Advisory: Banking Fraud via. Email Compromise

BtCIRT has been reported of multiple incidents involving the compromise of Gmail accounts that are linked to bank accounts of customers in Bhutan. In these incidents, unauthorized access to the Gmail accounts was subsequently used to compromise the associated bank accounts, resulting in unauthorized transactions and financial losses.

Such incidents have been observed among customers of multiple banks, thus all bank customers are advised to remain vigilant, as similar attacks could potentially affect accounts across any financial institution.

Immediate Actions for Affected or Suspected Users

Account holders who suspect that their Gmail or bank account may have been compromised are advised to take the following steps immediately:

1. Recover and Secure the Gmail Account

- Visit Google Account Recovery at https://accounts.google.com/recovery and follow the recovery process.
- Reset the Gmail password immediately using a strong, unique password not used elsewhere.
- Review account activity and security alerts in the Google Account "Security" section.
- Check and remove any unknown recovery email addresses, phone numbers, or third-party app access.
- Enable **Two-Step Verification** using an authenticator app or google prompts. Visit Google Help at https://support.google.com/ and look up Turn on 2-Step Verification.

2. Inform the relevant entities Immediately

- Review recent transactions and formally report any unauthorized activities to the respective bank's customer support or visit the nearest branch and report to police if fraudulent transactions have occurred without delay.
- Request temporary blocking of online banking, cards, and digital channels if suspicious activity is detected.
-

Proactive Security Measures to Prevent Similar Incidents

BtCIRT strongly advises all bank customers to adopt the following preventive measures:

- Use a **dedicated email account** exclusively for banking and financial services.
- Enable **Two-Factor / Two-Step Authentication** on both email and bank accounts.
- Avoid clicking on suspicious links or opening attachments received via email, SMS, or social media.

- Regularly review account login activity and security notifications.
- Do not share One-Time Passwords (OTPs), passwords, or verification codes with anyone under any circumstances.
- Keep devices updated with the latest security patches and use reputable antivirus software.
- Ensure recovery email addresses and phone numbers are secure and accessible only to the account owner.
- Avoid carrying out banking transactions over public or unsecured Wi-Fi for security reasons.

Reporting

Any such suspected incidents or attempted compromises should be promptly reported to:

- **The concerned bank and the Royal Bhutan Police(RBP)** for immediate intervention and investigation; and
- **Bhutan Computer Incident Response Team (BtCIRT)** for information sharing, technical support, and broader public awareness.