

Department of Supervision

Cyber Security and Information Technology Examination (CSITE)

"Cybersecurity Awareness Month – October 2024: Second Fortnightly Email Bulletin"

Cyber Security: Cultivating a Culture of Safety

As we continue our focus on cyber security, it's vital to recognize that securing our digital environments is an ongoing commitment. Just as we remain vigilant in our personal safety, we must apply the same diligence to our online interactions. In this bulletin, we present **eight essential cyber security habits** to reinforce our collective security efforts



CYBER SECURITY

ESSENTIAL HABITS

CONTROL ACCESS



Ensure that you use your secure access credentials to enter the premises and do not share them with others.

EMAIL SAFETY/SECURE BROWSING



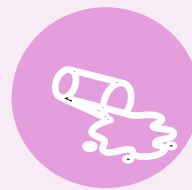
Avoid unknown links or attachments. Verify the sender before sharing information. Always use HTTPS for secure browsing.

PROTECT DATA



Always use encryption and strong passwords to safeguard sensitive information and prevent data breaches.

INCIDENT REPORTING



Report suspicious activity or breaches to your Bank/IT department immediately. Early reporting prevents damage and speeds up response.

SECURE DEVICES



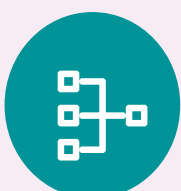
Keep your devices secure by locking them when not in use and using approved security software.

SOCIAL ENGINEERING VIGILANCE



Stay cautious of tricks like impersonation aimed at stealing information. Always verify requests for confidential details.

NETWORK SECURITY



Connect to secure networks when accessing confidential systems. Use VPNs for remote work and avoid public Wi-Fi for sensitive activities.

RESOURCES



Participate in regular training sessions on cyber security protocols and learn how to recognize potential threats.