# Hackers exploit anime fandom in soaring malware phishing attacks targeting Gen Z



The rising intersection of technology and culture has led to an alarming trend in cybersecurity: hackers are increasingly disguising malware threats as anime content, a tactic that exploits the medium's soaring popularity, particularly among younger audiences. Recent research by Kaspersky, analysing phishing attacks up until early 2025, found that over 250,000 phishing emails themed around anime have been targeted at victims, primarily among Generation Z.

This demographic, those born in the early 2000s, has shown an unprecedented affinity for anime, with approximately 65% reportedly consuming this form of entertainment regularly. Such engagement fosters a deep emotional connection to beloved characters, making them susceptible to malicious phishing attempts masquerading as genuine content. The anime "Naruto" led the pack with around 114,000 phishing attempts, followed by titles like "Demon Slayer" and "Attack on Titan." These criminals often lure victims with enticing offers of "exclusive episodes" or "leaked scenes," leading to potentially harmful outcomes, including malware downloads and identity theft.

The sophistication of these phishing strategies extends beyond anime. Kaspersky's broader analysis revealed that in 2024, nearly 900 million phishing attempts were thwarted, marking a dramatic 26% increase from the previous year. Attackers frequently leveraged popular brands and trends to gain traction. Cybercriminals capitalised on the holiday season and specific event releases, such as the trailer for a new "Shrek" film, to amplify their schemes. The diversity in targeting—from anime to children's franchises like LEGO and Disney—underlines the pressing necessity for increased digital vigilance among users.

Despite the entertainment industry's continuing technological evolution, it poses substantial risk due to the exploitation of emotional connections with characters and brands. The trend of using beloved cultural symbols to propagate malware is not new, with Kaspersky noting a concerning 35% rise in attacks exploiting children's favourite brands within a year. The prevalence of malicious scripts targeting vulnerable demographics has made parents and guardians essential in safeguarding younger users against these dangers.

Different methods employed by cybercriminals signal a troubling innovation in the realm of malware distribution. For example, malware has been disguised not only as anime apps but also as other well-known popular culture references. A case from Symantec highlighted a malicious application posing as an anime character targeted Android users, capturing sensitive contact information through deceptive means, illustrating the lengths to which attackers will go to infiltrate devices.

This evolving landscape poses a dire call to action for cybersecurity. Experts emphasise the importance of using reputable streaming services and remaining sceptical of "too good to be true" offers that circulate via email or social media. Enhancing awareness and adopting robust cybersecurity practices are paramount to mitigate the risk posed by these increasingly sophisticated threats. As the digital and cultural landscapes continue to intertwine, safeguarding personal information will remain a critical challenge for all users navigating this space.

## Reference Map:

* Paragraph 1 – [[1]](https://www.techradar.com/pro/security/is-it-over-9-000-report-claims-hackers-are-increasingly-disguising-malware-as-anime), [[2]](https://www.kaspersky.com/about/press-releases/kaspersky-reports-nearly-900-million-phishing-attempts-in-2024-as-cyber-threats-increase)
* Paragraph 2 – [[1]](https://www.techradar.com/pro/security/is-it-over-9-000-report-claims-hackers-are-increasingly-disguising-malware-as-anime), [[3]](https://www.kaspersky.com/about/press-releases/attempted-cyberattacks-exploiting-kids-favorite-brands-grow-by-35-in-q1-2024)
* Paragraph 3 – [[4]](https://ics-cert.kaspersky.com/publications/reports/2024/12/25/threat-landscape-for-industrial-automation-systems-q3-2024/), [[6]](https://threatpost.com/attackers-using-anime-character-spread-malicious-android-app-091112/76998/)
* Paragraph 4 – [[2]](https://www.kaspersky.com/about/press-releases/kaspersky-reports-nearly-900-million-phishing-attempts-in-2024-as-cyber-threats-increase)
* Paragraph 5 – [[3]](https://www.kaspersky.com/about/press-releases/attempted-cyberattacks-exploiting-kids-favorite-brands-grow-by-35-in-q1-2024), [[7]](https://www.govtech.com/security/man-admits-to-writing-anime-trojan.html)

Source: [Noah Wire Services](https://www.noahwire.com)

## Bibliography

1. <https://www.techradar.com/pro/security/is-it-over-9-000-report-claims-hackers-are-increasingly-disguising-malware-as-anime> - Please view link - unable to able to access data
2. <https://www.kaspersky.com/about/press-releases/kaspersky-reports-nearly-900-million-phishing-attempts-in-2024-as-cyber-threats-increase> - In 2024, Kaspersky blocked over 893 million phishing attempts worldwide, marking a 26% increase from the previous year. Cybercriminals frequently impersonated well-known brands like Booking, Airbnb, TikTok, and Telegram to steal credentials or install malware. Additionally, users encountered more than 125 million attacks involving malicious email attachments. The surge in phishing attempts was particularly notable during the holiday season, with a significant spike between May and July. Kaspersky emphasized the importance of vigilance and robust cybersecurity solutions to combat these evolving threats.
3. <https://www.kaspersky.com/about/press-releases/attempted-cyberattacks-exploiting-kids-favorite-brands-grow-by-35-in-q1-2024> - Kaspersky's research revealed a 35% increase in cyberattacks exploiting children's favorite brands in Q1 2024 compared to the same period in 2023. Attackers targeted popular brands like LEGO, Paw Patrol, Bluey, and Disney to distribute malware. Notably, over 1.2 million infections were attributed to downloaders, which, while not inherently malicious, often serve as conduits for additional unwanted applications. The study highlighted the growing trend of cybercriminals leveraging children's entertainment to spread malware and emphasized the need for enhanced cybersecurity awareness among parents and guardians.
4. <https://ics-cert.kaspersky.com/publications/reports/2024/12/25/threat-landscape-for-industrial-automation-systems-q3-2024/> - Kaspersky's Q3 2024 report on industrial automation systems highlighted a significant increase in malicious scripts and phishing pages targeting these systems. The rise was attributed to widespread phishing attacks in August and September, where threat actors used malicious scripts mimicking CAPTCHA interfaces and browser error messages to deceive users into executing commands that downloaded additional malware. These attacks were distributed through various channels, including phishing emails, malicious links, and malvertising networks found on adult sites, file-sharing services, betting platforms, anime resources, and web apps that monetize through traffic.
5. <https://en.wikipedia.org/wiki/Rensenware> - Rensenware is a unique form of ransomware that encrypts files on Windows computers and demands the user achieve a high score in the bullet hell video game 'Undefined Fantastic Object' before decrypting the files. Developed as a joke by Korean programmer Kangjun Heo in 2017, Rensenware encrypts files using AES-256 and appends '.RENSENWARE' to the filenames. The ransomware's main window displays Minamitsu Murasa, a character from the Touhou Project. Heo later released a patch to neutralize Rensenware after it gained attention.
6. <https://threatpost.com/attackers-using-anime-character-spread-malicious-android-app-091112/76998/> - Symantec warned Android users about a malicious application posing as a popular anime character, designed to steal personal contact information and send it to a third party. The app, named Anaru, was actually the Android.Maistealer malware, a Trojan that collects data such as contact names and email addresses. It was distributed through third-party marketplaces imitating Google Play. Upon installation, the app requests access to storage, network communication, and personal information, which it uses to steal data from the device.
7. <https://www.govtech.com/security/man-admits-to-writing-anime-trojan.html> - A Japanese man, Masato Nakatsuji, admitted in court to creating a data-destroying Trojan horse that used copyrighted anime footage to spread via the Winny file-sharing system. The malware displayed images of popular anime characters while deleting music and movie files from users' computers. Nakatsuji was charged with copyright infringement and defamation for embedding an acquaintance's photograph into the malicious code. This case marked one of the first instances of a virus writer being arrested in Japan.