eCore Techno Solutions

eCore Techno Solutions Pvt Ltd

www.eCoreTechnoS.com

HackingTechnologies Powered by eCore

www.HackingTechnologies.com

SCO 62-63, 3rd floor, Opposite Hotel Taj, Sector 17-A, Chandigarh - 160017 India

+91 (172) 461 0064 | +91 (172) 400 9111

www.eCoreTechnoS.com | info@eCoreTechnoS.com

Wi-fi Threats

Attack Type	Explanation	Business Impact
Malware	Malicious code is the term used to describe any code in any part of a software system or script that is intended to cause undesired effects, security breaches or damage to a system. Malicious code describes a broad category of system security terms that includes attack scripts, viruses, worms, Trojan horses, backdoors, and malicious active content.	**Worst anyone can think of. It can lead to complete Network/Server hijack with NO Control over it.**
Data Interception	Data sent over Wi-Fi can be captured by eavesdroppers – easily, within a few hundred feet; even farther with directional antennas.	Confidential Data Loss
Denial of Service	A denial-of-service attack (DoS attack) or distributed denial- of-service attack (DDoS attack) is an attempt to make a machine or network resource unavailable to its intended users.	Complete/Partial Server and/or Network Shutdown. Resulting in loss of productivity.
Rogue APs	Business network penetration by unknown, unauthorized APs has long been a top worry.	Business Client's Leads Loss
Wireless Intruders	Detecting malicious Wi-Fi clients operating in or near a business' airspace.	Hack into Network. **Legal implications***.
Mis-configured APs	Configuration errors posed a significant security threat. Prioritization and segmentation for multi-media further complicates configuration.	IT Implementation Revenue Loss, Hacking of Network, Misuse of Bandwidth.
Ad Hocs and Soft APs	Wi-Fi laptops have long been able to establish peer-to-peer ad hoc connections that pose risk because they circumvent network security policies.	Malware Injection in Organization Network or Client's System
Misbehaving Clients	**END USERS** that form unauthorized Wi-Fi connections of any type, whether accidentally or intentionally, put themselves and corporate data at risk.	Cyber Crime Liability on Organization Owner/Head **Legal implications***.
Endpoint Attacks	Automated attack tools like Metasploit can now be used to launch Wi-Fi endpoint exploits with minimal effort. Numerous exploits have been published to take advantage of buggy Wi-Fi drivers, using buffer overflows to execute arbitrary commands	Business Operations Disruption
Evil Twin APs	Fraudulent APs can easily advertise the same network name (SSID) as a legitimate hotspot or business WLAN, causing nearby Wi-Fi clients to connect to them	Cyber Crimes on Organization Wi-Fi Name. **Legal implications***.
Wireless Phishing	Man-in-the-middle application attacks, hackers continue to develop new methods to phish Wi-Fi users. Once poisoned, clients can be redirected to phishing sites long after leaving the hotspot, even when connected to a wired enterprise network.	Financial Data & Revenue Loss. **Legal implications***.

We would like to draw your kind attention to some provisions of the Information Technology Act that impose stringent liabilities upon organizations **handling sensitive personal data or information**.

Sensitive personal data or information has been defined by the Central Government in exercise of the powers conferred by clause (ob) of subsection (2) of section 87 read with section 43A of the Information Technology Act, 2000 (21 of 2000), to include information relating to:

- password
- financial information such as Bank account or credit card or debit card or other payment instrument details
- physical, physiological and mental health condition
- sexual orientation
- medical records and history
- Biometric information
- any detail relating to the above clauses as provided to body corporate for providing service and
- any of the information received under above clauses by body corporate for processing, stored or processed under lawful contract or otherwise

***Legal implications – Please read below**

Section 43 A	Section 72 A
Compensation for failure to protect data	**Punishment for disclosure of information in breach of lawful contract**
Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected.	Save as otherwise provided in this Act or any other law for the time being in force, any person including an intermediary who, while providing services under the terms of lawful contract, has secured access to any material containing personal information about another person, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain discloses, without the consent of the person concerned, or in breach of a lawful contract, such material to any other person, shall be punished with imprisonment for a term which may extend to three years, or with fine which may extend to five lac rupees, or with both.

Tips

1. Don't leave important ,sensitive, or confidential material lying around the office
2. Always Verify your Credentials
3. Keep your password secret
4. If you print it, go get it right away!
5. Use Google's cached mode to avoid spyware
6. Read error messages and checkboxes
7. Look before you click
8. Just don't Format data, Wipe it!
9. Update your software
10.Protect your PC, Phone, Emails data with backups
11.Use a firewall always
12.Install and update anti-virus software
13.Install and run anti-spyware software
14.Strengthen your web browser security
15. Install the latest OS service pack

Thank you for your business!

Our Portals

www.eCoreTechnoS.com

www.HackingTechnologies.com

www.LearnHackingSecurity.com

SCO 62-63, 3rd Floor, Sector – 17 A, Chandigarh | 0172-4009111 | 0172-4610064