

HAPPENING IN MAY:

- The Third ASEAN Cyber Shield (ACS) Hacking Contest
- Brunei Cyber Security Association Executive Committee 26th Meeting
- Overseas Learning Journey to Kuala Lumpur
- Cyber Awareness Programme at Cahaya Bina Islam School
- cyber673 Session #7
- Brunei Global Ace - Board of Governance Meeting
- Cyber Security Essentials Training
- AJCCA Board meeting, Philippines (Cebu)
- CISO Lounge
- Offensive Security 673: Everything You Need to Know in 3 Minutes

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!



www.bcsa.bn



pksbrunei@gmail.com



[@bcsa.bn](https://www.bcsa.bn)

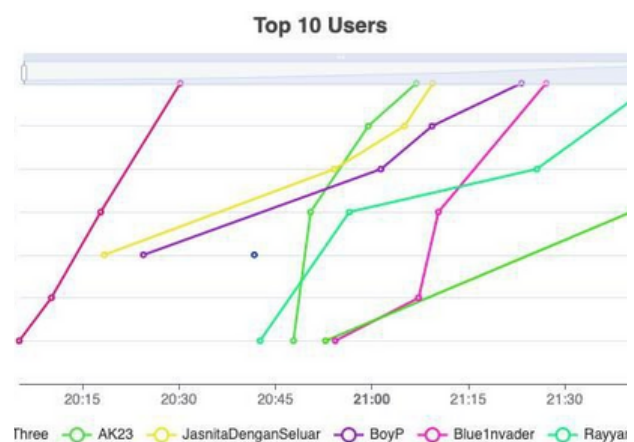


+673 8382272

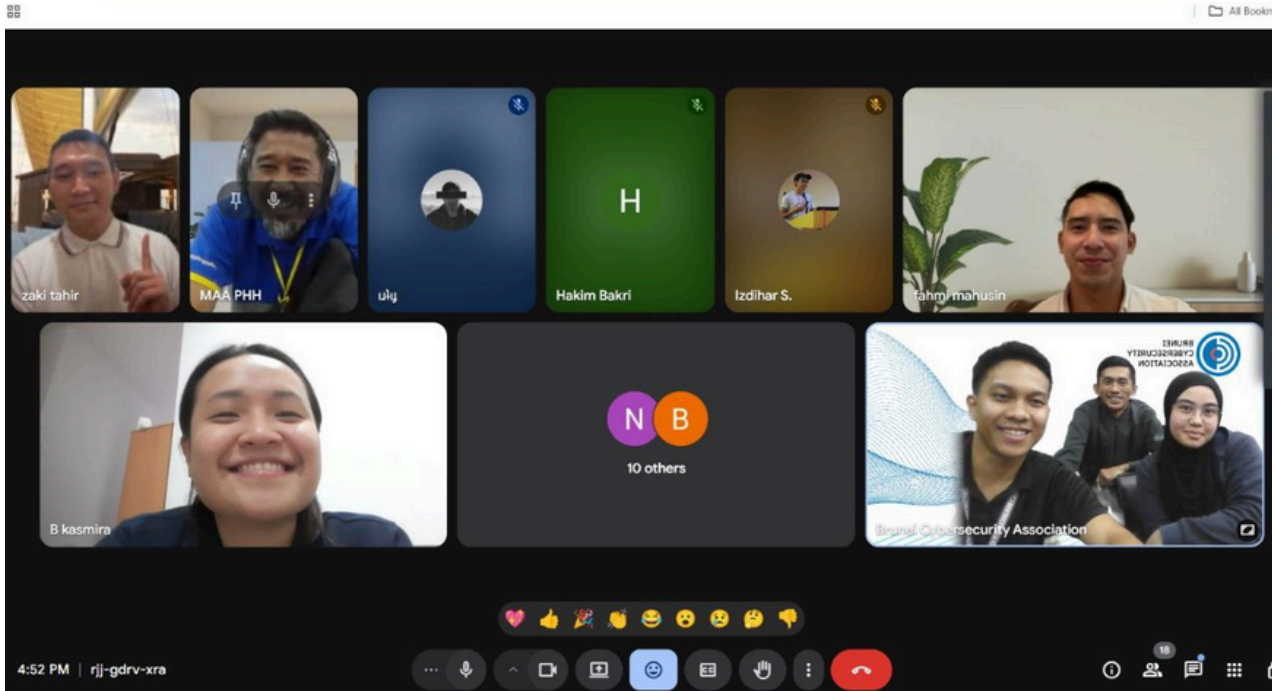
The Third ASEAN Cyber Shield (ACS) Hacking Contest

Place	User	Score
1	UserOne2Three	700
2	AK23	700
3	JasnitaDenganSeluar	700
4	BoyP	700
5	Blue1nvader	700
6	Rayyan	700
7	daniel.az	400
8	nsrisan	300

cyber673 held a mini-CTF for the selection of ACS Student Division. The CTF had 3 web based questions and goes from easy to hard. A total of 8 out of the 14 registered students participated in the CTF. The top from the CTF was later appointed as team leads for the 2 teams going to ACS CTF in November.



Brunei Cyber Security Association Executive Committee 26th Meeting



The BCSA Executive Committee convened its 26th meeting on **Friday, 16th May 2025, from 3:00 PM to 4:50 PM** via an online platform. The session gathered key members to align on ongoing plans and future initiatives.

Discussions focused on preparations for the upcoming CySec 2025 conference, including event logistics and pending administrative matters. The committee also confirmed that the Cyber Security Awards will be held during the CySec Appreciation Night.

Further agenda items included updates on membership, complete planning for the 2025 Overseas Learning Journey (OLJ), and preparations for the ASEAN Cyber Shield (ACS) Hacking Contest. In addition, members reviewed internal matters such as banking arrangements and the upcoming Board of Governors (BoG) meeting and workshop.

The session reflected the committee's continued commitment to advancing cybersecurity initiatives and community engagement in Brunei.

Overseas Learning Journey to Kuala Lumpur



From **18th to 23rd May 2025**, selected students from Brunei's higher learning institutions took part in the Overseas Learning Journey (OLJ) to Kuala Lumpur, aimed at exposing them to real-world practices in cybersecurity, digital governance, and technology in Southeast Asia.

The program included visits to key agencies and institutions such as Cyber Security Malaysia, NACSA, Group-IB, TM One, and Asia Pacific University, where students engaged in discussions, workshops, and facility tours to learn about national policies, cybersecurity trends, and technological innovation.

Students participated in hands-on activities like Capture-The-Flag (CTF) workshops and observed real-time operations in cybersecurity centres, gaining valuable insights into fraud detection, policy-making, and enterprise tech solutions.

The trip concluded with a visit to the Brunei High Commission in Putrajaya, highlighting the importance of international collaboration. OLJ 2025 successfully blended academic enrichment with practical exposure, contributing to students' personal and professional growth. **Special thanks to our sponsors, EVYD Technology and Nitro Security,** for their generous support in making this experience possible.

Nitro Security T-Shirt Order



Click [here](#) or scan the
QR Code to order

Cyber Awareness Programme at Cahaya Bina Islam School



On 24th May 2025, Sekolah Cahaya Bina Insan successfully hosted a "Cyber Awareness Programme" in collaboration with Anak IT BN and SPI BN, involving around 80 students from Year 1 to Year 6. The event aimed to raise awareness of cyberbullying and promote safe digital practices among young learners. Zulfadly Ismail, leader of Anak IT BN and EXCO member of the Brunei Cybersecurity Association (BCSA), delivered an inspiring talk titled "Say NO to Bully," which addressed both physical and online bullying, urging students to stand up against harmful digital behavior.

Students then engaged in hands-on learning through parallel activities that introduced digital skills in a fun and interactive way. Lower primary students participated in "Code & Go with Beebot," learning basic coding using Beebot robots, while upper primary students explored robotics in the "Power Up and Drive with MicroBit" session. These activities, led by facilitators from SPI BN, complemented the school's ongoing STEM programme. The event received overwhelming positive feedback and showcased the powerful impact of collaborative efforts between educational institutions and cybersecurity advocates in nurturing digitally responsible youth.

cyber673 Session #7

The **cyber673 sessions in May** covered a range of cybersecurity topics, blending theoretical knowledge with practical, hands-on experience.



We started off with a light talk by Fauzan Salleh Rahman Harith and Rabbani A. on Infra Cyberattacks and they shared how utilizing frameworks helps in organizing your defense.

Then, we proceeded with the Table Top Exercise, it was the first time we ever organized one. Quite a change of scenery as we usually run mini-CTFs and when that happens, participants are usually quiet and focused, but in this case, it was like a pasar with all the active discussions. The group was split into 5 with 5 different scenarios.

Since the exercise was only a short 45 minutes, we gave them template slides so that they don't start from scratch. Then at the end of it, each group presented how they would respond to their scenario. It was fun to see the different ideas each group had on how to tackle the scenarios.



The session was also a debut to our first POAP! It's a thing that we managed to bring back from meeting 0x F. at Infosec In the City, SINCON. We'll probably have a web3 session in the future and will work around creating incentives to its use. Cool thing is they have this new feature where you can tag the POAP to the location so people can just scan the location to mint the POAP!

Brunei Global Ace – Board of governance Meeting



Global Ace Certification Malaysia (CSM) conducted a Board of Governance session with the BCSA Executive Committee to initiate the formation of the Global Ace Certification Brunei Chapter. The session began with an opening speech by YM Dato Amir and remarks from the BCSA President. Key discussions included an in-depth overview of roles and responsibilities within the Brunei Chapter, aligned with international standards such as ISO 9001, ISO/IEC 17024, and ISO/IEC 27001. The meeting concluded with a token of appreciation from CSM to BCSA members in recognition of the collaboration.

After the session, BCSA hosted the CSM delegates for lunch at Rumbia, where they enjoyed traditional Bruneian cuisine—an especially memorable experience for first-time visitors. In the afternoon, the delegation visited the Cyber Security Brunei (CSB) office, where they were warmly received by Tuan Shamsul, further strengthening ties between the organizations.

Cyber Security Essentials Training



On 27th May 2025, I conducted a one-day training session for CyberSecurity Malaysia (CSM) trainers at ISB School, attended by 19 participants from the Brunei Cyber Security Association, including members, affiliates, and student members. The workshop, led by Encik Hafiz from CSM, began with an overview of digital security essentials and covered seven topics and one quiz before lunch, as part of CSM's Global ACE Certification program. Participants had the opportunity to network during the lunch break, kindly hosted by Ms. Carol from ISB.

In the afternoon, the session resumed with the remaining topics, followed by a second quiz and an engaging use-case scenario discussion. The day wrapped up with a Hi-Tea session, a Q&A, and a group photo at the ISB Piano Steps. I am thankful for the trust placed in me to lead this session and deeply appreciate the knowledge and experience gained through the workshop.

AJCCA Board Meeting, Philippines (Cebu)



Boracay, Philippines, 27th May 2025. During the AJCCA Board Meeting, BCSA presented several notable initiatives that reflect its growing impact in the cybersecurity landscape. The association now has 199 active members and successfully held its first Annual General Meeting in February 2025. In partnership with AITI, BCSA organized the PDPO Sprint for SMEs to support local businesses in understanding data protection requirements. The “Ladies in Cyber” initiative, held in collaboration with Women in Security and Laksamana College of Business, empowered women in cybersecurity through Capture the Flag (CTF) activities, panel discussions, and tabletop exercises, attracting over 140 participants.

BCSA also conducted an Overseas Learning Journey to Malaysia, providing students and lecturers with valuable industry exposure. It continues to lead nationwide cyber awareness sessions in schools and companies, promoting best practices and distributing antivirus software. The association remains committed to supporting Cyber673, a grassroots initiative focused on building offensive and defensive cybersecurity skills. Looking ahead, BCSA is preparing for the Brunei Cybersecurity Conference 2025 with the theme “Beyond Protection: Empowering a CyberSmart Society,” and has introduced a Corporate Membership Framework to better engage organizations in enhancing Brunei’s cybersecurity ecosystem.

CISO Lounge



Beyond the Noise: Focus on What Matters

In today's hyperactive cybersecurity landscape, organizations face a constant barrage of alerts, threats, and vulnerabilities—often leading to burnout and misjudged priorities. This article calls for a shift in mindset: effective cybersecurity is no longer about reacting to everything, but about filtering the noise and focusing on what truly matters. As Brunei's digital transformation progresses, visibility grows, but discerning real threats from background data requires maturity, context, and discipline.

Cyber-mature organizations exemplify this focus by prioritizing based on business impact, employing structured response systems, and maintaining clarity in decision-making. True strength lies not just in quick reactions, but in resilience—knowing what's critical, securing identities, maintaining asset inventories, and testing recovery plans.

Across sectors, the most successful teams stay composed under pressure, acting with purpose rather than panic. Ultimately, cybersecurity success isn't about doing more – it's about doing what matters, when it matters, with confidence and clarity.

Read full article [here](#)



Offensive Security 673: Everything You Need to Know in 3 minutes



Mike Tyson's quote, "Everybody has a plan until they get punched in the face," reflects how many organizations believe they are secure—until a real cyberattack exposes their weaknesses. Often, plans fall apart in moments of panic and chaos. Offensive security, or ethical hacking, plays a vital role in testing an organization's defenses by simulating real-world attacks to uncover vulnerabilities.

This proactive approach helps reduce cybersecurity risks, improve incident response, boost awareness, and prevent reputational and financial damage. To get started in offensive security, basic knowledge of networking, Linux, and programming is helpful, but more important are curiosity and persistence—essential traits for thinking like a hacker and continuously overcoming obstacles.

Read the full article [here](#)



Upcoming Events in June

AJCCA BOARD MEETING

Date: 13 June 2025

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

27TH BCSA EXECUTIVE COMMITTEE MEETING

Date: 16 June 2025

Monthly Executive Meeting of the Association, scheduled to take place on may 2025. This meeting will bring together the executive committee members to discuss key initiatives, strategic plans, and ongoing projects shaping the future of our association.

CYBERSECURITY AWARENESS TALK

Date: 17 June 2025

An engaging session aimed at empowering SMEs with essential cybersecurity knowledge and practices. This talk will cover key areas such as understanding cyber threats, best practices for cyber hygiene, incident response and recovery, and tools available for SMEs—including complimentary antivirus licenses. Real-world case studies and a Q&A segment will provide valuable insights tailored to your industry.

CYBERSECURITY AWARENESS TALK AND DISTRIBUTION OF ANTI-VIRUS TO COSMOPOLITAN COLLEGE

Date: 18 June 2025

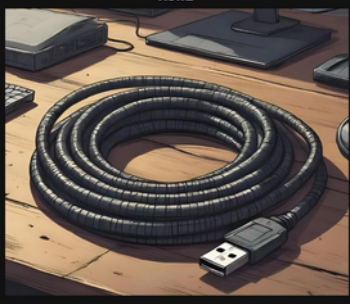
The session introduced BCSA's mission and initiatives, emphasizing the importance of using antivirus software to protect personal and organizational devices from cyber threats. To support this effort, BCSA distributed Trend Micro antivirus license keys to attendees for use on their personal devices. This initiative aims to promote greater cybersecurity awareness and enhance digital protection across the wider community.



Upcoming Events in June

CYBER673

Cyber673 is a group of cybersecurity enthusiasts dedicated to sharing knowledge and enhancing local capabilities in both offensive and defensive cybersecurity.

cyber673 x 	cyber673 x 	cyber673 meetup session
 TALK: PWN	 TALK: DIGITAL FORENSICS	 TALK: HACKING DEVICES
WITH WORKSHOP	WITH WORKSHOP	LIVE DEMO ON WIFI, USBNINJA, FLIPPER & MORE
		
SATURDAY JUNE 21ST @ 2PM BRUNEI INNOVATION LAB, KNOWLEDGE HUB	SATURDAY JUNE 21ST @ 7:30PM BRUNEI INNOVATION LAB, KNOWLEDGE HUB	WEDNESDAY JUNE 25TH @ 7:30PM BRUNEI INNOVATION LAB, KNOWLEDGE HUB
POWERED BY  	POWERED BY  	POWERED BY  
SUPPORTED BY 	SUPPORTED BY 	SUPPORTED BY 

PWN WITH WORKSHOP

Date: 21 June 2025

Time: 2:00PM

Venue: Brunei Innovation Lab, KHUB Building, Anggerek

DIGITAL FORENSICS WITH WORKSHOP

Date: 21 June 2025

Time: 7:30PM

Venue: Brunei Innovation Lab, KHUB Building, Anggerek

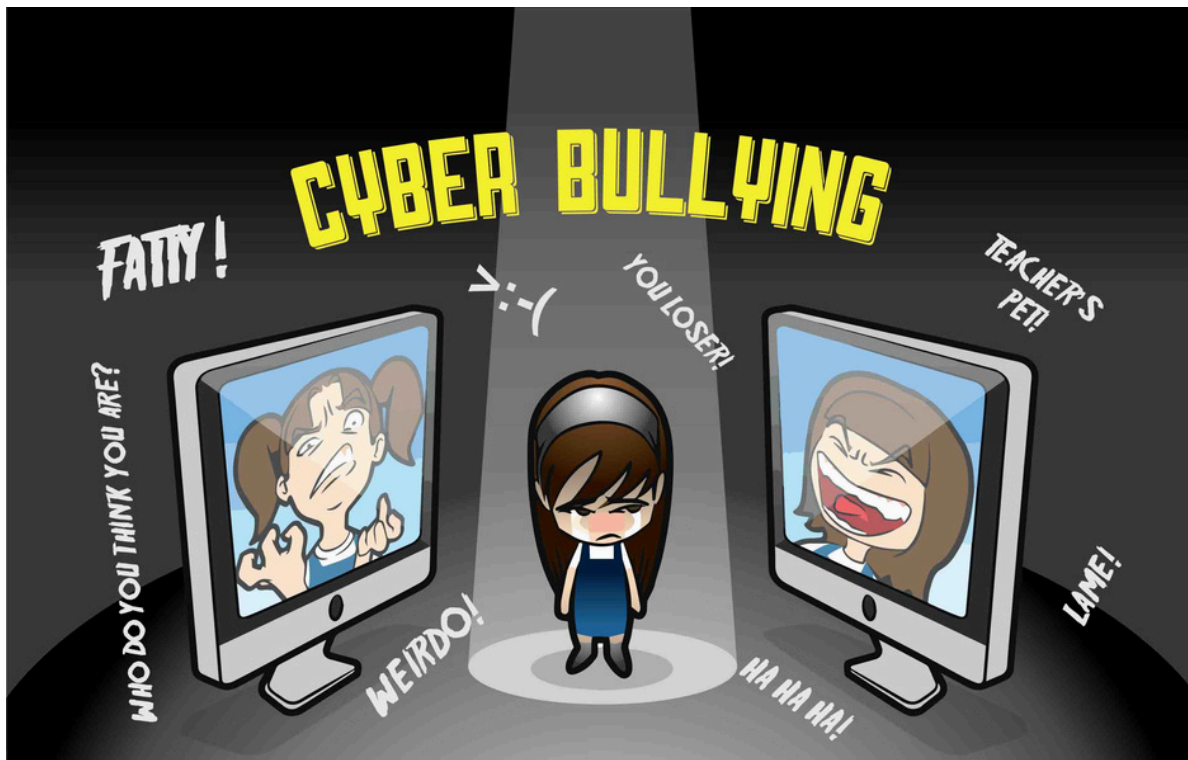
HACKING DEVICES WITH LIVE DEMO

Date: 25 June 2025

Time: 7:30PM

Venue: Brunei Innovation Lab, KHUB Building, Anggerek

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

f i t t
@bruneicert

Report any Cybersecurity Incident [here](#)



www.bcsa.bn



pksbrunei@gmail.com



[@bcsa.bn](https://www.instagram.com/bcsa.bn)



+673 8382272

CERTIFIED INFORMATION SECURITY MANAGER

20th – 24th October 2025

Elevate your career with our CISM preparation seminar! In collaboration with the ISACA Local Chapter, we'll guide you through all four essential domains of the CISM exam. Learn from industry experts and gain the knowledge you need to pass with confidence. Sign up now and become a Certified Information Security Manager!



Special Offer: BCSA members save 15%
Register or join BCSA to get your discount

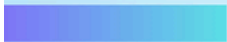


Scan the QR Code to register!

LEVEL UP YOUR IT CAREER WITH SYNERGY SKILLS!

Are you ready to boost your professional skills and get industry-recognized certifications? Join **SYNERGY Skills** for a series of expert-led, hands-on training programs in 2025! Whether you're starting your IT journey or looking to advance to the next level, we've got you covered.

Upcoming Training Programs for 2025:

	COMPTIA A+	<u>16 Jun - 20 Jun</u>
	COMPTIA A+	<u>07 July - 11 July</u>
	COMPTIA NETWORK+	<u>30 Jun - 04 July</u>
	COMPTIA NETWORK+	<u>21 July - 25 July</u>
	COMPTIA SERVER+	<u>28 July - 01 Aug.</u>
	COMPTIA SECURITY+	<u>04 Aug - 08 Aug.</u>
	COMPTIA A+	<u>06 Oct - 10 Oct</u>
	COMPTIA NETWORK+	<u>20 Oct - 24 Oct</u>
	COMPTIA SECURITY+	<u>03 Nov - 07 Nov</u>

Secure your spot early and elevate your skills with one of Southeast Asia's trusted training providers!

Register now : <https://synergyskills.com/>

For inquiries, email: info@synergyskills.com

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

Information Security Body-of-Knowledge (IS-BOK 2.0)

IS-BOK 2.0 INFORMATION SECURITY BODY OF KNOWLEDGE Published by AiSP ASSOCIATION OF INFORMATION SECURITY PROFESSIONALS	DOMAIN	TOPICS
	Governance and Management	- Information Security Concepts and Principles - Information Security Governance - Information Security Risk Management - Information Security Management
	Physical Security, Business Continuity & Audit	- Physical and Environmental Security - Business Continuity Management - Information Systems Audit
	Security Architecture & Engineering	- Cryptography - Security Architecture - Security Engineering Life cycle
	Operation & Infrastructure Security	- Operations Security and IT Service Management - Infrastructure Security - Identity and Access Management (IAM) - Malware - Security Log and Event Management - Security Incident Management
	Software Security	- Secure Software Development Life cycle - Development Security Operations (DevSecOps) - Cloud-Native Application Security
	Cyber Defence	- Cyber Threat Intelligence - Security Analytics - Red Team Blue Team

AiSP

3

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](#)

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](#)

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.
- **COMMITMENT:** 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.
- **COMMITMENT:** 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.
- **COMMITMENT:** 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.
- **COMMITMENT:** Encouraged to engage in BCSA events and activities to deepen their knowledge and involvement.

Register your interest [here!](#)



Membership Benefit for You!

As a **BCSA member**, you are eligible to **claim one (1) license key**, Providing you with a **one-year subscription** to Trend Micro Maximum Security.

How to Claim Your License Key:

1. Create a Trend Micro Account

- Please create a Trend Micro account before proceeding: [Trend Micro Account Setup](#).

2. Fill Out the Claim Form

- After creating your account, click the link below to fill out the required details.

[Claim Your Free Antivirus License from this [Form](#)]

3. Receive Your Activation Key

- Once your details are submitted, we will email you the activation code along with easy-to-follow instructions to activate your antivirus software.

Important Notes:

- Use the same email address in the form as used for your Trend Micro account.
- This license is for personal use and must be activated on your personal devices.
- Activation must be completed by **August 30, 2025**.
- Each key can protect up to three devices, including mobile security for Android and iOS.

For more information, check our website [here](#)

