Cyber-secure behaviour in linked industrial environments

Scope

How can something as simple as opening an attached file with malicious content lead to the entire production of a firm suddenly ending up in the hands of a hacker?

Most people use digital technology at work today, in one way or another, and that means there are risks that everyone needs to face, regardless of their role.

Industrial automation has been rapid and today many processes are controlled and monitored digitally. Equipment can be linked to the company's other systems to help industry become more efficient. Unfortunately, this linking also makes it easier for whoever wants to carry out a cyber attack that could impact on the firm's safety as well as production.

The purpose of this guide is to increase awareness of cyber security among those working in an industrial environment and to give an understanding of the risk behaviour that can lead to incidents and dangerous situations. The guide is especially aimed at those who are not yet familiar with cybersecurity issues.

Contents