ARMY CRIMINAL INVESTIGATION DIVISION

29 April 2024

# Cybercrime Prevention Flyer

## Criminal Use of Artificial Intelligence

Artificial Intelligence (AI) is the automation of the human learning process and human intelligence using machines, computers, and digital devices. Applied in most fields, such as commerce, education, engineering, finance, government, healthcare, logistics, and many others, AI reduces human error, enables faster decision making, and increases productivity and efficiency, surpassing the ability and performance of humans.

Arguably, AI has more advantages than disadvantages. Cybercriminals, recognizing the advantages, are leveraging AI to make their "work" more effective, scalable, and yield higher payoffs.

**Audio/Visual Impersonation**

A/V impersonation refers to creating or altering videos for the purpose of committing fraud or influencing the recipient of the content. AI provides criminals the capability to create high-quality, photorealistic images and videos of people, to include nonconsensual sexual images or videos used by sextortion scammers.

Recommendations:

- Be cautious communicating with unknown individuals online.
- Look for movement anomalies in the video and listen for audio discrepancies.

**Voice Cloning**

Voice cloning refers to the use of AI to generate a voice that replicates that of someone you know, such as a family member or friend, or a voice that is publicly recognizable, such a public figure or well-known person. For example, voice cloning has been used in virtual kidnapping scams.

Recommendations:

- If the voice is recognized but the call is questionable, verify the caller's identity by calling the person back on a known number or contacting them by other means.
- If the call involves virtual kidnapping, call a mutual friend or family member of the "kidnapped" victim to verify the person is safe. Even contact the "kidnapped" victim via other means to confirm their safety.
- If the call is a scam, hang up and block the number.

**Robocalls**

Robocalls refers to using automated-dialing software to contact millions of mobile phone users with a prerecorded scam message. Paired with a known cloned voice, scammers can make the robocall appear authentic and legitimate, increasing the likely success of the scam.

Recommendations:

- If the number is unknown, do not answer the call.
- If answered, hang up and block the number.
- Do not respond to any questions or any prompts.
- Register with the Federal Trade Commission National Do Not Call Registry.

**Password Cracking**

With the assistance of AI, criminals can quickly automate brute force or dictionary password attacks. AI assisted password cracking is used to reduce the amount of time it takes a criminal to hack into an account.

Recommendations:

- Change passwords frequently.
- Use long passwords with a combination of upper and lowercase characters, numbers, and symbols.
- Enable two-factor authentication.
- Do not use passwords across multiple accounts.

**Malware**

AI is evolving malware, making it easier to develop, especially for the novice hacker, and more sophisticated, harder to detect by network defenders and antivirus software. With AI, cybercriminals can expand the attack volume, increasing the likelihood of success. On the plus side, AI can assist the victim system with a level of protection, but the victim, end-user, remains the weakest link.

Recommendations:

- Keep operating systems and anti-virus software updated.
- Avoid opening unknown or unrequested attachments.
- Do not click on links in suspicious emails.
- Do not click on infected system notification pop-ups.

**Phishing Emails and Text Scams**

A common tip for identifying phishing emails and text message scams is to look for typos and grammatical errors. AI provides a way criminals can create grammatically correct and convincing emails and text messages; even legitimate appearing personalized emails or messages. The more legitimate the content appears, the increased likelihood the email or text is believed and the scam succeeds.

Recommendations:

- Do not click on unrequested links.
- Do not download unknown files or attachments.
- Do not respond to requests for account information, passwords, or personally identifiable information (PII).
- Do not respond to requests for personal identification numbers (PINs) if you did not actually log into the account.
- If an email or text appears legitimate, contact the sender directly using a phone number or contact method found on the sender's official website. It's common for financial institutions to send legitimate emails or text messages.

**Department of the Army Criminal Investigation Division: Report a Crime**
**FBI Internet Crime Complaint Center (IC3): File a Complaint**
**Federal Trade Commission: Report Fraud**
**National Center of Missing and Exploited Children (NCMEC): Report Incident**



To receive Cyber Field Office Cybercrime Prevention Flyers, send an email to: CYDIntel@army.mil

CPF 0019-2024-CID461

Cyber Field Office
Russell Knox Building
27130 Telegraph Road
Quantico, VA 22134