SESSION HIJACKING ATTACK

In a session hijacking attack, cyber criminals gain unauthorized access to an active user session by exploiting vulnerabilities in web applications or networks. By taking control of the session, they can impersonate the user, access sensitive information, or conduct unauthorized actions, compromising the user's privacy and security.

IT Sections Applicable

IT Act Section 43 – This section deals with unauthorized access to computer systems, data theft, and other computer-related offenses.

IT Act Section 66C – This section specifically addresses identity theft. If a session hijacking attack is carried out with

the intention of impersonating an individual or causing financial or reputational harm to them, this section could be invoked.

IT Act Section 66D – This section covers cheating by impersonation using a computer resource.

IT Act Section 66E – This section deals with violation of privacy.

IT Act Section 72 – This section protects the confidentiality and privacy of information handled by service providers.

Don't let cyber intruders hijack your online ride;
secure your sessions and protect your stride.

PROMPT ENGINEERING

Prompt engineering refers to the manipulation of users through carefully crafted messages or prompts to deceive them into revealing sensitive information or performing unintended actions. This social engineering technique is commonly used in phishing attacks, where cyber criminals trick individuals into disclosing passwords, personal data, or financial details.

IT Sections Applicable

IT Act Section 43 – Unauthorized access to computer systems.

IT Act Section 66 – Computer-related offenses, including hacking.

IT Act Section 67 – Punishment for publishing or transmitting obscene material in electronic form.

IT Act Section 69 – Power to issue directions for interception or monitoring or decryption of any information through any computer resource.

IT Act Section 72 – Breach of confidentiality and privacy.

IT Act Section 79 – Intermediaries not to be liable in certain cases.

IT Act Section 84A – Modes or methods for encryption. The Central Government may, for secure use of the electronic medium and for promotion of e-governance and e-commerce, prescribe the modes or methods for encryption.

IT Act Section 85 – Offenses by companies.

Stay cautious and alert, so prompt engineering won't make you divert.

FILELESS ATTACKS

This attack evades traditional antivirus and detection systems by executing malicious code directly in computer memory, without leaving traces on the file system. These stealthy attacks exploit vulnerabilities in software, making them harder to detect and providing cyber criminals with remote access to systems for data theft, surveillance, or launching further attacks.

IT Sections Applicable

IT Act Section 43 (Unauthorized Access) – This section deals with unauthorized access to computer systems, data, or networks.
IT Act Section 43A (Compensation for Data Breach) – This section deals with the compensation for improper disclosure of personal information.
IT Act Section 66 (Computer-Related Offenses) – This section covers various computer-related offenses, including hacking.
IT Act Section 66B (Punishment for Receiving Stolen Computer Resources or Communication Devices) – If fileless attacks involve receiving stolen computer resources or communication devices, this section might be invoked.
IT Act Section 66C (Identity Theft) – If a fileless attack leads to identity theft, this section might apply.
IT Act Section 66E (Violation of Privacy) – In cases where privacy is violated through fileless attacks, this section might be invoked.
IT Act Section 66F (Cyber Terrorism) – If the fileless attack is carried out with the intent of causing terror or destabilizing critical infrastructure, this section could apply.

Silent and sneaky, fileless foes;
fortify your defenses and block their throes.

DELIVERY SCAM

A delivery scam involves cyber criminals sending fake notifications or tracking information to deceive recipients into believing they have a package or delivery pending. The scam aims to trick victims into revealing personal information, clicking on malicious links, or paying fake shipping fees, leading to financial loss or data compromise.

IT Sections Applicable

IT Act Section 43 – Penalty for unauthorized access, damage to computer systems, etc.

IT Act Section 66 – Computer-related offenses, including cheating by personation using a computer resource.

IPC Section 419/BNS 319 – Punishment for cheating by personation.

IPC Section 420/BNS 318 – Cheating and dishonestly inducing delivery of property.

Don't fall for the scammer's snare;
verify before you click 'Accept' or 'Share'.

VIRTUAL KIDNAPPING

This is a psychological extortion scheme where perpetrators manipulate victims into believing a loved one has been kidnapped, demanding ransom to ensure their release. Though no actual abduction occurs, the emotional distress and fear generated can lead victims to comply with the demands.

IT Sections Applicable

Information Technology Act, 2000

IT Act Section 66C – This section deals with identity theft, which could be relevant if someone's identity is misused in a virtual kidnapping scenario.

IT Act Section 66D – This section covers cheating by impersonation using a computer resource, which could apply if the perpetrator impersonates the victim.

Indian Penal Code (IPC)

IPC Section 503/BNS 351

This section deals with criminal intimidation, which could be relevant if threats are made in a virtual kidnapping scenario.

IPC Section 506/BNS 351

This section deals with criminal intimidation by threat of injury to a person's reputation, etc.

Guard your virtual realm with might;
virtual kidnappers shall lose the fight.

FORMJACKING

It is an attack that involves injecting malicious code into e-commerce websites' payment forms. The code steals payment card details or personal information entered by customers during online transactions, allowing cyber criminals to engage in payment fraud or identity theft.

IT Sections Applicable

Information Technology Act, 2000:

IT Act Section 43 – This section deals with unauthorized access to computer systems and data breaches.

IT Act Section 43A – This section deals with the compensation for failure to protect sensitive personal data.

IT Act Section 66 – This section deals with computer-related offenses,including hacking.

IT Act Section 66C – This section deals with identity theft.

Indian Penal Code, 1860:

IPC Section 420/BNS 318 – This section deals with cheating and dishonestly inducing delivery of property.

IPC Section 463/BNS 336 – This section deals with forgery.

IPC Section 464/BNS 335 – This section deals with making a false document.

Protect your forms with utmost care;
formjackers won't find their share.

CYBERSQUATTING

It refers to the practice of registering domain names similar to established brands or trademarks with the intent to profit from the brand's reputation or sell the domain back to the rightful owner at an inflated price. This can lead to brand dilution, reputation damage, and confusion among consumers.

IT Sections Applicable

IT Act Section 2(1)(r) – Defines "domain name," which is crucial in understanding the context of cybersquatting.

IT Act Section 43 – This section deals with penalties and compensation for damage to computer systems

IT Act Section 66-D – This section covers the offense of cheating by impersonation using a computer resource

IT Act Section 66-A – Although this section was struck down by the Supreme Court of India in 2015 for being unconstitutional,

IT Act Section 79 – While not directly focused on cybersquatting, this section deals with intermediary liability.

IT Act Section 81 – This section ensures that the provisions of the IT Act have an overriding effect, not with standing anything inconsistent in any other law for the time being in force.

Stake your claim in the digital space;
cybersquatters will find no place.

DNS HIJACKING

This attack involves altering the Domain Name System (DNS) settings of a computer or network, redirecting legitimate traffic to malicious websites. By intercepting and manipulating DNS queries, attackers can lead users to phishing pages, distribute malware, or engage in other malicious activities.

IT Sections Applicable

IT Act Section 43 – This section deals with unauthorized access to computer systems and data.

IT Act Section 66 – This section deals with computer-related offenses like hacking, which could cover unauthorized access, interference, or damage to computer systems.

IT Act Section 66C– This section deals with identity theft. If someone uses another person's identity to commit an offense related to DNS hijacking, this section could be invoked.

IT Act Section 66D – This section covers cheating by personation using computer resources.

IT Act Section 66E– This section deals with violation of privacy.

IT Act Section 72 – This section protects the privacy and confidentiality of information stored in a computer resource.

Don't let your online path divert; secure your DNS, stay alert.

SMS BOMBING

It is a form of harassment where attackers overwhelm a victim's mobile device with a large number of unwanted text messages, disrupting normal communication and potentially causing psychological distress. This attack aims to disrupt the victim's peace of mind or sabotage their ability to use their phone.

IT Sections Applicable

IT Act Section 66C – Identity theft : This section deals with punishment for identity theft, which includes dishonestly using another person's electronic signature, password, or any other unique identification feature.

IT Act Section 66D – Cheating by personation using computer resource :

This section addresses the act of cheating by personation using a computer resource, and it prescribes penalties for such actions.

IT Act Section 43 – Penalty and compensation for damage to computer, computer system, etc. : This section deals with penalties for unauthorized access to computer systems, data breaches, and causing damage to computer resources.

IT Act Section 66 – Computer-related offenses : This section covers various offenses related to computer systems, including hacking, unauthorized access, and introduction of viruses.

Bombarded by texts, it's no fun;
safeguard your phone, block the SMS gun.

INSIDER THREATS

Refers to security risks posed by individuals with legitimate access to an organization's systems, networks, or sensitive information. These threats may arise from employees, contractors, or business partners who intentionally or unintentionally misuse their privileges to steal data, commit fraud, or compromise the organization's security.

IT Sections Applicable

IT Act Section 43A – Compensation for Data Breach

IT Act Section 66C – Identity Theft

IT Act Section 66D – Cheating by Personation by using Computer Resource

IT Act Section 72 – Breach of Confidentiality and Privacy

IT Act Section 72A – Punishment for Disclosure of Information in Breach of Law

IPC Section 408/BNS 316 – Criminal Breach of Trust by Clerk or Servant

Be cautious of those who reside within;
trust but verify, and potential harm will thin.