

THE INDIAN MUSIC INDUSTRY

266, Kanchawala Bldg, 2nd Floor, Dr AB Road, Opp Passport Office, Above Saraswat Bank,
Worli, Mumbai - 400030 • Email: info@indianmi.org • Website: www.indianmi.org
GST No: 27AAAAT3648J1Z8

To

Date: 03rd October 2022

Ms. Pallavi D,

Joint Director, CDAC Pune and Member Convener of the Working Group

Ministry of Electronics and Information Technology (Government of India)

Electronics Niketan, 6, CGO Complex,

Lodhi Road, New Delhi – 110003

Subject: Representation in response to Draft Mobile Security Guidelines by the Ministry of Electronics and Information Technology (MeitY) issued on July 20, 2022 – Providing suggestions on addressing the cyber security implications caused due to the menace of digital piracy

Executive Summary

Digital Piracy: A Cybersecurity Threat to Mobile Device Users

Pirate websites and apps lure users to their platforms by offering “free content” as bait and subject users to cyber security threats by injecting malicious code onto the devices owned and operated by the users. The rate of digital music piracy in India stands at 68% and it is estimated that visits to illegitimate websites and apps lead to revenue losses of ₹217 crore to ₹300 crore annually to the recorded music industry.

As per a recent study by the Audiovisual Anti-piracy Alliance, there is an average 57% chance of an audiovisual piracy app being installed with embedded malware. Further, as per the Timeline to Compromise Report by Asia Video Industry Association, consumers could be exposed to cybersecurity threats within 42 seconds of clicking on a pirate website. Moreover, consumers using pirate websites and apps are 3 times more likely to be exposed to malware.

Suggestions to the Draft Mobile Security Guidelines with respect to

- Obligations of Service Providers

affiliated to



representing the
recording industry
worldwide

- Ad-tech service providers must conduct due diligence before purchasing ad-space on apps/ websites to ensure that they are not exposing users to security threats by using ad-space on pirate websites/ apps.
- Service providers such as mobile app stores must have technological measures in place to scrutinize mobile apps and prevent the listing of rogue apps that provide pirated content which is embedded with malware.
- Social media and mobile apps must work with network operators to ensure that links to pirate websites and apps that pose threat to mobile security are not being circulated amongst users.
- **Obligations of Network Operators**
 - The term “rogue apps” must be defined to include within its ambit all kinds of content piracy, in order to attribute legal certainty to the obligations provided under the Guidelines.
 - Network operators must implement robust detection systems for malware and other cybersecurity threats for displaying warnings to users.

Suggestions on Guidelines for Mobile Device Users

- Mobile device users must be sensitized on the grave nature of digital piracy and its link with malware and security vulnerabilities.
- Users must be provided guidance on how to spot a pirate site/ app.
- Users must be made aware of the different types of malwares (browser hijackers, keyword loggers etc.) and the various methods in which such malware is onboarded onto user devices.

Respected Madam,

The Indian Music Industry (IMI) is the apex body that represents the business and trade interests of the recorded music industry in India. IMI is registered under the West Bengal Societies Registration Act, 1961. We are writing this representation with reference to Draft Mobile Security Guidelines (“the Guidelines”) by the Ministry of Electronics and Information Technology (“MeitY”).

At the outset, as a key stakeholder in the digital content economy, IMI would like to highlight its appreciation for MeitY's initiative to issue security guidelines for mobile device and services. The Guidelines aim to protect sensitive data and provide security of transactions of every mobile device user, by following the mobile security control measures prescribed for various stakeholders involved in the mobile service ecosystem. **Given that pirate websites and apps expose mobile phone users to security threats of sensitive information loss and misuse of personal data by adversaries, we request you to consider our comments on the Draft Guidelines and provide for additional obligations on service providers, network operators and mobile device users.**

Digital Piracy and Malware: A Threat to Cybersecurity of Mobile Users

Digital piracy has a significant impact on the economy, as it adversely impacts future investments in creative content and affects government revenue streams. The rate of digital music piracy in India stands at 68%¹ and it is estimated that visits to illegitimate websites and apps lead to revenue losses of ₹217 crore to ₹300 crore annually to the recorded music industry.² However, the lesser-known consequence of digital piracy is cybersecurity risks for consumers.³ Pirate websites and apps lure users to their platforms by offering "free content" as bait and subject users to cyber security threats by injecting malicious code onto the devices owned and operated by the users.

As per a recent study by the Audiovisual Anti-piracy Alliance, there is an average 57% chance of an audiovisual piracy app being installed with embedded malware.⁴ Further, as per the Timeline to Compromise Report by Asia Video Industry Association, consumers could be exposed to cybersecurity threats within 42 seconds of clicking on a pirate website.⁵ Moreover, consumers using pirate websites and apps are 3 times more likely to be exposed to malware.⁶

Malware can be downloaded through malicious advertising, malicious popups, fake browser extension installations, browser notification hijacking, blocking notifications, adware,

¹ <https://indianmi.org/wp-content/uploads/2022/03/Digital-Music-Study-Report-2021-ONLINE.pdf>

² <https://indianmi.org/wp-content/uploads/2021/05/IMI-Economic-Report-Final.pdf>

³ <https://www.interpol.int/en/Crimes/Illicit-goods/Shop-safely/Digital-piracy>

⁴ <https://www.aapa.eu/study-on-malware-and-audiovisual-piracy-highlights-significant-risks-to-european-consumers>

⁵ <https://avia.org/how-cyber-criminals-use-ads-to-compromise-devices-through-piracy-websites-and-apps/>

⁶ <https://www.digitalcitizensalliance.org/clientuploads/directory/Reports/Breaking-Bads-Report.pdf>

malicious software installation and banner ads. Malware installed through a pirate site/ app can be used for capturing network traffic and banking credentials typed into a browser to commit financial fraud, facilitating identity theft by capturing personal data stored on a device, and moving laterally within a network to reconnoitre and further infect other, higher-value devices on the network, such as finance and payment systems.⁷

Suggested Obligations of Service Providers

The Guidelines must expressly include entities providing ad-tech services within the ambit of “Service Providers”. While providing content illegally, pirate apps and websites use advertisements to generate revenues and accord the element of legitimacy to the pirate app or website. In doing so, they not only give a boost to piracy by increasing site/app traffic but also expose consumers to cybersecurity threats.

Ad-tech companies are intermediaries whose services are used by brands or ad agencies for ad placement on publishing spaces available in the market. Take for instance, Google’s advertising technologies, which include its content delivery network and advertising delivering systems, appear to have provided 51% of ads to piracy apps.⁸ Approximately, 1 in 3 piracy websites and apps have advertising that exposes consumers to fraud and malware.⁹ Nearly 80 percent of pirate sites served up malware-ridden ads to their users and on average 1 in 6 times, a visit to a piracy site leads to an attempt to serve malware to the user.¹⁰ Therefore, the Guidelines must obligate ad-tech service providers to conduct due diligence before purchasing ad-space on apps/ websites to ensure that they are not exposing users to security threats by using ad-space on pirate websites/ apps.

Moreover, the Guidelines obligate network operators to deploy network and edge intelligence to eliminate rogue mobile apps and alter users of fraudulent transactions. Similarly, service providers such as mobile app stores must be obligated to have technological measures in place to scrutinize mobile apps and prevent the listing of rogue apps that provide pirated content which is embedded with malware. Furthermore, social media and mobile apps must work with

⁷<https://www.aapa.eu/study-on-malware-and-audiovisual-piracy-highlights-significant-risks-to-european-consumers>

⁸ <https://www.digitalcitizensalliance.org/clientuploads/directory/Reports/Breaking-Bads-Report.pdf>

⁹ <https://www.digitalcitizensalliance.org/clientuploads/directory/Reports/Breaking-Bads-Report.pdf>

¹⁰ <https://www.digitalcitizensalliance.org/clientuploads/directory/Reports/Unholy-Triangle-Report.pdf>

network operators to ensure that links to pirate websites and apps that pose threat to mobile security are not being circulated amongst users.

Suggested Obligations of Network Operators

We laud the acknowledgement of proliferation of rogue mobile apps and the inclusion of an obligation on network operators to deploy network and edge intelligence to eliminate them. However, it is pertinent that the term “rogue mobile apps” be defined to include within its ambit all kinds of content piracy, in order to attribute legal certainty to the obligations provided under the Guidelines. Guidance in this regard should be taken from the Delhi High Court judgment in *UTV Software Communication Ltd. and Ors. v. 1337X.TO and Ors.* (2013) wherein the factors to be considered for determining whether a website is a rogue website were laid down as follows: (i) whether the primary purpose of the website is to commit or facilitate copyright infringement, and (ii) the flagrancy of the infringement, or the flagrancy of the facilitation of the infringement.

Furthermore, network operators should be obligated to implement robust detection systems for malware and other cybersecurity threats for displaying warnings to users similar to browsers providing an intermediate warning page, that prevents the user from proceeding, until they click a button, acknowledging the risk detected.

Suggested Guidelines for Mobile Device Users

We applaud MeitY’s initiative to issue guidelines for mobile device users to facilitate awareness on basic security precautions and best practices to safeguard them from mobile device security threats. In this regard, it is pertinent to take note of the serious lack of awareness about digital piracy and its far-reaching consequences in terms of security breach. IMI’s empirical research on piracy shows that 27% of the surveyed respondents did not know the meaning of piracy and 32% did not know the consequences of pirating music.¹¹ Therefore, the Guidelines must also include sensitisation of mobile device users on the grave nature of digital piracy and its link with malware and security vulnerabilities to explain that even though consumption of pirated content can be tempting, the associated risks far outweigh its benefits.

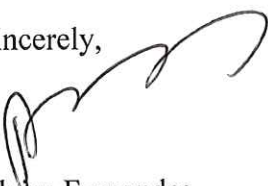
¹¹ <https://indianmi.org/wp-content/uploads/2022/04/Preventing-music-Piracy-through-Nudge-effect-Final-1.pdf>

We appreciate that the Guidelines lay down that users must use only official app stores for installing mobile applications and avoid third-party app stores unless they are sure about its authenticity. On similar lines, users must be provided guidance on how to spot a pirate site/app. For instance, one must be wary of any site offering a huge amount of content for a low price (or for free). Additionally, users must be made aware of the different types of malwares (browser hijackers, keyword loggers etc.) and the various methods in which such malware is onloaded onto user devices. Furthermore, the Guidelines must encourage use of trusted content from trusted sites and warn users against accepting copies from friends or unfamiliar sources.

Concluding Remarks

The pervasiveness of malware and fraudulent advertising on piracy websites and apps poses a significant risk to internet users who are targeted by an unholy union of pirate operators and hackers to infect and infiltrate their devices for profit. MeitY can assume an imperative role in imposing obligations on service providers and network operators to take steps to minimise the cybersecurity risks arising from pirate websites and apps as well as in raising awareness among consumers about the malware dangers associated with visiting pirate websites and apps. Therefore, we request you to consider our submissions and address the connection between content piracy and cybersecurity threats to mobile users in the Mobile Security Guidelines.

Sincerely,



Blaise Fernandes

CEO & President,

Indian Music Industry (IMI)