CURRENT CYBER THREATS

How to Protect the Organization

Next

Most cyber attacks don't start with hacking systems...

THEY START BY TRICKING PEOPLE.

That means, the biggest risk to any organization... is not the technology.

IT'S HOW WE USE IT.

Cybersecurity = Protection ?

Cybersecurity is...

the practice of protecting hardware, software, networks, data, processes, controls, programs, and systems from unauthorized access.

From Awareness → Business Protection

Cybersecurity = **Business Continuity enabler**, not just protection.

- Cyber risk is now **one of the top enterprise risks globally**.
- Cyber threats are **increasing in frequency and sophistication**.

Every organization, regardless of size is a **target**.

Cyber incidents can lead to:

- **Financial loss**
- **Operational disruption**
- **Reputational damage**

Why Cybersecurity Matters

The question today is no longer **"WILL WE BE ATTACKED?"**

But, **WHEN?**

From Prevention → Resilience and Recovery

Cybersecurity directly supports:

- Revenue protection
- Customer trust
- Regulatory compliance

CYBER INCIDENT IMPACTS

Data Breaches and Loss

Operational Disruption

Financial Losses

Reputational Damage

Current Cyber Threat Landscape

Beyond "Threats Exist" → "Threats Are Targeted and Strategic"

Attackers are:

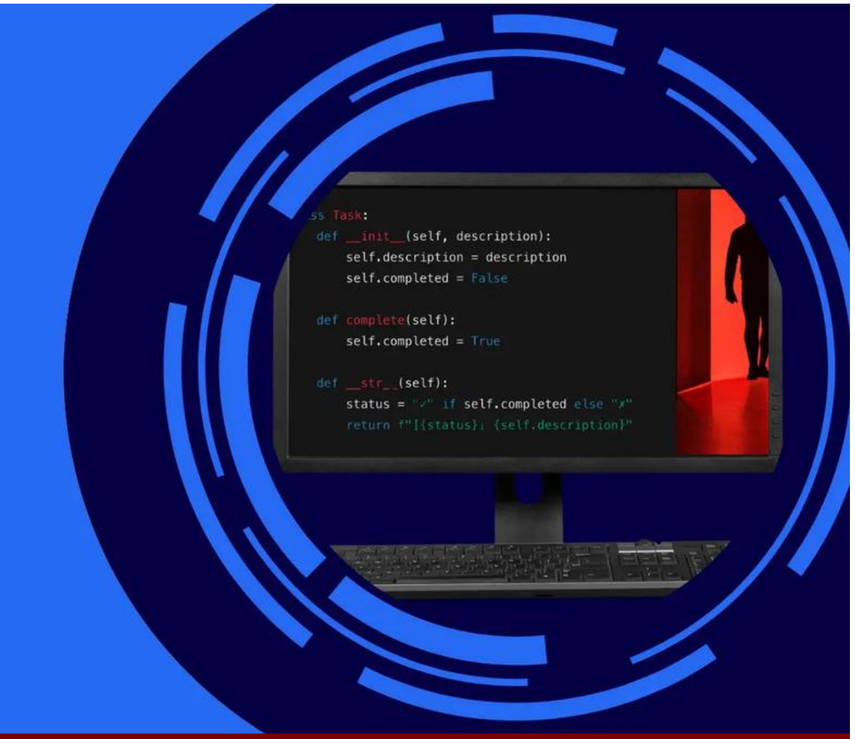
Organized (cybercrime groups, ransomware-as-a-service)

Financially motivated

Increasingly automated (AI-assisted attacks)

Beyond "Threats Exist" → "Threats Are Targeted and Strategic"

Organizations are targeted based on:

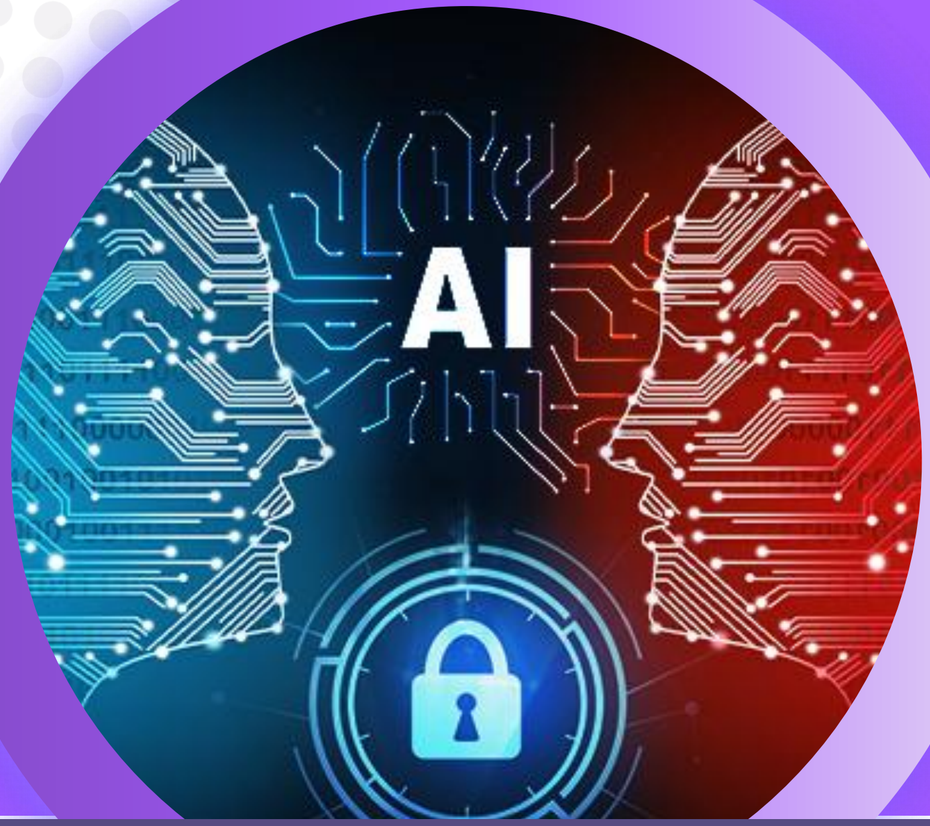


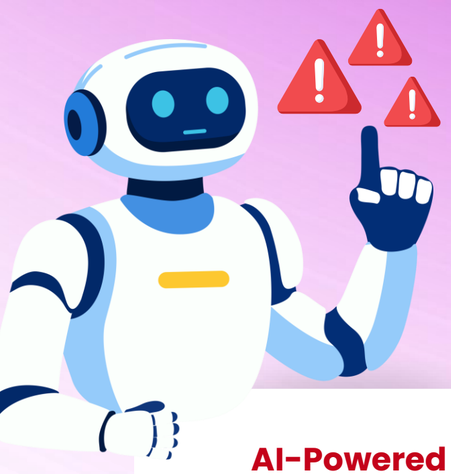
Weakest entry points
(e.g., unpatched systems)

Human behavior
(e.g., clicking a suspicious link)

Third-party exposure
(e.g., vendor system breach)

According to the World Economic Forum's Global **Cybersecurity Outlook 2026** report published in January 2026...



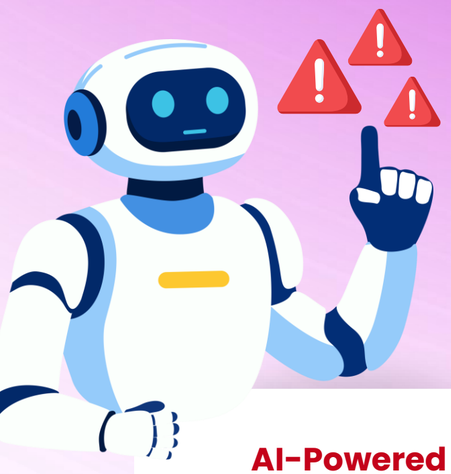


AI-Powered Cyber Attacks

AI is making attacks faster, more advanced, and harder to detect.

Threat actors are leveraging AI to:

- **Automate phishing campaigns.**
- **Generate realistic deepfake identities.**
- **Bypass traditional detection systems.**

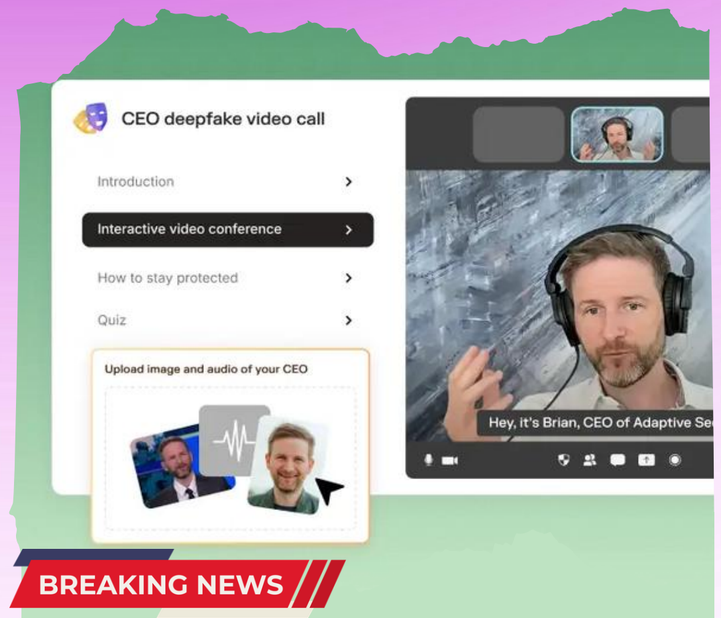


AI-Powered Cyber Attacks

AI is making attacks faster, more advanced, and harder to detect.

Rising & More Sophisticated Threats

Cyberattacks are increasing in frequency, scale, and complexity.



BREAKING NEWS

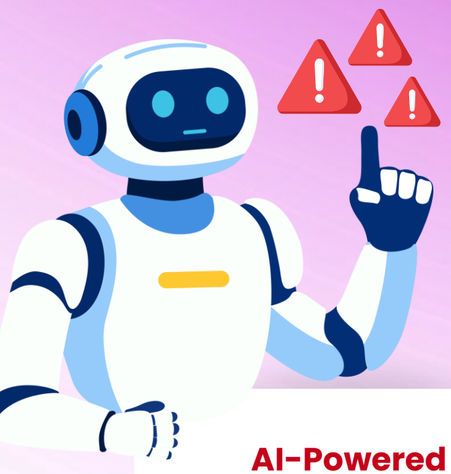
Arup Deepfake: How An AI-Generated Video Stole $25 Million

Source: PurpleSec (January, 2026)

- AI can **bypass traditional verification** (voice/video ≠ trusted anymore)
- Attacks are **multi-stage** (not just one method).

  e.g., **Started with phishing email → then deepfake video call.**
- **Human trust is the main target.**

  No systems were hacked. People were manipulated.



AI-Powered Cyber Attacks

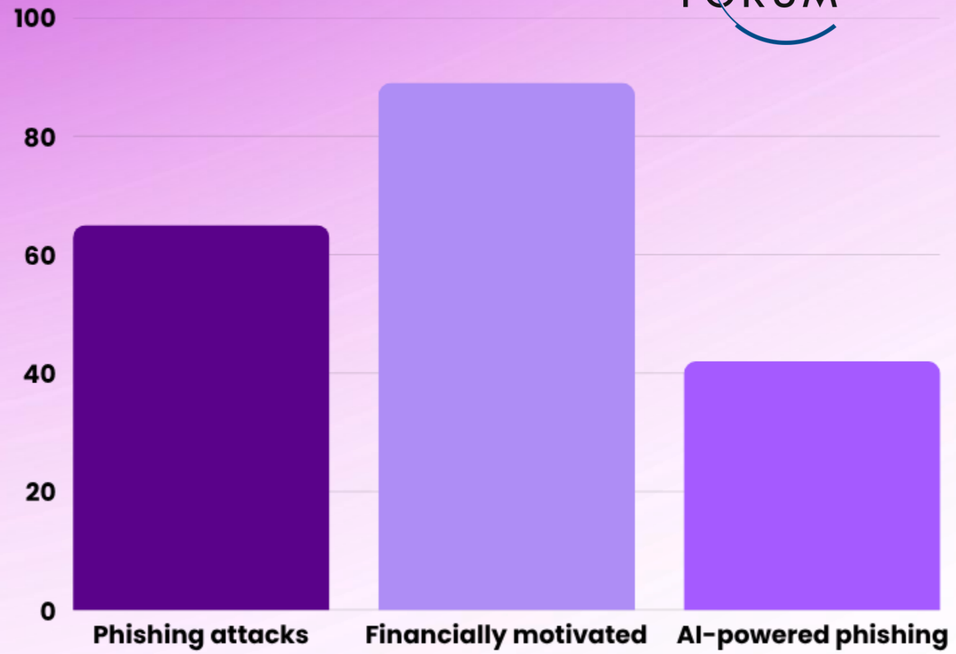
AI is making attacks faster, more advanced, and harder to detect.

Rising & More Sophisticated Threats

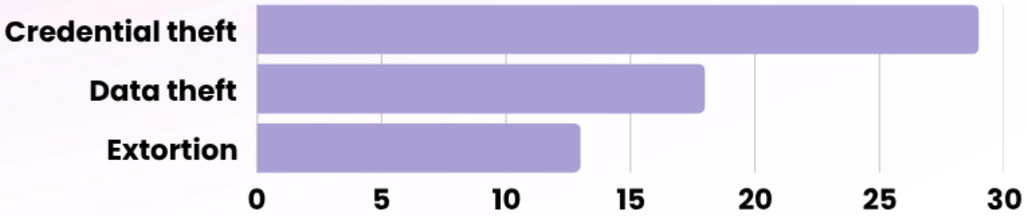
Cyberattacks are increasing in frequency, scale, and complexity.

Growth of Cyber Fraud & Social Engineering

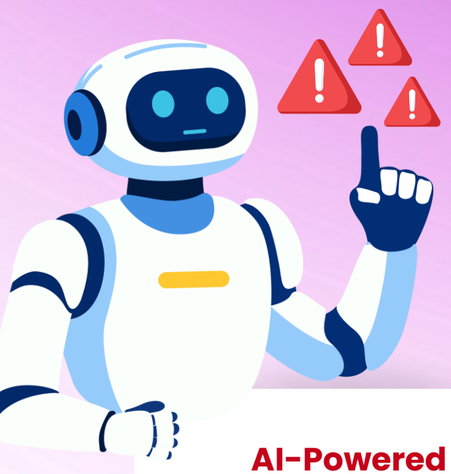
Phishing, scams, and deepfakes are becoming major threats to organizations.



The Outcomes of Social Engineering Attacks



Source: SpaceLift (January, 2026)



AI-Powered Cyber Attacks

AI is making attacks faster, more advanced, and harder to detect.

Rising & More Sophisticated Threats

Cyberattacks are increasing in frequency, scale, and complexity.

Growth of Cyber Fraud & Social Engineering

Phishing, scams, and deepfakes are becoming major threats to organizations.

Supply Chain & Geopolitical Risks

Attacks target vendors and are influenced by global conflicts.

Ransomware Attack

Often delivered through:

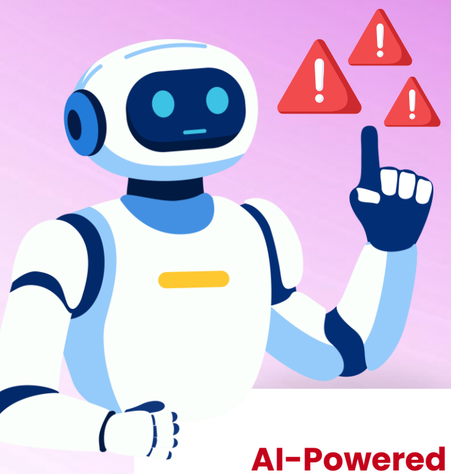
- ✓ Compromised software updates.
- ✓ Infected vendor systems.

Attackers use supply chains to:

- ✓ Scale attacks (one entry → many victims)
- ✓ Increase pressure → higher ransom payments.

sains

WORLD ECONOMIC FORUM



AI-Powered Cyber Attacks

AI is making attacks faster, more advanced, and harder to detect.

Rising & More Sophisticated Threats

Cyberattacks are increasing in frequency, scale, and complexity.

Growth of Cyber Fraud & Social Engineering

Phishing, scams, and deepfakes are becoming major threats to organizations.

Supply Chain & Geopolitical Risks

Attacks target vendors and are influenced by global conflicts.

Lack of Cyber Preparedness

Many organizations are still not ready, making cyber resilience critical.

Social Engineering and Phishing Attacks

- Phishing is still the **#1 entry point for cyber attacks**.
- The real risk is not the email; it is the **action taken**.
- Attackers exploit:
  - Urgency
  - Authority
  - Curiousity

HOW WE REDUCE RISK?

Slow down decision-making under pressure.

Verify requests via secondary channels.

Report even if unsure (false alarm is acceptable).

Malware and Ransomware

- Ransomware is now a **business disruption strategy**, not just an IT issue.
- Modern attacks include:
  - Data theft + extortion
  - Targeting backups

HOW WE REDUCE RISK?

Limit spread (network awareness, access control)

Encrypt sensitive data (at rest and in transit)

Early reporting = Smaller impact

Ransomware Hits Swinburne Sarawak 2024

How It Happened?

Hackers broke into the system and stole a large amount of data (hundreds of GBs).

Action Taken

- The university team is working quickly to resolve the issue and reduce impact.
- The Computer Emergency Response Team (CERT) of the Malaysia National Cyber Security Agency has been notified.

Lesson Learned

- Quick action can help limit damage and stop the attack from spreading.
- Notifying authorities (like national cybersecurity agencies) helps bring in expert support and coordination.
- Ongoing effort is needed to fully minimize impact.

Source: Swinburne University of Technology (2024)

Human Factor

*“It only takes **one** click.”*

How Human Error Fuels Cyber Attacks

According to findings from KnowBe4, cybersecurity incidents involving human factors increased by **90%** in 2025.

From this report, one thing is clear:

The biggest cyber risk is not the system, but the user.

NOW, WHY AWARENESS MATTERS?

- Help users recognize threats (phishing, scams, suspicious links).
- Reduces risky behaviors (password reuse, unsafe downloads).
- Strengthens the first line of defense: **people**.

Best Practices for Cybersecurity

HOW ACTIONS REDUCE RISK AND PROTECT THE BUSINESS?

Passwords & MFA

Action:
Strong passwords + MFA

Risk Reduced:
Unauthorized access

Business Value:
Prevents system compromise

Email Awareness

Action:
Verify before clicking

Risk Reduced:
Phishing entry point

Business Value:
Prevents ransomware incidents

Device Security

Action:
Secure devices, avoid unknown USBs

Risk Reduced:
Malware infection

Business Value:
Maintains operational continuity

From Controls to Confidence

Organizational Controls That Protect the Business

- Implement layered security (defense-in-depth).
- Regular backups and recovery testing.
- Continuous monitoring and detection.
- Employees awareness programs.

Roles and Responsibilities

WHAT TO DO INCASE OF A CYBER INCIDENT?

1. Stay calm and act quickly.
2. Identify and isolate the issue.
3. Do NOT attempt to fix it yourself (unless trained).
4. Preserve evidence; do not delete data or shut down endpoints.
5. Report immediately to the IT team.

Follow organization incident response procedures.

Incident Reporting Channels

Report incidents via:

- Dedicated Security Team / CDO or ACDO of your department.

Contact Center: **1-300-88-7246** or
contactcentre@sains.com.my

Use official channels only (avoid informal reporting).

Provide clear details:

01 What happened?

02 When it happened?

03 Affected system/device and screenshot (if possible)

Cyber Incidents Examples
Reporting Guides

PHISHING (FAKE EMAILS/MESSAGES)

e.g., User received a suspicious (likely phishing) email.

TrustedBank™

Dear valued customer of TrustedBank,

We have recieved notice that you have recently attempted to withdraw the following amount from your checking account while in another country: $135.25.

If this information is not correct, someone unknown may have access to your account. As a safety measure, please visit our website via the link below to verify your personal information:

http://www.trustedbank.com/general/custverifyinfo.asp

Once you have done this, our fraud department will work to resolve this discrepency. We are happy you have chosen us to do business with.

Thank you,
TrustedBank

What Should You Do?

1. Do not click any links or reply.
2. Click the “Report Phishing” button (if available).
3. If you clicked a suspicious link, change your password immediately.
4. Report to IT team immediately.

Cyber Incidents Examples
Reporting Guides

MALWARE INFECTION (NON-RANSOMWARE)

e.g., User downloads a malicious attachment → endpoint infected.

TrustedBank™

Dear valued customer of TrustedBank,

We have recieved notice that you have recently attempted to withdraw the following amount from your checking account while in another country: $135.25.

If this information is not correct, someone unknown may have access to your account. As a safety measure, please visit our website via the link below to verify your personal information:

http://www.trustedbank.com/general/custverifyinfo.asp

Once you have done this, our fraud department will work to resolve this discrepency. We are happy you have chosen us to do business with.

Thank you,
TrustedBank

What Should You Do?

1. Stop using the device.
2. Disconnect from Wi-Fi/network.
3. Do not try to fix it yourself.
4. Report to IT team immediately.

Cyber Incidents Examples
Reporting Guides

RANSOMWARE (FILES LOCKED)

e.g., Files encrypted, ransom note displayed.

What Should You Do?

1. Disconnect from the network immediately.
2. Do not click anything or pay.
3. Report to IT team immediately.
4. Inform your manager or CDO/ACDO.

SIMPLE STEPS TO REMEMBER

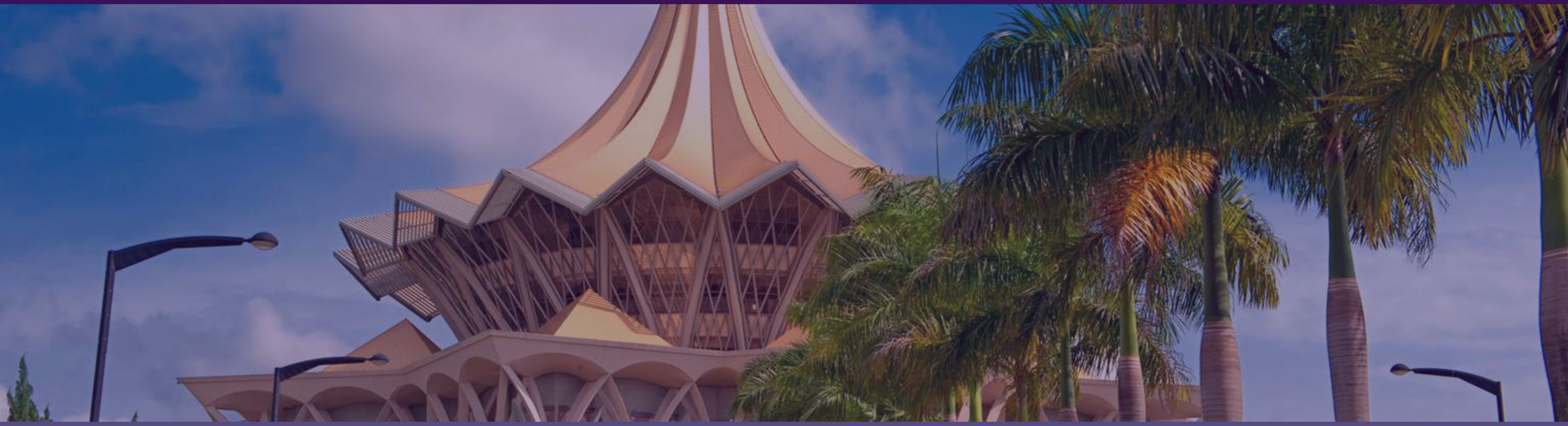
Stop → **Disconnect** → ***Report***

- **Stop** → Do not click, do not continue.
- **Disconnect** → Turn off Wi-Fi if needed.
- **Report** → Immediately inform IT team.

Cybersecurity is not just an IT issue

it is a shared responsibility across the organization.

One quick action, such as reporting a suspicious email, can prevent a major incident.



Thank You

Remember:

> Cybersecurity is a leadership issue, not just an IT issue.