

AI and the Internet of Things (IoT)

How internet-enabled devices can introduce information security risks and how to protect them.

As AI technology becomes increasingly integrated into everyday work environments, it's crucial to understand the associated risks.

While these IoT devices enhance productivity and streamline operations, they also introduce new vulnerabilities that malicious actors can exploit.

A compromised smart printer could become an entry point into the company's network, potentially allowing unauthorized access to sensitive information.

Hackers can manipulate AI algorithms, which could lead to data breaches or even disrupt business operations.

*So, how can you help mitigate these risks?
Here are some important steps to follow:*

Ensure that all smart devices you use are regularly updated with the latest security patches.

Implement strong, unique passwords for your accounts and devices, and enable multi-factor authentication wherever possible.

Be proactive in participating in regular security audits to help identify and address potential vulnerabilities.

Equally important is fostering a culture of security awareness.

Regular training sessions can help you recognize and respond to potential threats, ensuring everyone plays a vital role in safeguarding data, networks and the organization from threats to IoT devices.

