# Cybersecurity Awareness Month

## 2025

## Think Smart, Act Secure: Cyber Awareness in the Age of Artificial Intelligence

**Sponsored by**

**Our kind sponsor**

# Table of Contents

# 1. Introduction

The National Cybersecurity Week was first observed in 2021 by the Bhutan Computer Incident Response Team (BtCIRT). In 2023 the initiative was expanded into a month-long observance starting to align with global Cybersecurity Awareness Month efforts. The initiative is crucial for fostering a cybersecurity culture among the Bhutanese population, raising awareness of various cyber threats, and strengthening national capabilities to address them effectively.

The theme for the National Cybersecurity Awareness Month of 2025 was "Think Smart, Act Secure: Cyber Awareness in the Age of Intelligence." A number of initiatives were conducted throughout the month including cybersecurity awareness programs for GovTech officials, general public and government executives; a conference, 2 technical workshops and Capture The Flag (CTF) program. The details of the activities and programs are included as a part of this report.

# 2. Events organized

## 2.1 Half-day cyber hygiene Workshop for employees in the GovTech Agency

As part of observance of National Cybersecurity Month, the BtCIRT organized a **Cyber Hygiene Workshop** tailored for the staff of **GovTech**. Since GovTech plays a pivotal role in coordinating and advancing information and communication technology (ICT) initiatives across the country and are in charge of critical systems of the nation, it is imperative that the staff maintain a high level of cybersecurity awareness and practices.

The awareness session was held on 13th October at GovTech's premises, aimed to strengthen the cybersecurity awareness and practices of those managing the country's critical digital infrastructure to protect both institutional and national digital assets.

During the session, BtCIRT presented an overview of the global and national threat landscape. The presentation included analysis of notable cyber incidents from the previous year, focusing on the evolving tactics of threat actors with the rise of the Large Language Model (LLM) and Artificial Intelligence (AI). Participants were also introduced to malware trends and statistics, helping them understand how common malicious software has become.

In addition, the session emphasized a set of core cyber hygiene practices that individuals and GovTech as a whole should adopt to minimize cyber attack risks. Topics included secure password management, system updates, phishing awareness, data backup, safe internet usage and the importance of multi-factor authentication (MFA).

## 2.2 Technical workshop on digital forensics and network analysis

In collaboration with the Czech Republic, NUKIB conducted a three-day workshop on "Digital forensics and Network analysis" from 14th - 16th October 2025 in the GovTech premises. Around 35 participants took part from different agencies around Thimphu.

### 2.2.1 The outcome of the workshop

By attending the workshop, participants gained practical knowledge and hands-on experience in digital forensics and incident analysis. They learned key methodologies and explored real-world case studies presented by experts from two leading Czech institutions—NUKIB and the National Counterterrorism, Extremism, and Cybercrime Agency (NCTEKK). Through expert presentations, group discussions, and practical demonstrations, participants enhanced their understanding of current challenges, shared best practices, and strengthened their ability to respond to cybersecurity incidents encountered by national cybersecurity teams.

## 2.3 Cyber Hygiene Open Awareness Program

Among the programs laid out throughout the month, considering the recent observation of many people falling victim to OTP sharing and losing money through scams, an Open Awareness Program on cybersecurity hygiene was conducted in Thimphu. The program also focused on Safe Mobile and Social Media Use, Password and Authentication Hygiene, Digital Payments and Banking Security, Workplace Cyber Hygiene and Cyber Reporting.

### 2.3.1 Event Details

The program was conducted on the 17th of October in three locations - Kaja Throm, Bank of Bhutan (BOB)and Tashi Bank (TBank). Location approvals were sought from the Thimphu Thromde (for Kaja Throm) and the management of the respective banks to conduct the program from 09:00AM - 04:30PM.

Upon BtCIRT's request, the De-suung Headquarters deployed 10 De-suups to conduct the awareness program. A survey form was developed using Google Forms to assess the cybersecurity practices and hygiene of the respondents. 10 tablet devices were arranged from the National Statistical Bureau to conduct the survey, so that personal devices of the De-suups and participants were not used, thereby ensuring data privacy and security.

The first 100 participants with TashiCell number were provided with a Nu. 199/- data package through the sponsor sponsored by TashiCell private limited of Nu.19,900.

The De-suups attended a half-day training session on the 16th of October in GovTech. The training was conducted with the objective of equipping them with the necessary skills and knowledge to independently deliver the awareness program the following day.

The following topics were covered in the training:

- BtCIRT - Roles and procedures for reporting
- Safe Mobile and Social Media Use
- Password and Authentication Hygiene
- Digital Payments and Banking Security
- Workplace Cyber Hygiene
- Incident Reporting mechanism

### 2.3.2 Survey Results

A total of 253 responses were collected through the survey revealing a male-to-female ratio of 122:131. The chart below illustrates the distribution of occupations among the respondents.

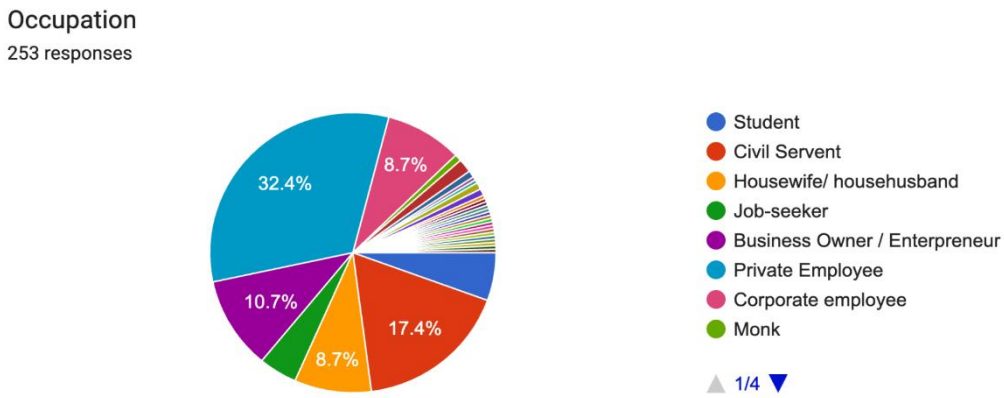


*Figure 1. Occupation of the respondents*

Overall, the survey indicates that the public is generally aware of good cybersecurity practices. Notably, 79.8% of respondents are aware of online frauds like scams and phishing while performing online banking or transactions.

77.5% users have enabled two-factor authentication on their online accounts and 77.9% said that they would change their password immediately and secure their account, if they receive a notification about a suspicious login or breach.

Positively, 84.2% of respondents responded that if they receive any calls or messages asking for the OTP or payment code, they will not share it. In addition to that, 69.9% responded that if they encounter any cyber related issues, they will report it to IT or the relevant authority immediately.

Furthermore, it is worth noting that approximately 71.3% of respondents are aware of the proper channels or authorities for reporting cyber incidents in their organization or country.


*Figure 2: Open awareness for public*

## 2.4 Cyber conference on 24th October 2025

The Bhutan Cybersecurity Conference 2025 was a successful hybrid event held in October 2025 in Thimphu. It brought together local and international cybersecurity experts, practitioners, and attendees to share knowledge and promote collaboration with the main objective is to enhance cybersecurity awareness, facilitate knowledge exchange, and strengthen partnerships in Bhutan. The main sponsor for the event was the Royal Monetary Authority, with the Bhutan NDI sponsoring the gifts - a token of appreciation for the speakers.

### 2.4.1 Event Details

*Figure 3: Participants at the Cybersecurity Conference*

### 2.4.2 Outcomes and Impact

The event featured 13 speakers (including 5 international experts) and attracted over 60 attendees from public and private sectors, both in-person and online. The event successfully disseminated actionable knowledge, fostering networking between local and global experts, and helping strengthen Bhutan's cybersecurity community.

The conference covered a wide range of critical cybersecurity topics through speaker sessions, including:

- Cybersecurity as a **national priority**.
- Real-life cyber threats and securing national systems.
- **Zero Trust Architecture**, proactive vulnerability management, and cost-effective Security Operations Centers (SOCs).
- Protecting **critical infrastructure** and simplifying Governance, Risk, and Compliance (GRC).

- The importance of **collaboration** among defenders.

### 2.4.2 Speaker Sessions & Key Takeaways

Dasho Secretary (GovTech Agency): Emphasized the importance of cybersecurity as a national priority and the role of Cybersecurity Month in safeguarding citizens. Welcomed all speakers and thanked for the effort taken in promoting Cybersecurity.

**Speaker 1**

Adli, International Expert, APNIC, Asia Pacific Network Information Centre, Malaysia

Topic: Culture, Community and Collaboration: A Path to Cyber Resilience

Adli shared case studies on cyber resilience initiatives, including the Tonga Women ICT Bootcamp, Phoenix Summit, and FS-ISAC collaboration.

**Speaker 2**

Mr. Tshering Dorji, Dy. Chief ICT Officer, Cybersecurity, GovTech:

Topic: National Cybersecurity Strategy and BtCIRT's plan

Tshering Dorji discussed real-life cyber threats and outlined BtCIRT Background, National Cybersecurity Strategy, Four Strategic Goals and action plan, Cybersecurity maturity model (CMM) and Global Cybersecurity Index (GCI)

**Speaker 3**

Mr. Tshewang Chojay, Dy. Chief ICT Officer, WoG, GovTech Agency

Topic: Securing Authentication Across Government Systems Using Bhutan NDI Wallet

Mr Chojay highlighted on the NDI - The Challenges of Authentication, the current online issues, The Bhutan NDI Wallet, The NDI Trust Architecture, Integrations Across Government Systems and Why we need to integrate with NDI.

**Speaker 4**

Mr. Ngawang Tashi Dorji, Dy. Chief ICT Officer, Cybersecurity, GovTech

Topic: Vulnerability Management: Protecting Your Organization from Threats

Ngawang stressed the importance of proactive vulnerability management in mitigating risks, CVEs, Vulnerability information, remediation and challenges.

**Speaker 5**

Darren Arnott, Cybersecurity professional, Australia (Online via Zoom), Australia

Topic: L'affaire du télégraphe. The Bordeaux hackers of 1834

Explored early wireless data transmission methods and monetization of cyber threats, drawing parallels to modern challenges.

**Speaker 6**

Imtiaz Rahman, Cyber security specialist, APNIC Community Trainer, Bangladesh

Topic: Building a cost-effective SOC- with open-source tools

Imtiaz advocated for building efficient Security Operations Centers (SOCs) using tools like Shodan and emphasized the "secure more, spend less" approach.

**Speaker 7**

Manoj Adhikari, NUK 9 Private Limited, Thimphu

Topic: Zero Trust Architecture

Manoj presented case studies on Zero Trust Defense, including the Makop ransomware attack, and highlighted the principle of "Never trust, always verify."

**Speaker 8**

Ollie Kwan, CEO, Gathid, (Online via Zoom)

Topic: OT Security & Identity Governance.:

Ollie addressed operational technology (OT) security, emphasizing the need for better visibility and audit controls.

**Speaker 9**

Prashant Singh, Director, ISACA, WA Chapter, Australia. (Online via Zoom)

Topic: Beyond Firewalls: Navigating Cyber Threats with AI, Zero Trust, and Future-Ready Strategies

Discussed AI-driven threat navigation, Zero Trust strategies, and the challenges of IoT and data governance.

**Speaker 10**

Sumdho Tshering & Jigme Sherab, Engineer - BPCL, Smart Grid Section

Topic: Securing Critical Communication Networks in Smart Power Grid

They highlighted cybersecurity measures for critical infrastructure, defensive models for power grid including lessons from the Ukraine Power Grid failure.

**Speaker 11**

Deepesh Chitroda, Founder Director, Cybersecurity Professional, India

Topic: Making GRC Simple

Mr Chitroda highlighted the importance of Governance, Risk, and Compliance (GRC). GRC is like a "Google Maps" for organizations and debunked myths around modern GRC.

**Speaker 12**

Pratima Pradhan, Dy. Chief ICT Officer, Cybersecurity, GovTech

Topic: Defenders must Collaborate: Not compete

She urged defenders to collaborate rather than compete, emphasizing the role of local firms and knowledge-sharing.

## 2.5 Capture the Flag challenge

The BtCIRT collaborated with Gyalpozhing College of Information Technology (GCIT) and Jigme Namgyel Engineering College (JNEC) to host the CTF competition at GCIT. The Capture The Flag (CTF) competition was organized to promote cybersecurity knowledge across the country. The event offered practical, hands-on challenges in web security, cryptography, digital forensics, and network analysis, helping participants experience real-world cyberattack and defense scenarios.

Students from GCIT, JNEC, and the College of Science and Technology (CST), along with professionals from government and private sectors, took part, creating strong opportunities for knowledge sharing, mentorship, and networking. With two tracks covering multiple challenge categories, the event was dynamic, inclusive, and aligned with BtCIRT's goal of nurturing young talent and strengthening Bhutan's cybersecurity culture. Such initiatives play a vital role in building a resilient digital ecosystem and supporting Bhutan's long-term technological growth.


*Figure 4. Participants at capture the flag challenge*

### 2.5.1 Event Details

The Cybersecurity CTF event, held from October 24–25, 2025, featured five speakers and began with a full-day hands-on workshop that introduced participants to essential cybersecurity concepts, practical tools, exploitation demonstrations, and a CTF orientation.

Day One started with registration at 9:00 AM and the official program at 9:45 AM, bringing together students and professionals from various colleges and domains. The sessions covered Child Online Protection initiative, Cybersecurity Awareness, CTF-related tools, exploitation demonstrations, and an overview of CTF rules and scoring. The day concluded with a walkthrough of the CTF platform interface and guidance on setting up labs and tools, ensuring participants were fully prepared for the Day Two competition.





*Figure 5. Presenter at capture the flag challenge*

Day Two of the event began at 9:00 AM with participants organized into shuffled groups for the Capture the Flag (CTF) competition, conducted across two tracks: Track One for college students with 65 challenges across six categories, and Track Two for final-year students and industry professionals with 50 challenges in six categories. The six-hour competition allowed participants to take tea and lunch breaks at their convenience. The event concluded with an award ceremony led by the President of Gyalpozhing College of Information Technology (GCIT), Ms. Audrey Low, where winners from both tracks received certificates and prizes. Prizes for the CTF winner were sponsored by two companies : GIC-Bhutan Reinsurance Ltd and Thimphu Tech Park Limited (TTPL). Closing remarks from the organizers highlighted the participants' enthusiasm, teamwork, and active engagement, reflecting a successful program that fostered collaboration, learning, and healthy competition.

*Figure 6. Winners of capture the flag challenge*

### 2.5.2 Feed back from participants

The participants shared very positive feedback about the event. They expressed that they thoroughly enjoyed the program and were eager to participate in similar events in the coming years. Many noted that they gained valuable knowledge and hands-on experience, which helped them understand what real cyber threats feel like. Participants also appreciated the opportunity to network and make new friends within the cybersecurity community. Finally, they extended their gratitude to the organizing team for successfully conducting a well-structured and engaging two-day event.

## 2.6 Cyber Threat Management and monitoring Workshop

*Figure 7. Participants at technical workshop*

A four-day workshop on Cyber Threat Management and Monitoring was successfully conducted with the participation of over 50 professionals from various sectors. The participants represented ICT and cybersecurity Professionals from GovTech divisions, other government agencies,, financial institutions, telecommunications companies, regulatory bodies, Royal Bhutan Army, and academic institutions.

### 2.6.1 Event Details

During the first two days, participants received in-depth training on key areas of cyber threat identification, vulnerability assessment, and risk management. The sessions also covered global cybersecurity frameworks, policies, and best practices, aimed at strengthening participants' understanding of contemporary cyber governance and risk mitigation strategies.

The final two days of the workshop focused on hands-on practical exercises designed to enhance participants' technical proficiency in security monitoring and incident response. Practical sessions featured the deployment and use of several open-source security tools, including Wazuh, Suricata, Pi-hole, OpenVAS, Wireshark, Honeypot, and IRIS Case Management. Through these activities, participants gained valuable experience in real-time threat detection, network traffic analysis, vulnerability scanning, and case management for incident response.

Overall, the workshop provided a comprehensive blend of theoretical and practical learning, equipping participants with the knowledge and skills required to effectively manage and respond to evolving cyber threats in their respective organizations.

## 2.7 Self-pace study - Cybersecurity

The cyber-hygiene refresher course was developed as a self-paced online training delivered through Google Forms, allowing staff to complete it at their convenience without requiring additional logins or technical setup. The course focused on essential daily cybersecurity practices, including strong password management, safe browsing, social engineering awareness, and phishing defense. Each topic was designed with practical examples, scenario-based learning, and multiple-choice assessments to ensure relevance and engagement for all participants, particularly IT personnel.

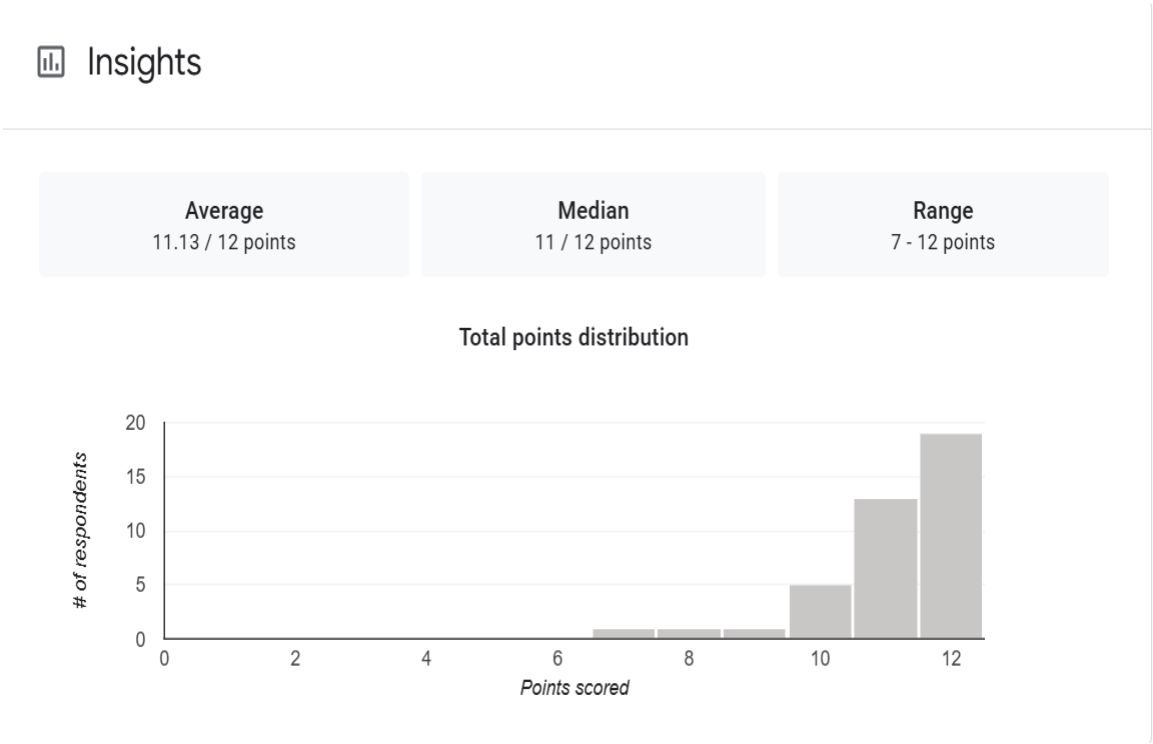


*Figure 8. Score Vs respondents*

The course was launched on 20 October 2025 with a one-week completion window, giving participants until 27 October 2025 to finish. A total of 40 staff participated in the training. The highest score achieved was 12/12, while the average score was 11.13, reflecting a strong understanding of the material across participants. These results indicate that the course effectively reinforced core cyber-hygiene practices and that most staff are aware of and able to apply security measures in their daily workflows. The data collected through Google Forms will also serve as a baseline to guide future training initiatives, highlighting areas that may require additional focus or deeper engagement.

Overall, the refresher course emphasized that cybersecurity is a shared responsibility, and even small daily actions can significantly strengthen the organization's security posture. By combining awareness, practical guidance, and interactive learning, the training successfully promoted disciplined habits that contribute to a safer digital environment for both personal and organizational assets. The course will continue to support ongoing efforts to maintain high cybersecurity standards and prepare staff to respond effectively to evolving threats.

## 2.8 Cybersecurity awareness program and quiz for executives and Phishing simulation

First, we conducted a phishing simulation on October 22, 2025 at around 4:30 pm. The phishing simulation email was sent to 54 participants mainly targeting the executives, Dasho Secretaries and Directors of the various Ministries and Agencies upon the approval received from the GovTech Secretary. Of those, 2 participants opened the email and 1 clicked on the malicious link. The phishing email was themed around cryptocurrency investment, claiming that the recipient had won a Bitcoin and urging them to click on a malicious link to claim the reward. The overall engagement was low, likely because many participants were occupied with their schedules and also did not show interest in cryptocurrency-related content, which reduced the likelihood of them opening such emails.

The following week, an awareness program and quiz were developed in Google Forms and circulated to 54 executives in the government. The quiz aimed to enhance understanding of cyber threats and emphasized phishing, along with techniques to identify phishing emails. The quiz covered the following key sections:

- Phishing
- Password Management
- Device Security
- Emerging Threats

Overall, the participants performed well in all sections; however, there were instances where they submitted incomplete responses, particularly in questions that allowed for multiple correct answers. It will be a lesson for us to refine the quiz design in future iterations, ensuring that participants are fully aware of how to approach questions with multiple correct responses.

The program ran over 7 days, during which 9 executives completed the program. It remains open for other executives to participate at their convenience whenever they can manage their time.

## 3 Conclusion

Cyber Awareness Month has strengthened our collective understanding of online safety and the need for proactive cybersecurity practices. The training and initiatives carried out have helped reinforce the importance of staying vigilant in today's digital environment.

We extend our sincere thanks to all sponsors and partners for their invaluable support, which made these activities possible. As cyber threats continue to evolve, it is important that we carry forward the lessons learned and continue working together to build a safer and more resilient digital ecosystem.

# 4 Annexure: List of expenditure and sponsor

| Sl.No. | Events / Activities | Amount (in Nu.) | Sponsored by |
|---|---|---|---|
| 1 | Public Awareness - data recharge to public | 19900 | TashiCell |
| 2 | Cybersecurity self pace study and quiz competition | 22200 | Bank of Bhutan |
| 3 | Gift hamper for conference speaker | 29000 | Bhutan NDI |
| 4 | Conference Lunch and refreshment | 93499.20 | Royal Monetary Authority (RMA) |
| 5 | Prizes for Capture the flag (CTF) winners (Beginner) | 20000 | Thimphu Tech Park Ltd (TTPL) |
| 6 | Prizes for Capture the flag (CTF) winners (Professionals) | 20000 | GIC-ReInsurance Bhutan Ltd |
| 7 | Printing of cybersecurity -pamphlet/ banner / standee | 15000 | National Pension Provident Fund (NPPF) |
| 8 | Resource person for Cyber Threat Management and monitoring workshop | | Asia Pacific Network Information Center (APNIC) |
| 9 | Resource persons for Digital Forensics and network analysis | | Czech Republic embassy and NUKIB |
| 10 | Two Workshops Lunch and refreshment | 1,39,755 | RGOB |
| 11 | Visa processing fees for 4 Czech experts | 20000 | RGOB |
| | **Total Expenditure** | **3,79,354.2** | **Sponsors and RGOB** |