BRUNEI CYBERSECURITY ASSOCIATION

January 2026 Newsletter

HAPPENING IN JANUARY:

- Bruneians Represent Nation at YSEALI CyberSafe ASEAN 2026
- CTF101 #1: ezctf
- Common Vulnerabilities and Exposures Report
  - CVE-2026-0629
- Cyber Threat Intelligence Report
  - PDFSIDER Malware Exploits DLL Side-Loading to Evade AV and EDR Defenses

ANNOUNCEMENT!

We are excited to share that the Brunei Cyber Security Association (BCSA) has moved to a new official website!

NEW WEBSITE	https://www.bcsa.bn
OLD WEBSITE	https://www.pksbrunei.org (***no longer in use***)

Please update your bookmarks and visit our website for the latest updates and events!

BRUNEI CYBERSECURITY ASSOCIATION

[Saedah Hasnal]

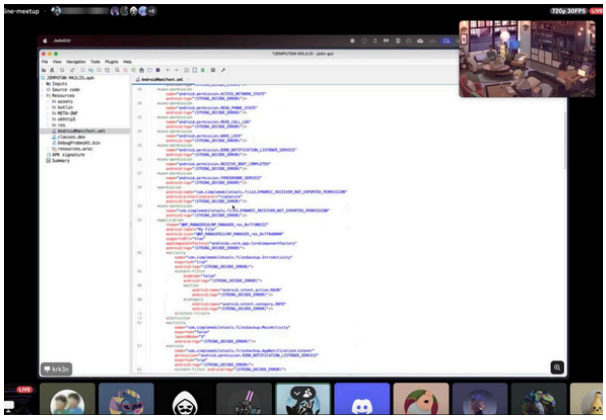
Bruneians Represent Nation at YSEALI CyberSafe ASEAN 2026

Three Bruneian cybersecurity professionals—Rahman Harith (Cybersecurity GRC, Darussalam Assets Sdn Bhd), Haziq Halidi (Assistant Land Officer, Ministry of Development), and Saedah Hasnal (Community Builder, Women in Cybersecurity Brunei)—represented Brunei at the YSEALI CyberSafe ASEAN 2026 workshop in **Jakarta** from **26–31 January 2026**. They joined young leaders and experts from across Southeast Asia in high-level discussions at the ASEAN Secretariat, focusing on strengthening regional cybersecurity cooperation and addressing the growing challenge of cross-border online scams and cyber threats.

The workshop emphasized practical, action-oriented problem solving through "Strike Teams," where participants developed and presented real-world solutions during an intensive solution sprint. Through this experience, the Bruneian participants gained deeper insights into regional cyber threats, built strong professional networks across ASEAN, and acquired practical frameworks that can be applied locally, contributing to stronger national cybersecurity resilience for Brunei.

CTF101 #1: ezctf

Place	User	Score
1	PostMelonnn	1000
2	testuser	900
3	Nightmare23	900
4	OrangBiasaV2	850
5	Blue1nvader	850



CTF101 is a monthly/bi-monthly online CTF that we run through discord, the CTFs will feature easy to solve challenges and aims to prepare potential CTF players for bigger CTF competitions. CTF101 will also be used to scout for potential CTF players to send out for regional competitions.

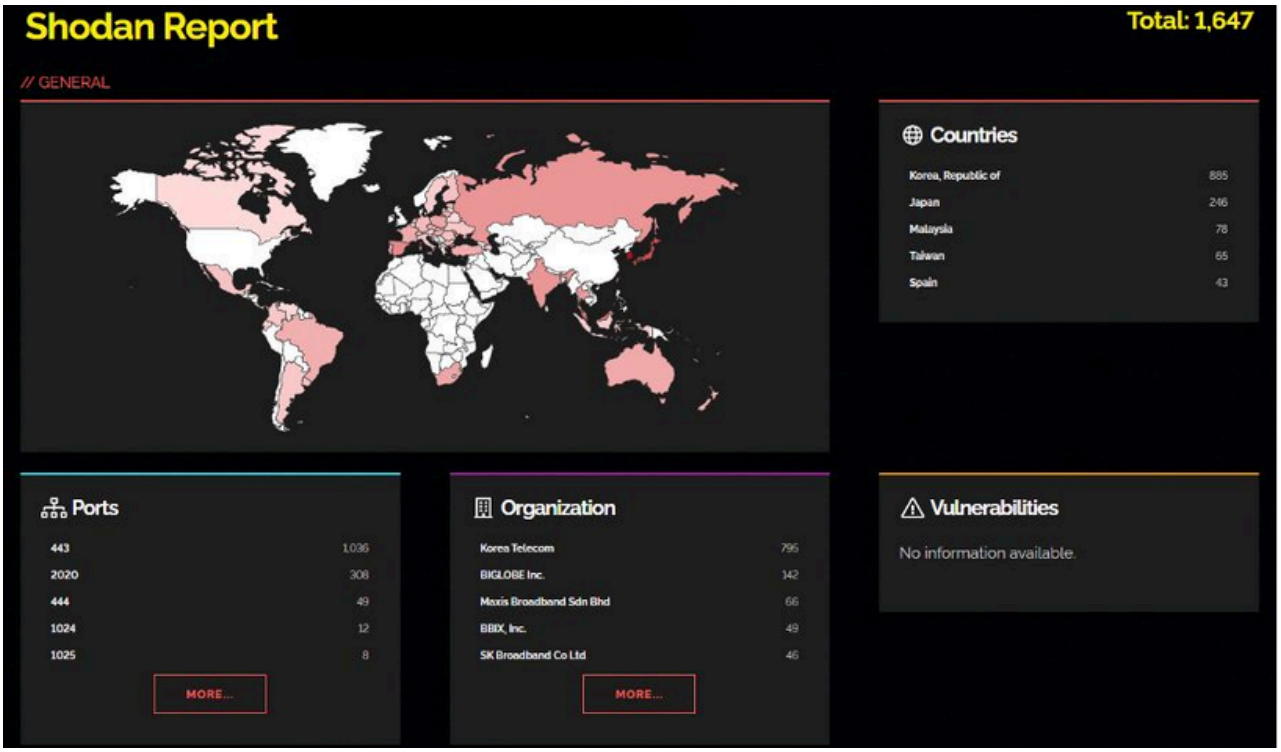
CTF101 #1: ezctf, was held on **29th January 2026 at 730PM**. During the event, Hafiz also shared technical research into latest scam tactics where scammers shared APK files. Hafiz demonstrated how to reverse engineer the APK file and use GenAI to summarize the findings. After that, Izdihar did a quick share on how to use Claude Code with its skills and agents to solve the CTF. A total of 12 participants joined the CTF with Abdul Mujib being the winner of the CTF.

Click **here** for future event details

BRUNEI CYBERSECURITY ASSOCIATION

Common Vulnerabilities and Exposures Report

CVE-2026-0629



A critical vulnerability (CVE-2026-0629) was discovered in TP-Link VIGI surveillance devices, involving an improper authentication flaw that could allow unauthorized access to administrator accounts and live camera feeds. While the interface was designed for local access, research via Shodan showed that over 1,000 devices were publicly accessible, indicating a significant potential impact. Following responsible disclosure, TP-Link promptly issued a security advisory and released patched firmware for all affected devices. The case highlights the importance of proactive security research, timely vendor response, and collaborative vulnerability disclosure to prevent real-world cyber incidents.

Read the full article **here**

BRUNEI CYBERSECURITY ASSOCIATION

Cyber Threat Intelligence Report

PDFSIDER Malware Exploits DLL Side-Loading to Evade AV and EDR Defenses

Resecurity disclosed PDFSIDER in early 2026 as a newly identified advanced persistent threat (APT)-style malware that exploits DLL side-loading to achieve stealthy execution and bypass antivirus (AV) and endpoint detection and response (EDR) tools. The malware masquerades as the legitimate Windows cryptbase.dll, which is side-loaded by a vulnerable signed binary, allowing it to deploy an in-memory backdoor. Once active, PDFSIDER performs system reconnaissance, executes remote shell commands interactively, and exfiltrates output covertly, while incorporating anti-VM/sandbox evasion checks. Delivered primarily via spear-phishing, the backdoor has already been observed in use by multiple ransomware actors as an initial payload delivery mechanism, reflecting a broader trend toward reliable, exploit-free execution techniques such as DLL side loading over vulnerability exploitation.

Click **here** to read more

BRUNEI CYBERSECURITY ASSOCIATION

Upcoming Events in February

HACK101 #1: NETWORKS

Date: 13th February
Time: 7.30 PM
Venue: Brunei Innovation Lab, Level 1, KHUB

This is an introduction level workshop in hacking network infrastructures. Network VAPTs refers to assessing systems and infrastructure that connecting and accessible through a network. In this session we will cover the tools and techniques of testing your own network for vulnerabilities!

Register **here**

AJCCA BOARD MEETING, KUALA LUMPUR

This annual gathering brings together member association representatives to exchange insights and discuss cybersecurity initiatives across the region.

BRUNEI CYBERSECURITY ASSOCIATION

Professional Training & Certification Program Schedule 2026

BRUNEI CYBERSECURITY ASSOCIATION

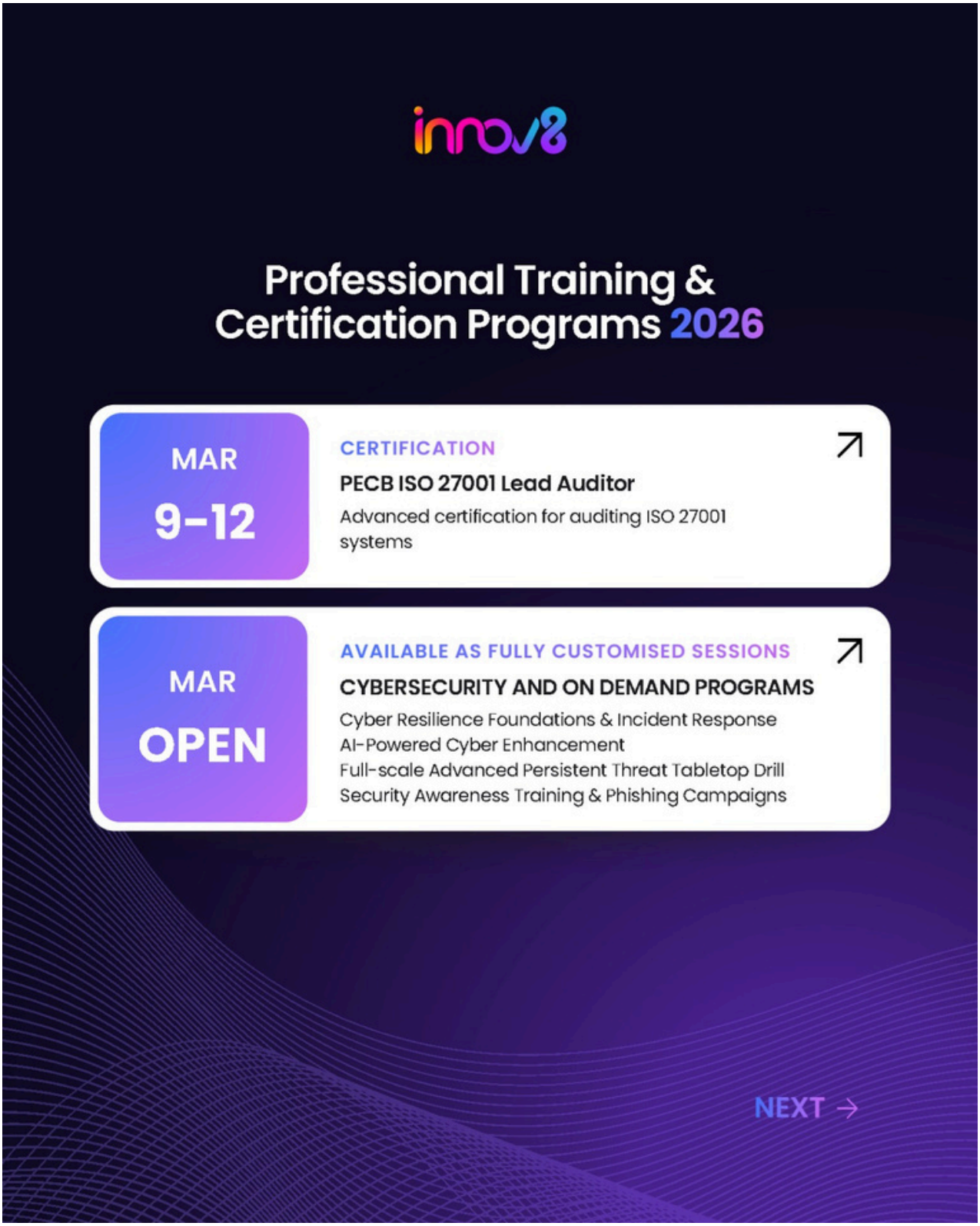
Professional Training & Certification Program Schedule 2026

BRUNEI CYBERSECURITY ASSOCIATION

Professional Training & Certification Program Schedule 2026

BRUNEI CYBERSECURITY ASSOCIATION

Professional Training & Certification Program Schedule 2026



BRUNEI CYBERSECURITY ASSOCIATION

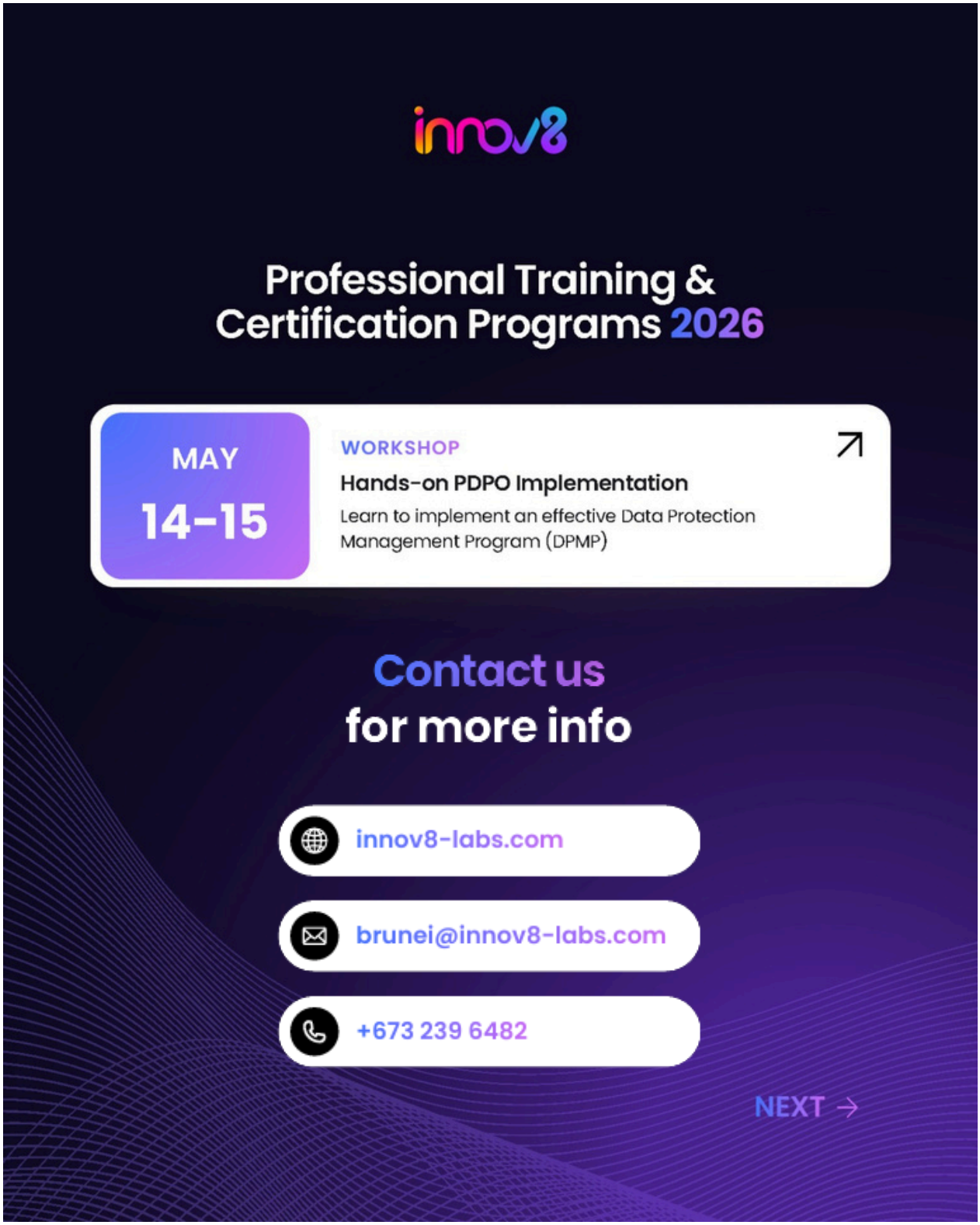
Professional Training & Certification Program Schedule 2026

BRUNEI CYBERSECURITY ASSOCIATION

Professional Training & Certification Program Schedule 2026

BRUNEI CYBERSECURITY ASSOCIATION

Professional Training & Certification Program Schedule 2026



BRUNEI CYBERSECURITY ASSOCIATION

Strong Passwords, Stronger Protection

28 January 2026

ALERT

149 Million Login Credentials Found in Publicly Accessible Database

A massive credential leak has exposed over 149 million usernames and passwords from services like Gmail, Facebook, Netflix and other online accounts in January 2026. The stolen data, 96GB in size, was collected by infostealer malware and left in an unsecured, publicly accessible database, posing serious risks of credential stuffing and identity theft.

IMPACT

- Account takeovers (email, social media, streaming, financial services)
- Identity theft
- Credential stuffing attacks, where attackers try leaked passwords on many sites
- Targeted phishing or impersonation campaigns

RECOMMENDATIONS

- Perform a full system scan using a reputable and updated antivirus or anti-malware tool.
- Regularly back up important data to offline storage.
- Change passwords for all primary email accounts.
- Use unique, strong passwords for every service or account.
- Do not reuse passwords across multiple accounts.
- Enable multi-factor authentication (MFA) on email accounts.
- Terminate all active login sessions
- Update operating systems to the latest supported versions.
- Stay alert for phishing emails.
- Consider reinstalling the operating system or restoring the device to factory settings to ensure complete removal.

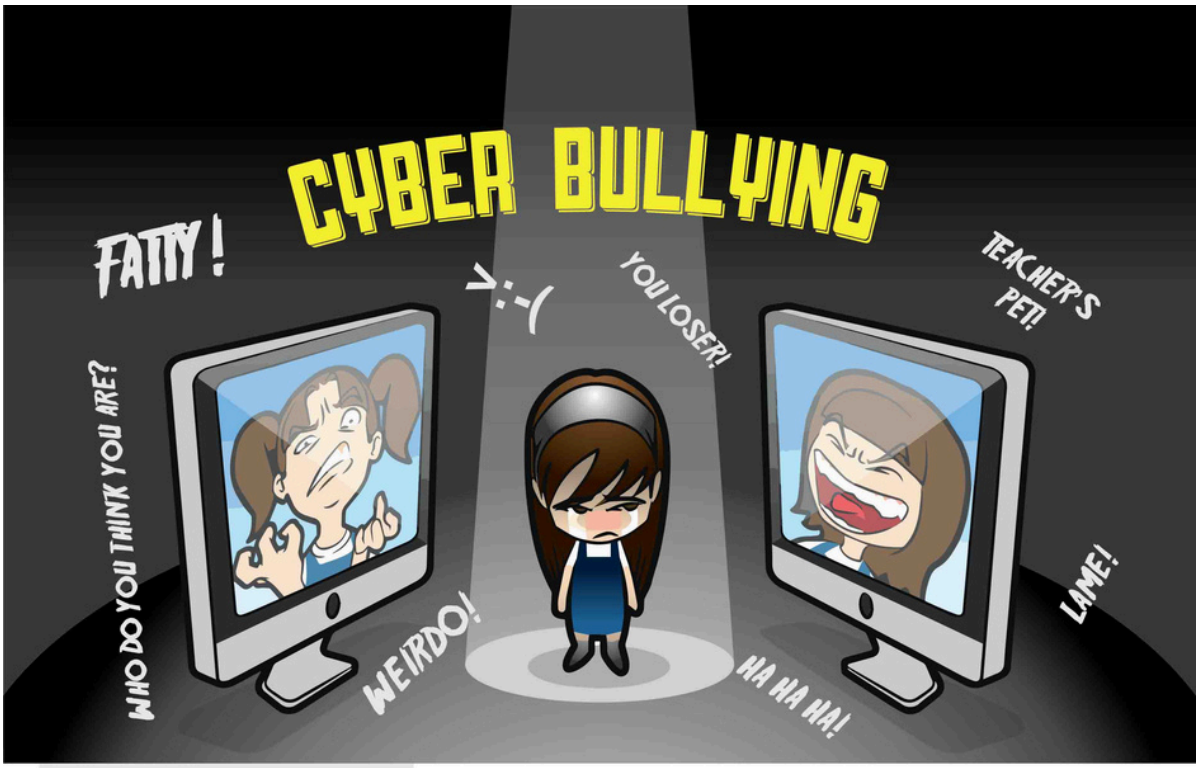
CSB CYBER SECURITY BRUNEI

BRUCERT BRUNEI COMPUTER EMERGENCY RESPONSE TEAM

Report any Cybersecurity Incident here

BRUNEI CYBERSECURITY ASSOCIATION

Be Smart. Be Safe.
Say No to Cyber Bullying



Cyber bullying occurs when the Internet or mobile phones are used to harm other people in a deliberate, repeated, and hostile manner. This includes threatening, intimidating, harassing, or causing embarrassment to the victim. It often occurs in social networks, blogs, through SMS, email or instant messaging. In Brunei, it is common for people to express their anger or frustration through social networking sites such as Facebook, Twitter and MySpace. If these online posts are directed at a specific person, it could lead to cyber bullying.

Most cyber bullies are often motivated by anger, revenge or frustration. Many do it for their own entertainment or to get a reaction.

IF YOU ARE BEING CYBER BULLIED

- Do not react to a bully. It might only motivate them more.
- Do not reply to any messages from a bully.
- If you are being cyber bullied by someone on a social network, you can "Block" or "Unfriend" them.
- If you are being cyber bullied by phone, you could change your phone number.
- Do not delete messages from a bully. They can serve as evidence when you lodge a report about the bullying.
- Report the bullying to your parents or even to the police.
- Many social networking sites allow users to report cyber bullying. For example, you can report bullying on Facebook's Help Center.

BEST PRACTICES

- Be careful what photos and personal information you post on the Internet. Keep in mind that anything you post might be seen by anyone in the world.
- If someone has posted something negative about another person, do not "Like" the post. When you "Like" it, you are supporting the bully's behaviour.
- Do not assume a picture of someone you met online is real. Often, what you see on the Internet or on social networking sites is not true.

An initiative by BRUCERT (Brunei Computer Emergency Response Team)

A team under CSB (Cyber Security Brunei)

Learn more about online safety

SVC secure verify connect

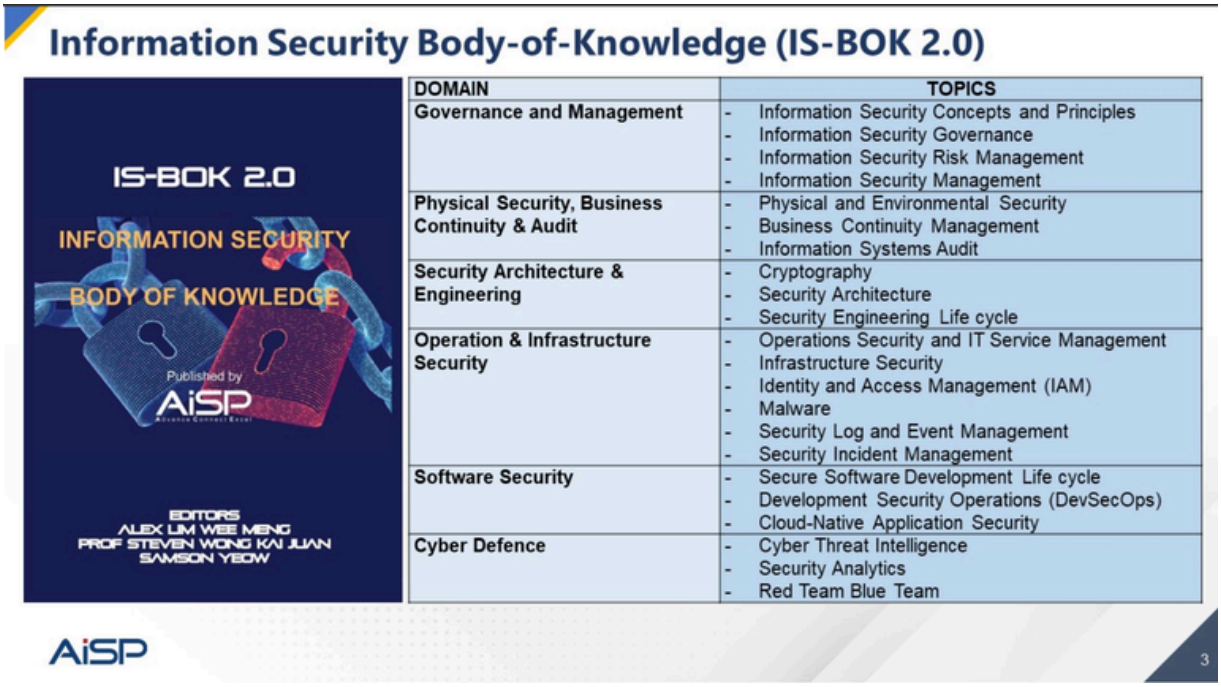
www.SecureVerifyConnect.info

@bruneicert

Report any Cybersecurity Incident here

BRUNEI CYBERSECURITY ASSOCIATION

Preorder IS-BOK 2.0 Information Security Body of Knowledge Published by AiSP



Since 2009, the Association of Information Security Professionals (AiSP) has developed the Information Security Body of Knowledge (IS BOK) to support professionals in building and updating their expertise. The latest BOK 2.0 aligns with Brunei's cybersecurity landscape, referencing the Skills Framework for Infocomm Technology. Continuously evolving, it prepares professionals for industry applications and is covered in the NICF – AiSP Qualified Information Security Professional (QISP®) Course.

For more information, click here

BRUNEI CYBERSECURITY ASSOCIATION

Nitro Security T-Shirt Order

Click here or scan the QR Code to order

BRUNEI CYBERSECURITY ASSOCIATION

Preorder Brunei Cybersecurity Association Polo-Shirt

Type	Sizes	Price (BND)
Short Sleeve	XS - 2XL	$20
	3XL	$21
	4XL	$22
Long Sleeve	XS - 2XL	$22
	3XL	$23
	4XL	$24

Preorder here

www.bcsa.bn contact@bcsa.bn @bcsa.bn +673 8382272

BRUNEI CYBERSECURITY ASSOCIATION

Join Our Membership!

PROFESSIONAL / FELLOWSHIP: BND45

BENEFITS

- Exclusive access to resources, events, and recognition
- Mentorship and leadership opportunities
- Get discounts on training programs
- Advance your career with our high-level network

REQUIREMENTS

- **EXPERIENCE:** Minimum three (3) years of experience in relevant fields with a recognized degree OR five (5) years of experience with a non-related degree or no degree.
- **CV SUBMISSION:** Required.
- **PROFESSIONAL INVOLVEMENT:** Demonstrates significant engagement in information security or related areas.
- **COMMITTMENT:** Must adhere to a code of conduct and actively participating in BCSA activities.

ORDINARY: BND30

BENEFITS

- Access to a wealth of resources and professional development opportunities
- Discounts on training and certifications
- Be represented in industry and government forums

REQUIREMENTS

- **EXPERIENCE:** Minimum one (1) year of experience in relevant fields with a recognized degree OR three (3) years of experience with a non-related degree or no degree.
- **CV SUBMISSION:** Required.
- **COMMITTMENT:** Must adhere to a code of conduct and actively participating in BCSA activities.

AFFILIATE: BND20

BENEFITS

- Connect with industry professionals and explore partnerships
- Get discounts on training programs
- Your voice in the cybersecurity landscape

REQUIREMENTS

- **INTERESTS:** Open to individuals who are passionate about cybersecurity, regardless of their formal background in the field.
- **COMMITTMENT:** Encouraged to engage in BCSA events and activities to deepen their knowledge and involvement.

STUDENT: BND15

BENEFITS

- Access to essential resources and networking events
- Exclusive discounts on training and certifications
- Get discounts on training programs
- Mentorship and career development opportunities

REQUIREMENTS

- **ELIGIBILITY:** Open to any students currently enrolled in an educational institution with a valid student status.
- **COMMITTMENT:** Encouraged to engage in BCSA events and activities to deepen their knowledge and involvement.

Register your interest here!