# Cybercriminals increasingly target social media influencers with sophisticated scams and hijackings



Cybercriminals are increasingly targeting influential social media accounts, particularly on platforms like YouTube and Instagram, to exploit trending topics and trick viewers into losing cryptocurrency or falling victim to scams, malware, and data theft. According to recent research by Bitdefender Labs, account hijackings of content creators surged sharply throughout 2024 and have continued evolving into 2025.

These hijackings primarily affect popular content creators and influencers with millions of followers and billions of views. Bitdefender detected over 9,000 malicious livestreams on YouTube in 2024 alone. These livestreams often occur on compromised channels that impersonate trusted public figures or well-known brands to spread fraudulent schemes and malware. For example, one hijacked account amassed a total of 12.4 billion views—meaning that if just 1% of viewers were deceived, over 124 million users could be affected.

Attackers frequently masquerade as prominent companies such as Tesla, Ripple, or SpaceX. They employ deepfake technology to simulate public personalities like Elon Musk or Donald Trump during fake livestreams, promoting cryptocurrency scams and phishing links. This elaborate impersonation aims to build trust and lure unsuspecting users into revealing sensitive information or transferring funds.

Instagram has also become a significant target for hackers, especially through phishing attacks. Cybercriminals impersonate Meta or Instagram Support via fraudulent emails, create cloned login pages, and manipulate creators into disclosing SMS verification codes necessary for account access. In addition, malicious sponsorship offers have been used as an infiltration tactic. Content creators are enticed to download files purporting to be promotional materials, which instead contain malware. Malvertising campaigns promoting fake AI tools or anticipated games like GTA VI have also been detected, often installing information stealers or remote access trojans on victims’ devices.

Events that attract large online audiences tend to be exploited by scammers. Notable examples include Apple keynotes, the high-profile XRP-SEC lawsuit, and CS2 gaming tournaments. During such events, cybercriminals launch fake official livestreams or run fabricated contests to exploit peak viewer interest. For instance, at the 2025 White House Crypto Summit, fraudulent YouTube streams advertised fake cryptocurrency airdrops designed to deceive attendees into surrendering confidential data or funds.

Bitdefender has issued several safety recommendations for creators to safeguard their accounts and audiences. These include using browsers with built-in security features, enabling multi-factor authentication (MFA), and vigilantly monitoring accounts for unusual activity. Creators are encouraged to scrutinise unexpected sponsorship offers, particularly those linked to trending topics. Implementing advanced Distributed Denial of Service (DDoS) protection can help prevent service interruptions following account takeovers. Additionally, the use of trusted proxy services can add layers of anonymity and security when managing multiple social media accounts.

Training team members on emerging cybersecurity threats and keeping abreast of official security updates from platforms and cybersecurity researchers are also essential steps. Bitdefender offers specialised products, such as Bitdefender Security for Creators, which provides 24/7 account monitoring, scam email filtering, and guided support for account recovery in the event of a breach.

The Tech Radar is reporting these developments as the digital landscape for content creators and their communities faces escalating cyber threats, underlining the growing need for robust security measures.

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

## Bibliography

1. <https://www.bitdefender.com/en-us/blog/hotforsecurity/account-takeover-attacks-on-social-media-a-rising-threat-for-content-creators-and-influencers> - This article corroborates the claim that cybercriminals increasingly target social media content creators, especially on platforms like YouTube and Instagram, with a surge in account takeovers and malicious livestreams continuing into 2025 as reported by Bitdefender Labs.
2. <https://www.mi-3.com.au/10-04-2025/rise-cybercrime-activities-targeting-content-creators-bitdefender> - This source supports the specific statistic that over 9,000 malicious livestreams on YouTube were detected in 2024, showing the scale of hijackings involving compromised channels impersonating trusted figures.
3. <https://securitybrief.com.au/story/rising-threats-to-influencers-as-cyber-attacks-escalate> - This article confirms details about the large-scale impact of hijacked creator accounts, including impersonations of public figures and brands, the massive view counts on compromised channels, and the use of malicious domains linked to scams and malware.
4. <https://securitybrief.asia/story/rising-threats-to-influencers-as-cyber-attacks-escalate> - Similar to the previous source, this coverage supports the description of tactics used by cybercriminals such as rebranding YouTube channels, deepfake impersonations, and targeting creators with phishing and malware campaigns on Instagram.
5. <https://www.bitdefender.com/en-us/blog/hotforsecurity/how-to-protect-your-social-media-accounts-from-hackers> - This Bitdefender resource validates the safety recommendations given to creators, including the use of multi-factor authentication, browser security features, monitoring for unusual account activity, advanced DDoS protection, and caution with suspicious sponsorship offers.
6. <https://www.techradar.com/news/influencers-are-increasingly-targeted-by-cybercriminals-heres-how-to-protect-yourself> - Tech Radar's report complements the article by highlighting the escalating cyber threats to content creators and their audiences, emphasizing the rising need for robust cybersecurity measures in the digital influencer space.
7. <https://www.techradar.com/pro/millions-at-risk-as-cybercriminals-successfully-compromise-popular-youtube-accounts-heres-how-to-stay-safe> - Please view link - unable to able to access data