AL2025_18 YouTube Warns of AI-Generated CEO Video Used in Phishing Attacks (18th March 2025)

Description

YouTube has issued a warning regarding a phishing campaign leveraging AI-generated deepfake videos of CEO Neal Mohan. Scammers use these videos to trick content creators into divulging their login credentials. The fraudulent campaign falsely claims that YouTube is altering its monetization policies, and it employs urgent tactics to pressure victims into compliance. The phishing scheme has been active since late January 2025, with YouTube launching an official investigation in mid-February.

Attack Details

The attackers distribute the AI-generated video via private YouTube messages and emails, falsely claiming it contains critical updates regarding monetization policy changes. The phishing email directs recipients to a fake YouTube Partner Program (YPP) verification page (studio.youtube-plus[.]com). Once users enter their credentials, they receive a deceptive message stating their channel is "pending" and are prompted to open a malicious document linked in the video description.

To manipulate victims further, the phishing emails explicitly state that YouTube does not share information via private videos, paradoxically advising users to report any suspicious channels. Additionally, the scammers create urgency by warning that failure to act within seven days will lead to restricted account functionality, including limited video uploads and demonetization.

Once credentials are stolen, scammers hijack the victims' accounts and re-purpose them for cryptocurrency scam streams, misleading their audiences and causing significant financial and reputational harm.

Indicators of Compromise (IoCs)

- Emails claiming to be from YouTube, announcing urgent changes to monetization policies.
- Private videos shared via YouTube or email, allegedly from YouTube's CEO.
- URLs mimicking legitimate YouTube domains, such as studio.youtube-plus[.]com.
- Phishing sites requesting re-authentication for YouTube Partner Program access.
- Fake confirmation messages stating that the channel is "pending" after entering credentials.
- Hijacked accounts used to stream cryptocurrency scams.

Remediation

YouTube continues to monitor and address this evolving phishing campaign, urging all users to remain vigilant against fraudulent schemes exploiting AI-generated content.

- **Do Not Click Suspicious Links**: Avoid clicking links in emails or private messages claiming to be from YouTube. Verify official announcements through YouTube's website.
- **Enable Two-Factor Authentication (2FA)**: Strengthen account security by enabling 2FA to prevent unauthorized access.
- **Report Suspicious Activity**: Report phishing attempts to YouTube via their official help center.
- **Check Official YouTube Channels**: YouTube does not share sensitive updates via private videos. Cross-check any major announcements on YouTube's official blog.
- **Recover Hacked Accounts**: YouTube provides a support assistant to help users recover compromised accounts and secure them from further attacks.
- **Educate and Raise Awareness**: Content creators should stay informed about phishing tactics and educate their communities to avoid falling victim to such scams.

The Guyana National CIRT recommends that users and administrators review this alert and apply it where necessary.

References

- FadilpaŠI, S. (2025, March 6). YouTube warns of phishing video using its CEO as bait. Retrieved fromTechRadar. https://www.techradar.com/pro/security/youtube-warns-of-phishing-video-using-its-ceo-as-bait
- Gatlan, S. (2025, March 5). YouTube warns of AI-generated video of its CEO used in phishing attacks. Retrieved from BleepingComputer. https://www.bleepingcomputer.com/news/security/youtube-warns-of-ai-generated-video-of-its-ceo-used-in-phishing-attacks/