UNIVERSITI TEKNOLOGI MARA
Cawangan Sarawak
Kampus Mukah

Inou Dengah UiTM Mukah?

5th Issue | VOLUME 1 : JULY 2026

UiTM di hatiku **BULLETIN**

EDITORIAL BOARD

MEET THE TEAM

PROFESSOR DR. FIRDAUS ABDULLAH
Patron

DR. ABDUL JABBAR ABDULLAH
Advisor

MS. SITI FARIDAH KAMARUDDIN
Chief Editor

MS. STEFANIE NATASHA RICH JOSEPH
MS. FAKHIRA JAFRI
MS. CINDY ROBERT
MRS. NUR NADIA QAUSAR JUHARI
MS. SHIRLEY CLARE JERI
Editors

MR. MUHAMMAD ANAS ABDUL RAZAK
Records & Archives

MRS. IRENE SELUROH
Layout & Design

MR. SHILEYIUSKEN MIJEN
Webmaster

MR. ANAS ASRAWY PENDAPAT
Photographer

MR. ERICKSON GRAVESENT MUZIDI
Internship Trainee

Published by:
Corporate Communication Unit, UiTM Mukah Campus
eISNN : 2976-257X
Published Date : 7 July 2026

NEWS AND ARTICLES

MALAYSIA'S BIGGEST CYBER THREATS IN 2026

Authors: Adeena Mazwa Rabytah Amir Abdullah and Fakhira Jafri

Malaysia's digital economy is expanding rapidly, and so are the threats. Recent reports show ransomware incidents have risen sharply and now hit small and medium enterprises disproportionately, while attackers increasingly use AI to automate and personalise attacks. As a result, these trends affect organisations across Peninsular Malaysia and East Malaysia, including Sarawak, so local businesses and citizens should prioritise basic cyber hygiene now.

To begin with, attackers use large language models and voice or video cloning to craft highly convincing scams and impersonations. This is called AI-powered phishing and social engineering. Moreover, deepfakes and AI-generated messages make verification harder. Therefore, always verify unusual requests through a second channel and train staff to spot subtle signs of fraud. Another growing concern is that ransomware attacks on Malaysian organisations have increased significantly. SMEs now account for a large share of victims, and the average breach cost has risen. To mitigate this risk, practical steps can be taken, including maintaining offline backups, applying timely patches, and testing incident response plans.

Beyond this, adversaries increasingly exploit vendors and hidden suppliers to reach targets. Research shows a high proportion of Malaysian software supply chains have been attacked, revealing unseen dependencies. Consequently, organisations must map third-party risk, enforce minimum security standards, and monitor vendor behaviour. At the same time, utilities, healthcare, finance, and telecoms face persistent, sophisticated probes from state and criminal actors. National authorities have elevated cybersecurity as a strategic priority, so accordingly, organisations in these sectors should adopt zero-trust segmentation and coordinate with regulators. Finally, attacks are staying hidden longer, detection times have increased, and this allows attackers to move laterally and exfiltrate data. In response, faster detection and continuous monitoring, including endpoint detection, log aggregation, and threat hunting, are essential to reduce impact.

The good news is that many protections are straightforward, such as enabling multi-factor authentication, keeping systems patched, backing up data offline, verifying unusual requests, and assessing vendor security. For example, for residents in Mukah and across Sarawak, starting with staff awareness and basic technical controls can make a significant difference. Overall, these low-cost steps dramatically reduce risk while national programmes and industry guidance continue to evolve.

Published by:

Corporate Communication Unit, UiTM Mukah Campus

eISNN : 2976-257X

Published Date : 7 July 2026

Telephone/Fax
084-876100/084-876300

Email Address
korporat_swk@uitm.edu.my

Website
https://sarawak.uitm.edu.my/

Address
Universiti Teknologi MARA (UiTM)
Cawangan Sarawak Kampus Mukah,
KM 7.5 Jalan Oya,
96400 Mukah, Sarawak.