

What is Digital Arrest?

October 27, 2025 • vajiramandravi.com



About Digital Arrest:

It is a new and innovative tactic employed **by cybercriminals** to defraud gullible victims and **extort money**.

- **Modus operandi:**

- The modus operandi in this cybercrime method is that **fraudsters pose as law enforcement officials** such as police, **Enforcement Directorate, CBI**, among others, and manipulate them into believing that they have committed some serious crime.
- In certain cases, the victims are “digitally arrested”, and forced to **stay visible over Skype or other video conferencing platforms** to the criminals until their demands are met.
- The cyber fraudsters deceive the victim into believing that he or she has been put under ‘digital arrest’ and will be prosecuted if they do not pay the scamsters a huge amount of money.
- The cyber criminals often force the naive victims to **self-arrest or self-quarantine themselves**, by tricking them into believing that they have been put under ‘digital arrest’ and cannot leave their house unless they pay up.

- **Preventing measures**

- **Cyber Hygiene:** It is done by regularly updating passwords, and software and also **enabling two-factor authentications** to reduce the chances of unauthorized access.
 - **Phishing Attempts:** These can be evaded by refraining from clicking on dubious links or downloading attachments from unknown sources and also authenticating the legitimacy of emails and messages before sharing any personal information.
 - **Secured devices:** By installing reputable **antivirus and anti-malware solutions** and keeping operating systems and applications up to date with the latest security protocols.
 - **Virtual Private Networks (VPNs):** VPNs can be employed to encrypt internet connections thus enhancing privacy and security. However one must be cautious of free **VPN** services and OTP only for trustworthy providers.
 - **Secure communication channels:** Secure communication techniques such as encryption can be done for the protection of sensitive information. Sharing of passwords and other information must be cautiously done especially in public forums.
 - **Awareness:** There is a need for preventive measures and increased public awareness.
-

Q1: What is Phishing?

It refers to an attempt to steal sensitive information, typically in the form of usernames, passwords, credit card numbers, bank account information or other important data in order to utilize or sell the stolen information.

Source: What is 'digital arrest', and what can you do to ensure you don't fall victim to cybercriminals?

Source: <https://vajiramandravi.com/current-affairs/digital-arrest/>

© Vajiram & Ravi. For personal use only.