Proactive Strategies Needed for Emerging Cyber Security Threats in 2024

The digital landscape never remains static. Technology continues to advance each year, driving productivity and innovation, making the impossible feel ever more possible. But the dark side of technology evolves just as quickly. Wise business leaders keep an eye on emerging security threats and adjust cyber security measures to keep pace.

In 2023, AI and machine learning top the list of cyber security concerns. But other emerging trends such as data poisoning have also gained attention. And common attack methods like ransomware and social engineering remain a persistent threat.

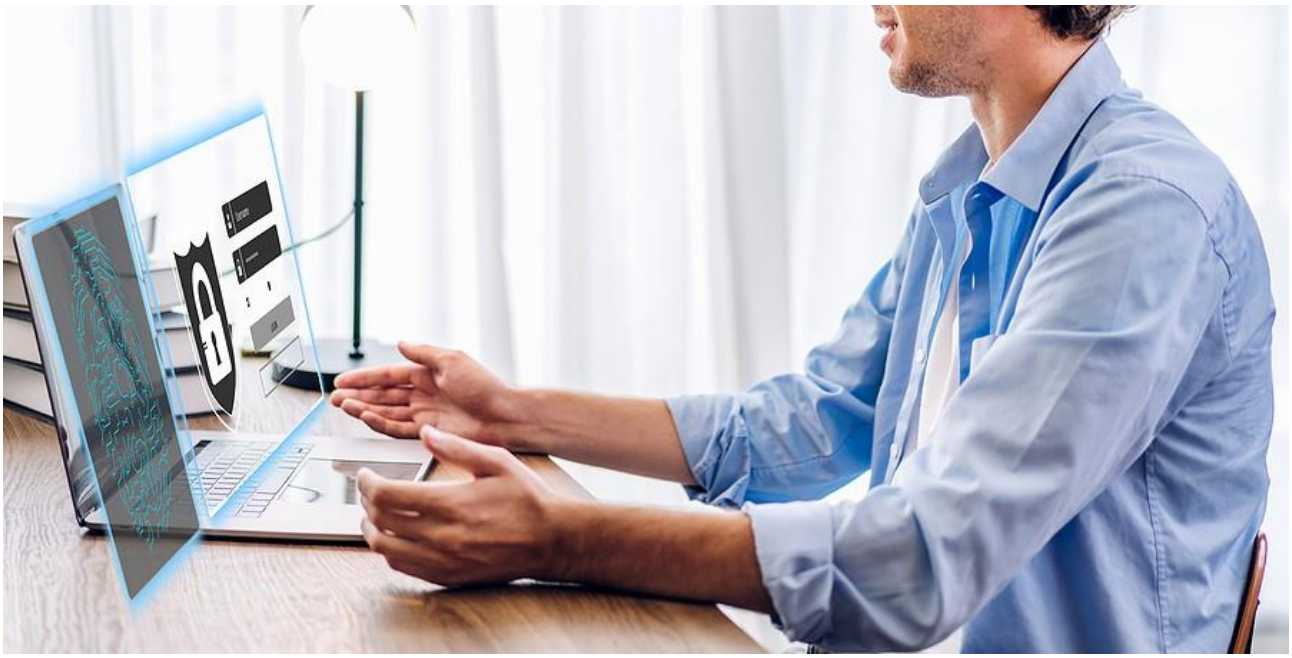
Forward-thinking organizations keep an eye on the horizon. They know the threats. And they proactively adjust security strategies to meet them head-on.

AI and Machine Learning

The technology world is of two minds regarding AI and machine learning. Some see AI as the ticket to a powerful future, with fantastic capabilities. Others worry that unchecked advances in AI technology will prove highly dangerous. Both perspectives have merit.

AI delivers incredible advances in nearly every facet of society, from manufacturing to healthcare and cyber security. Yet, at the same time, it introduces new vulnerabilities, as well as powerful tools for attackers to wield.

For instance, generative AI has increased attackers' ability to code malware more rapidly and target victim systems with greater precision. AI also enables attackers to take social engineering to new levels.



While users have become more savvy about recognizing classic signs of phishing, such as poor grammar or unusual wording, AI helps hackers fly under the radar. They can generate believable-sounding emails and text messages in almost any language. And by training AI models with data available online, they can mimic specific individuals very precisely.

In a related threat, AI provides the tools bad actors need to create increasingly convincing deepfakes. Audio and video deepfakes can prove almost impossible to distinguish from reality. In addition to spreading misinformation, they can be used to enhance phishing scams.

Data and SEO Poisoning

AI relies on complex algorithms and large language models (LLMs) trained on huge sets of data. When hackers manipulate the data used to an LLM, they can cause the model to produce biased or incorrect information. This can have disastrous results. For example, poisoning the data used in a manufacturing LLM could result in serious safety issues.

Hackers can also conduct SEO poisoning. By manipulating search engine results, they can make malicious websites appear higher in search results and thus more authentic. Unsuspecting users who click on a malicious link prove more likely to follow prompts to download malware-infected files.

Tried and True Attack Methods Evolving

Emerging threats rightly have security professionals concerned. However, ransomware and social engineering remain favorite weapons and continually evolve. As indicated above, AI-powered social engineering attacks have become more targeted and highly convincing. In fact, a 2023 report by Comcast shows that 90 percent of breach attempts began with phishing.

Ransomware players also continue to adjust their methods. For instance, the FBI has warned of threat groups that conduct multiple ransomware attacks in quick succession on the same victim. A subsequent attack on an already compromised network can cause substantial harm. Attackers have also begun using wiper tools, which erase data rather than encrypting it.

Emerging Cyber Security Threats Require Updated Solutions

Faced with increasingly sophisticated cyber threats, security strategies must also evolve. AI-powered security tools allow security teams to respond to threats in real time and at scale. Microsoft 365 enhanced security features offer a powerful example of how AI can improve defender capabilities and efficiency in the face of threats.

To learn more about Microsoft 365 security and other essential security strategies, contact the information security professionals at eMazzanti Technologies.