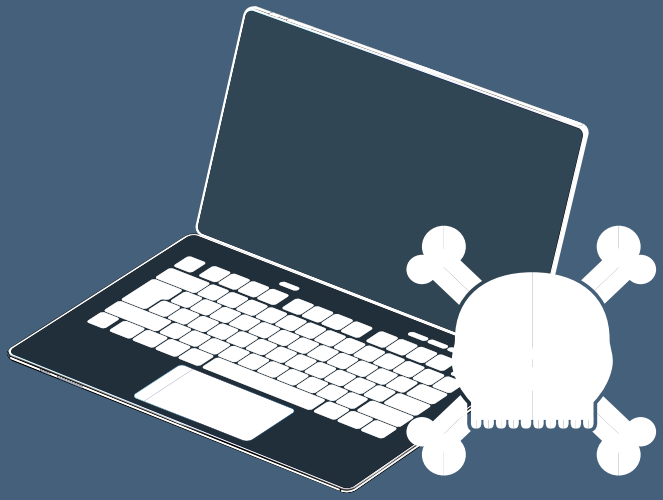
5 WAYS CYBER-CRIMINALS ARE WEAPONISING ARTIFICIAL INTELLIGENCE

Recent years have seen artificial intelligence (AI) surge in popularity among both businesses and individuals. Applications of this technology are widespread, but some of the most common include computer vision solutions, natural language processing systems, and predictive and prescriptive analytics engines. Although AI technology can certainly offer benefits in the realm of cyber-security, it also has the potential to be weaponised by cyber-criminals. As such, it's crucial for businesses to understand the cyber-risks associated with this technology and implement strategies to minimise these concerns. Here are five ways cyber-criminals are leveraging AI technology and tips to help businesses safeguard themselves against its weaponisation.

1. CREATING AND DISTRIBUTING MALWARE



In the past, only the most sophisticated cyber-criminals were capable of writing harmful code and deploying malware attacks. However, AI chatbots are now able to generate illicit code in a matter of seconds, permitting cyber-criminals with varying levels of technical expertise to launch malware attacks with ease. In addition to writing harmful code, some AI tools can generate deceptive videos claiming to be tutorials on downloading certain versions of popular software that distribute malware to targets' devices when they view this content.

2. CRACKING CREDENTIALS

Many cyber-criminals rely on brute-force techniques to reveal targets' passwords and steal their credentials so they can then utilise their accounts for fraudulent purposes. Yet, these techniques may vary in effectiveness and efficiency. By leveraging AI technology, cyber-criminals can bolster their password-cracking success rates, uncovering targets' credentials at record speeds.

3. DEPLOYING SOCIAL ENGINEERING SCAMS

Social engineering consists of cyber-criminals using fraudulent forms of communication (eg emails, texts and phone calls) to trick targets into unknowingly sharing sensitive information or downloading harmful software. Unfortunately, AI technology could cause these scams to become increasingly common by giving cyber-criminals the ability to formulate persuasive phishing messages with minimal effort. It could also clean up errors in human-produced copy to make it appear more convincing.

4. IDENTIFYING DIGITAL VULNERABILITIES

When hacking into targets' networks or systems, cyber-criminals usually look for software vulnerabilities they can exploit, such as unpatched code or outdated security programs. While various tools can help identify these vulnerabilities, AI technology could permit cyber-criminals to detect a wider range of software flaws, thus providing additional avenues and entry points for launching attacks.

5. REVIEWING STOLEN DATA

Upon stealing sensitive information and confidential records from targets, cyber-criminals generally have to sift through this data to determine their next steps—whether it's selling this information on the dark web, posting it publicly or demanding a ransom payment in exchange for restoration. This can be a tedious process, especially with larger databases. With AI technology, cyber-criminals can analyse this data much faster, allowing them to make quick decisions and speed up the total time it takes to execute their attacks. In turn, targets will have less time to identify and defend against attacks.

PROTECTING AGAINST WEAPONISED AI TECHNOLOGY

Looking ahead, AI technology will likely contribute to rising cyber-attack frequency and severity. By staying informed on the latest AI-related developments and taking steps to protect against its weaponisation, businesses can maintain secure operations and reduce associated cyber-threats. Key safeguards for businesses to consider include adopting workplace policies that promote proper cyber-hygiene, implementing automated threat detection technology to engage in continuous network monitoring, creating detailed cyber-incident response plans and purchasing ample cyber-cover.

WE CAN HELP

Above all, it's important for businesses to understand that they don't need to navigate this evolving cyber-risk landscape alone. Trusted insurance professionals can provide much-needed guidance and cover solutions. Contact us today for further resources.