

NATIONAL CYBER SECURITY AWARENESS MONTH - OCTOBER 2021



OCTOBER 2021

CYBER SECURITY AWARENESS MONTH

DO YOUR PART **#BECYBERSMART**

WEB SURFING SECURITY

- Visit only trusted sites and always check for https or the lock sign while browsing any site

- Keep an eye on automatic content download. These can be trojans, viruses

- Verify full URL using mouse hover before clicking any button or shortened link

- Don't browse the internet using system admin credentials

- Never activate save password feature in your browser for official accounts



NATIONAL CYBER SECURITY AWARENESS MONTH - OCTOBER 2021



OCTOBER 2021

CYBER SECURITY AWARENESS MONTH

DO YOUR PART **#BECYBERSMART**

Maintain Social Media Hygiene

THINGS YOU CAN CONTROL IN SETTINGS



NATIONAL CYBER SECURITY AWARENESS MONTH - OCTOBER 2021



OCTOBER 2021

CYBER SECURITY AWARENESS MONTH

DO YOUR PART *#BECYBERSMART*

WORK FROM ANYWHERE
CYBER SECURITY TIPS



KEEP SOFTWARE & BROWSER UPDATED AND VISIT HTTPS WEBSITES ONLY



CREATE SECURE EMAIL & ONLINE ACCOUNTS



CHECK SOCIAL MEDIA PRIVACY SETTINGS FREQUENTLY



CREATE A STRONG PASSWORD & ENABLE WPA2 + AES SECURITY



DO NOT USE UNSECURE OR OPEN WI-FI FOR OFFICIAL COMMUNICATION



OCTOBER 2021

CYBER SECURITY AWARENESS MONTH

DO YOUR PART **#BECYBERSMART**



Portable Media Security



Perform full scan of Hard drives, Pen drives & SD card with an updated antivirus before you open/use them



Avoid sharing official USB drives with other personal computers of family/friends around you



Use additional read/write security controls and enable event logging, if required





OCTOBER 2021

CYBER SECURITY AWARENESS MONTH

DO YOUR PART **#BECYBERSMART**

PASSWORD SAFETY CHAKRA

Do not include
personal details

Change them
periodically

Make them
unique

Never share
with anyone

Avoid saving
passwords in
browsers

Set up Two-Factor
Authentication
(2FA/MFA)



NATIONAL CYBER SECURITY AWARENESS MONTH - OCTOBER 2021



OCTOBER 2021

CYBER SECURITY AWARENESS MONTH

DO YOUR PART **#BECYBERSMART**

BEWARE OF PHISHING AND EMAIL SCAMS

1. Verify before clicking web links received over emails/SMS
2. Do not open suspicious emails claiming to be from known senders
3. Beware of possible malware in email attachments
4. Never share personal or financial information over the Internet

