འབྲུག་གཞུང་འཕྲུལ་རིག་ལས་སྡེ།

Government Technology (GovTech) Agency
Royal Government of Bhutan

A technologically advanced nation, with empowered citizens, and a thriving digital economy

GovTech(AS)-25/2023-2024 / 2189 23rd Nov 2023

NOTIFICATION: CYBERSECURITY ADVISORY-ENHANCE VIGILANCE DURING UPCOMING ELECTIONS

As we approach the upcoming elections, it is paramount to prioritize cybersecurity measures to safeguard our systems and websites against potential threats. Cyber adversaries often target critical infrastructure during high-profile events, and election periods are no exception.

Key Points to Consider:

1.Deepfake Threats: With the advancements in technology, deepfake videos and audio recordings pose a significant threat during elections. Deepfakes involve the manipulation of media content to create realistic but entirely fabricated materials. These could be used to spread false information, mislead voters, or damage the reputation of candidates.

2.Phishing Attacks: Be cautious of phishing emails and messages that may attempt to deceive you into disclosing sensitive information. Verify the authenticity of unexpected communications and avoid clicking on suspicious links or downloading attachments.

3.Update Software: Ensure that all software, including operating systems, antivirus programs, and content management systems, is up-to-date with the latest security patches. Regular updates help protect against known vulnerabilities.

4.Multi-Factor Authentication (MFA): Implement MFA wherever possible to add an extra layer of security to your accounts. This helps mitigate the risk of unauthorized access, even if login credentials are compromised.

5.Network Security Audit: Conduct a thorough audit of your network security to identify and address any vulnerabilities. Regularly monitor network traffic for unusual patterns and unauthorized access.

6.Employee Access Control: Review and update employee access privileges. Limit access to only those who require it for their specific roles. Regularly revoke access for employees who no longer need it.

7.Regular Backups: Ensure that critical data is regularly backed up, and test the restoration process. In the event of a ransomware attack or data loss, having reliable backups is crucial for recovery.

Your proactive efforts in reinforcing cybersecurity measures will contribute to the overall resilience of our systems and protect the integrity of the upcoming elections. Thank you for your diligence in this critical matter.

If you have any concerns or require further assistance, please do not hesitate to contact

Phone: +975-02-338606

Email: info@btcirt.bt (for general questions)

Email: cirt@btcirt.bt (for reporting incidents)

(Jigme Tenzing)
Acting Secretary

ACTING SECRETARY
Government Technology Agency
Thimphu Bhutan

འབྲུག་གཞུང་འབྲེལ་རིག་ལས་སྡེ།
GovTech
Bhutan
Government Technology Agency

Cc:

1. All Ministries & Agencies ICT focal.
2. Officiating Director, DDI & DDT ,GovTech Agency.
3. Head,Cybersecurity Division,GovTech Agency for na.