intercepting session cookies or listening in on network conversations.

[4] Yu-Sheng Yang, Shih-Hsiung Lee, Lightweight Authentication Mechanism for Industrial IoT Environment Combining Elliptic Curve Cryptography and Trusted Token, 2023

ISSN: 2582-6433

iv. Logout from Public Devices: Users should constantly keep in mind to log out of their accounts and delete their browser's cache and cookies after using shared or public computers. This lessens the possibility of session hijacking and helps prevent unwanted access to their accounts.

v. Features for Enabling Browser Security: Users can activate features for their browsers that prevent tracking cookies and dangerous scripts, as well as content security policies and private browsing mode. These enhancements improve browser security and privacy protections, which helps reduce the danger of side jacking and other web-based assaults.

MITIGATION STRATEGIES AND BEST PRACTICES

1. **Use of Virtual Private Networks**

   Protecting sensitive data and mitigating a variety of cyber dangers can be achieved by using virtual private networks, or VPNs. Effective VPN usage techniques for security and privacy include the following:

   i. Selecting a reliable VPN service provider: To guarantee robust security protocols and encryption, pick a VPN provider that has undergone extensive testing and evaluation.

   ii. Suitable setup: Make sure your VPN is set up correctly to ward against any weaknesses and intrusions.

   iii. Recurring updates: To avoid potential attacks and patch vulnerabilities, make sure your VPN software is up to date.

   iv. Monitoring in real time: Work together with your network security team to implement real-time monitoring so that you can react quickly to anomalous traffic patterns that could point to an upcoming attack.

   v. Additional security features: Enable the extra security measures that come with your VPN service to avoid having your actual IP address revealed. Some of these capabilities include automated VPN connection disconnection in the case that it drops.

ISSN: 2582-6433

vi. Stringent traffic filtering: To lower the attack surface, limit the ports, protocols, and IP addresses of network traffic to VPN devices by implementing stringent traffic filtering rules.

vii. Intrusion Prevention System (IPS): To keep an eye out for possible dangers, think about installing an IPS in front of the VPN gateway if traffic cannot be limited to a specific IP address.

2. Encryption and Secure Protocols

Sensitive data can be safeguarded and numerous cyber risks can be reduced with the use of encryption and security standards. Here are some tips for successfully utilizing security protocols and encryption for privacy and security:

i. Selecting robust encryption methods: Choose encryption methods like AES that are well-known and have a track record of security.

ii. Putting safe protocols into practice: To encrypt data while it's in transit, use secure communication protocols like SSL/TLS.

iii. Sensitive data encryption: To prevent unwanted access, encrypt sensitive data while it's in transit and at rest.

iv. Regular updates: Update your encryption software and protocols on a regular basis to stay ahead of potential exploits and repair flaws.

v. Real-time monitoring: Work with your network security team to set up this feature, which will allow you to respond quickly to anomalous traffic patterns that could point to an approaching attack.

vi. Strict access control: Put in place stringent access control guidelines to restrict who has access to private information and mandate the use of strong passwords.

vii. Two-factor authentication: For accounts that have remote access, higher rights, or high-value assets, use multi-factor authentication.

viii. Secure VPNs: To guarantee robust security protocols and encryption, choose a reliable VPN provider that has undergone extensive testing and vetting.

ix. Physical security: To avoid unwanted access, make sure your networks and equipment are physically secure.

ISSN: 2582-6433

3. Avoidance of sensitive transactions

Using a variety of techniques to safeguard private information and stop illegal access is part of mitigating the risk associated with sensitive transactions. Among the tactics to steer clear of delicate deals are:

i. Safe ways to pay: Make use of electronic payment options, which offer more security than paper checks, such as virtual cards and Automated Clearing House (ACH) transactions. [5]

ii. Tight access management: Restrict access to confidential data and guarantee that only individuals with the proper authorization can view it.

iii. Employee education: Inform staff members on the value of data security and the dangers of handling sensitive information.

iv. Monitoring in real time: Use real-time monitoring to identify suspicious transactions and activities right away.

v. Encryption: Strong encryption techniques, such the Advanced Encryption Standard (AES), should be used to safeguard sensitive data.

vi. Secure protocols: To encrypt data while it's in transit, use secure communication protocols like SSL/TLS.

vii. Adherence: Verify adherence to sector-specific laws, like the Payment Card Industry Data Security Standard (PCI DSS).

viii. Multiple payment options: It can be dangerous to rely just on one method of payment. To lessen reliance on a single supplier and provide clients more choices, diversify your payment options.

ix. Monitoring and preventing chargebacks: Establish chargeback monitoring and prevention systems to quickly detect and resolve problems; provide exceptional customer service, transparent refund guidelines, and channels for resolving disputes.

x. Physical security: To avoid unwanted access, make sure your networks and equipment are physically secure.

[5] N. Arshadi, Blockchain Platform for Real-Time Payments: A Less Costly and More Secure Alternative to ACH, Technology & Innovation, 31 October 2019, https://www.semanticscholar.org/paper/Blockchain-Platform-for-Real-Time-Payments%3A-A-Less-Arshadi/3070defb48f66e5b22a6e3467954d7ed09799160 { accessed 26 January, 2024}

ISSN: 2582-6433

CONCLUSION

Numerous sites have emphasized the serious risks associated with using public Wi-Fi. According to a Forbes research, 40% of participants reported that their information was compromised when utilizing public Wi-Fi, highlighting the frequent security threats connected to these networks. The Norton Cyber security Insights Report highlights further potential risks, as over 600 million users globally become victims of cybercrimes, many of which stem from hackers taking advantage of open connections. The hazards are further increased by the fact that public Wi-Fi networks lack encryption, leaving them open to several types of attacks including man-in-the-middle attacks. It is advised to utilize Virtual Private Networks (VPNs) to encrypt internet traffic and secure personal information when using public Wi-Fi in order to mitigate these risks and to adopt self-protective habits. Additionally, strong, one-of-a-kind passwords and the deployment of WPA3 and improved encryption standards can greatly improve Wi-Fi network security, reducing the hazards related to using public Wi-Fi. In conclusion, the extensive use of public Wi-Fi and the alarming numbers of compromised data emphasize how important it is for people and organizations to use caution and preventive measures when utilizing these networks to safeguard their data. Users can drastically lower the risks by putting strong security measures in place and following best practices, like using VPNs and adopting strong encryption standards.