ARMY CRIMINAL INVESTIGATION DIVISION

CRIME PREVENTION
GENERATIVE AI ENABLED THREATS

Authorized for widest release without restrictions.

The recent rollout of the GenAI.mil platform to all DoW employees underscores how generative AI has become a standard feature in today's digital landscape. This swift integration means similar capabilities are available on the open market, where criminals are already leveraging them to enhance their tactics. Adversaries are using AI to amplify traditional criminal methods, making them more scalable, personalized, and deceptively realistic. Stay informed about these emerging threats and learn how to protect yourself and your loved ones.

AI-ENABLED IMPERSONATION AND FINANCIAL FRAUD

Currently, this is the most prevalent and damaging category of AI-enabled crime.

- **Voice-Cloning Scams:** Criminals can create convincing audio clones of a person's voice using just a few seconds of publicly available audio. They often use these clones in "virtual kidnapping" scams, where a target receives a frantic call from what sounds like a loved one in urgent need of money.
- **Deepfake Video Fraud:** In a notorious incident, criminals used deepfake technology to impersonate a company's CFO during a video call, tricking a finance employee into transferring over $25 million.

AI-ENHANCED PHISHING AND INFORMATION THEFT

Generative AI enables criminals to mass-produce highly personalized phishing attacks that are increasingly difficult to detect.

- **Exploiting AI Summaries:** In one case, criminals embedded hidden text with a malicious phone number into a harmless email. AI tools, like Google Gemini, read this text and present the malicious contact as legitimate, directing unsuspecting users to scammers.
- **Sophisticated Phishing Emails:** AI tools allow foreign adversaries to craft grammatically correct and contextually relevant phishing emails, eliminating the spelling and grammar errors that once signaled a scam.

BEST PRACTICES

- Critically evaluate information, especially from digital channels, and cross-reference with trusted sources.
- Report phishing emails and content to the appropriate authorities.
- Verify unusual requests for information through official channels before responding.
- Establish a "safe word" or duress code with family to confirm identities during suspected emergency calls.
- Use strong passwords and enable multi-factor authentication.
- Avoid sharing sensitive information online.

ADDITIONAL RESOURCES

- FBI Warns of Increasing Threat of Cyber Criminals Utilizing Artificial Intelligence
- FinCEN Alert on Fraud Schemes Involving Deepfake Media Targeting Financial Institutions
- Hong Kong Clerk Defrauded of $25 Million in Sophisticated Deepfake Scam
- Google Gemini Tricked Into Showing Phishing Message Hidden in Email

Key Insights on Generative AI and Deepfakes

- ***Generative artificial intelligence*** focuses on creating new content, such as text, images, or code. It learns from existing data to generate new, original content.
- A ***deepfake*** is an image or video that uses AI to mimic a person's likeness, making it appear as though someone said or did something they never did.

Because these technologies are inexpensive to produce and widely accessible, criminals can now manufacture tailored disinformation with ease.

SUBMIT A TIP

Reporting is Anonymous

https://www.cid.army.mil/Submit-a-Tip/

SUBMIT A TIP