Be alert or #YouMayBeNext

YOUMAYBENEXT

On 1 June 2022, INTERPOL launched a campaign to raise awareness that cyber attacks can happen to anyone at any time.

The #YouMayBeNext campaign focuses on extortion-related cybercrimes such as:

- DDoS (Distributed Denial-of-Service) attacks - a hacking attack carried out from multiple locations simultaneously, the aim of which is to prevent the functioning of an entire service on the Internet (e.g. your website and mail located on the hosting),
- ransomware - malicious software that encrypts files or steals sensitive data from the system,
- pressure material - recordings, pictures with nudity used for blackmail.

The project outlines key tactics used by cybercriminals to exploit vulnerabilities, as well as tips on how to detect them, so that individuals and businesses increase their knowledge of how to secure their systems, networks and devices.

The campaign, which runs from 1-17 June primarily through social media, will involve 60 countries, private sector partners, NGOs and international organisations.

Full accessibility, low costs as well as the possibility of anonymisation make cyberterrorism one of the most popular forms of expressing terrorist acts for political or ideological reasons. The virtual world has entered practically every social, advertising, professional and social space, causing the boundaries between the real and virtual worlds to become completely blurred.

Cyber-security is one of five modules of an e-learning course on terrorist prevention, which TPCoE conducts via the portal: https://learning.tpcoe.gov.pl/

https://www.interpol.int/News-and-Events/News/2022/New-campaign-highlights-digital-extortion-threats-and-how-to-keep-safe

Previous Page
Next Page