

Cyber Security Awareness Month (CSAM)

October is globally marked as Cyber Security Awareness Month (CSAM) with a view to educate public and private sector to increase cyber resilience of the nation as recommended by National Security Council Secretariat (NSCS). NHA in its second year, as a continual effort to raise awareness about the importance of cyber security across PM-JAY ecosystem celebrated **Cyber Security Awareness Month (CSAM)**. The theme for occasion was chosen as **“Own IT. Secure IT. Protect IT”**. The entire month of October was marked full of security advisories and quizzes imparting the importance of both information security and data privacy to all PM-JAY personnel.

Goal 1: Ways to protect beneficiary’s data

Beneficiaries’ information is a valuable asset that needs to be secured, while processing/handling information at rest and in transit, and protect it from unauthorized use, disclosure or modification. 5 ways to protect beneficiary’s data was shared all across PM-JAY ecosystem via email.

CYBER SURAKSHA DISHANIRDESH
SECURITY QUICK BYTES

5 WAYS TO PROTECT BENEFICIARY DATA

- 1 Think before you click that link!**
 - What to do:** Don't click links in email from unidentified people. Always confirm the identity of the person.
 - Why:** According to Microsoft, phishing is still the number one favorite method of cyber attacks.
- 2 Be cautiously Social**
 - What to do:** Don't share beneficiary personal and health data over social media platforms and WhatsApp groups.
 - Why:** Beneficiary personal and health data can be used to recover account login. Don't give hackers way into online accounts.
- 3 Practice data purging**
 - What to do:** Make sure to keep data replication to a minimum. Purge or delete all old files containing beneficiary information if not in use.
 - Why:** Replication of beneficiary data leads to higher chances to data leakage.
- 4 Stay Safe from Ransomware**
 - What to do:** Do not click on pop-up ads in unknown websites, do not give everyone full user permissions. Install all security updates for your computer. Keep automatic updates enabled.
 - Why:** Ransomware attack leads to data hijacking and poor performance of the machines
- 5 Patch your devices**
 - What to do:** Keep your computers and mobile data devices patched and up to date.
 - Why:** Software vulnerabilities allow malware to infect your devices, which can steal data & login credentials.

CLEAR DESK & CLEAR SCREEN

Clear Desk

All PM-JAY sensitive information must be removed from the desk and locked in a drawer or filing cabinet. Further filing cabinets containing such information must be locked when not in use or when not attended.

Copies of documents containing classified or PM-JAY sensitive information must be immediately removed from printers.

Classified information must not be left unattended on or around the working area. Further all desks must be cleared at the end of each working day.

Documents or magnetic media, or other removable media such as CDs, DVDs etc. should be safely stored away.

Clear Screen

Locking the screen not only prevents someone else from using the PC, which is logged on in the user's name, but it also prevents someone from reading classified information left open on the screen.

Passwords must not be written down and stored near a computer/laptop or in any other accessible location

Lock workstations (computers, laptops and windows terminals) when unattended by pressing Windows + L. At the end of the working day close down all the applications and log off / shutdown the workstation.

Computers and laptops must not be left logged on when unattended, and must be protected by passwords, screensavers and other security controls that are available.

Goal 2: Clear Desk & Clear Screen Awareness

To help reduce the risk of security breaches within the PM-JAY workplace, clear desk and clear screen awareness was shared all across PM-JAY ecosystem via email. It covered areas like locking of workstations (computers, laptops) when left unattended, removing all PM-JAY sensitive information and keep it locked in a drawer or filing cabinet at the end of work day, etc.

Goal 3: Safe Internet surfing habits

Digital technologies provide us lot of possibilities at our fingertips, but at the same time we must be vary of security risks. It is vital to protect our online activities and be aware of the ways in which technology may compromise PM-JAY security. On '**International Internet Day**' celebrated on **29 October, 2020**, safe Internet surfing habits such as visit only trusted sites, never activate save password feature on browser, etc. was shared with all PM-JAY personnel.



International Internet Day 2020

As we are in the era of Digital World, the internet has become a basic necessity of everyone's life. Digital technologies provide us with a world of possibilities at your fingertips, but at the same time we must be vary of security risks that comes along with it.

It is vital to protect our online activities and understand the ways in which technology may compromise the security of PM-JAY information. Therefore, today, on the occasion of '**International Internet Day**'; here are a few Internet surfing security tips.

Safe Internet surfing habits

- Visit only trusted sites & always check for https or the sign while browsing.
- Keep an eye on automatic content download. These can be trojans and 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.

29 October, 2020 NHA IS team



REMEMBER
Sec" _ "rity is Incomplete
without
"U"

No amount of technical controls can keep NHA 100% safe unless "You" are aware of the information security threats and alert at all times. Cyber attackers understand that the easiest intrusion vector is people. It is imperative to be cyber-aware.

Be Alert | Be Vigilant | Be Careful

Do not forget to report any suspicious activities, to
R.securityincident@nha.gov.in

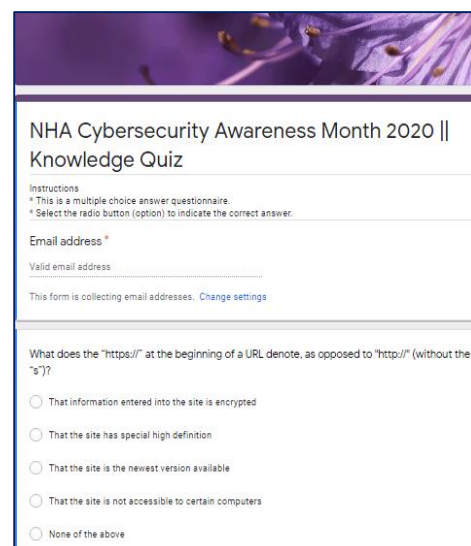
October, 2020 **THANK YOU** NHA IS team

Goal 4: Video cyber security message

Aiming to educate everyone and to collectively build cyber conscious culture across PM-JAY, a video message with anecdotes showcasing cyber security awareness guidelines was shared will all personnel. This was to encourage everyone in taking proactive steps to enhance cybersecurity and own their role in protecting a part of PM-JAY cyberspace.

Goal 5: Knowledge quiz for all

To mark the ending of Cyber Security Awareness Month at NHA, and to evaluate the learnings through the month, a cyber security awareness knowledge quiz was circulated among all PM-JAY personnel. There were 10 multiple choice questions carefully presented to PM-JAY personnel to choose one correct answer. There were 11 personnel who got all answers correct.



NHA Cybersecurity Awareness Month 2020 ||
Knowledge Quiz

Instructions
* This is a multiple choice answer questionnaire.
* Select the radio button (option) to indicate the correct answer.

Email address *

Valid email address

This form is collecting email addresses. [Change settings](#)

What does the "https://" at the beginning of a URL denote, as opposed to "http://" (without the "s")?

- That information entered into the site is encrypted
- That the site has special high definition
- That the site is the newest version available
- That the site is not accessible to certain computers
- None of the above