पेंशन निधि विनियामक एवं विकास प्राधिकरण
PENSION FUND REGULATORY AND DEVELOPMENT AUTHORITY

No. PFRDA/33/1/0001/2021-ICS INTDY

19-07-2022

To,
All NPS/APY Subscribers & Stakeholders

Subject: PENSION CYBER SPOTLIGHT - Newsletter for the Quarter ending March 2022

1. '**PENSION CYBER SPOTLIGHT**' The Quarterly Cyber Security and Technology Newsletter designed in a lucid way towards the objective of creating much needed awareness in a rapidly evolving cyber threat scenario, in order to safe guard one's prized assets.

2. '**PENSION CYBER SPOTLIGHT -VOLUME 4**' focuses on Digital assets and Neo-banks, attached at Annexure for the benefit of the stakeholders. The newsletter aims to brief the Financial Industry and Pension Sector stakeholders on the cyber security issues and the latest Financial Technology developments.

3. The bulletin is issued under section 14(2)(1) of PFRDA Act 2013 towards educating the subscribers and the general public on issues relating to pension, and the same placed at PFRDA's website retirement savings (www.pfrda.org.in) under the 'Pension Cyber Spotlight in the About Us' section.

Yours sincerely,

K.R Dasulath Ali Khan
General Manager

VOL 4| JULY 2022

PENSION CYBER SPOTLIGHT

CHAIRMAN'S DESK

In the epoch of digital world, the assets are confined not only to physical assets like oil, gold, capital and the likes but has also transgressed into digital arena. Today, digital assets hold much more value and significance than any other assets. The digital assets contain a gamut of information about their respective owners and hence can be used to targeted advertising, policy making, improving user shopping experience online. But the same set of data can expose owner to various risks. These digital assets and their data allow hackers and cyber-criminal to peep into one's life and launch sophisticated attacks. Hence, securing one's digital asset is of utmost importance.

The 4th volume of Pension Cyber spotlight deals with this pertinent issue and endeavours to make its stakeholders more cyber vigilant. The volume will help readers understand what, how and why of digital assets, so that they remain cyber secure.

FOCAL POINT

DIGITAL ASSETS

WHAT ARE DIGITAL ASSETS?

Today, we are living in digital world and Digital assets are the assets stored in an electronic form on the web or in the cloud. Digital assets are different from that of physical assets. The physical assets such as equipment, machinery, buildings, vehicles, physical documents, etc., which are also known as tangible assets, whereas trademarks, copy writes, licenses, organizational content available on websites, organizational applications, subscribers' data stored within organizational applications, publicly available information and material on websites that are known as digital assets and are also known as intangible assets. These intangible assets are stored by taking concert from public or subscribers and are fully owned by organizations that stores, processes and maintains these intangible assets which are digital in nature. A few examples of digital assets include your subscription accounts, email, with usernames and passwords.

WHY ARE DIGITAL ASSETS IMPORTANT?

These digital assets are important to an individual as they are associated with a value and any compromise of these digital assets shall have an impact to the individual or an organization. According to information security principles confidentiality, integrity, and availability, which are also known as CIA triad must be maintained for an information asset irrespective physical or digital. CIA are most important concept of information security that starts with each letter representing the foundational fundamental principles of cyber security.

COMMON RISKS

Legacy Technology

Non scalable legacy technologies, introduce additional security risks

Unhardened Information Asset

Unhardened information asset is vulnerable to ransomware attacks.

Unauthorized Access

Gaining access to Digital assets through compromised or shared credentials

Security Patching

Unpatched vendor released security patches make your digital ecosystem Vulnerable to cyber attacks

Unsecured Wi-Fi Networks

Information can be stolen while connecting through public Wi-Fi

HOW CAN AN ORGANIZATION OR PUBLIC PROTECT THEIR DIGITAL ASSETS?

Harden Your Systems

Ensure that servers and devices storing your digital assets are harder using industry best practices before commissioning

Password Management

Ensure that your password meet the length, complexity and change at regular frequency. Ex 10 Characters in length and is combination of at least one each of Alpha (at lease on UPPER & Lower Case), Numeric and special characters

Email security

Do not open or respond to unsolicited emails or click on links referred in such email. This can be a phishing attack to harvest your digital assets

User Access Management

Always ensure that your applications are enabled with two factor authentication and access users is enabled with least privileges by default

Encryption

Always ensure your applications are enabled with HTTPS (SSL/TLS 1.2 Ciphers) for encrypting data in transit and a lock symbol in the URL section of the browser

Malware Distribution

Always endure that your systems / devices are installed with licensed Antivirus software, updated with latest security patch, and configured to scan & quarantine

Always Stay Up to Date

Always ensure that your applications and systems are installed with vendor released stable security patches

NEO BANKS IN SPOTLIGHT

Neo banks are digital banks similar to regular banks, however not regulated by any financial regulator in India. They partner with licensed banks, NBFCs, and other financial institutions to provide financial services. They provide almost all financial services that a regular bank provides through apps that can be accessed through a smart device (e.g., Smartphone, tablet).

Visible characteristics of neo banks

- **They have no physical branch instead run on a digital platform**
- **Automate and facilitate customer service**
- **Usage of modern technology, like AI and chatbots, for virtual online support**
- **Allow opening accounts, payment and money transfers, loans, budgeting**

As Neo banks are taking charge in India, security risks to Neo bank accounts are also increasing as many banking/financial services are to be exposed to consumers/users that could be exploited with social engineering, vishing, phishing, etc. And at the same time as the Neo bank is using the CBS (Core Banking Solution) platform of the financial entity, they partner with therefore not just the Neo bank IT system however, the IT system of the inherent financial entity is exposed to the outer world as they use APIs/ISO messages to interact with CBS platform of partner financial institution that could lead to more security concerns (One such example was loyalty vulnerability).

Compared to large financial institutions, Neo Banks are relatively smaller entities; therefore, Neobanks could not afford to spend much on security or hire a full-time cybersecurity team, which might lead to facing serious security threats:

However, Neo Banks are the need of the hour as the new-generation prefer banking services on their smart device. Also, they meet the new reality, where online or contactless payments become more convenient and safer. This famous quote by Victor Hugo summarily captures the present situation of Neo Banks, *"No force on earth can stop an idea whose time has come."*

Therefore, Neo Banks would require robust solutions to ensure the adequate security level vital for financial institutions of any type.

CYBER CHANAKYA

Always follow these practices, and be the chanakya of cyber space.

GOVERNMENT INITIATIVE

Cyber Swachhta Kendra

The "**Cyber Swachhta Kendra**" (Botnet Cleaning and Malware Analysis Centre) under the Ministry of Electronics and Information Technology (MeitY) is a part of the Government of India's Digital India initiative to foster a secure and reliable cyber space by timely detection of botnet infections in India and notifying, enabling cleansing and protecting systems of end users to prevent any further infections. The "**Cyber Swachhta Kendra**" is established in accordance with the objectives of the "National Cyber Security Policy". This centre is being operated by the Indian Computer Emergency Response Team (CERT-In) under provisions of Section 70B of the Information Technology Act, 2000.

QUIZ TIME

KNOW YOUR AWARENESS LEVEL

1. _____ type of sites are known as friend-of-a-friend site.
a) Chat Messenger
b) Social networking sites
c) Tutorial sites
d) Chat rooms

2. Which of them is a proper measure of securing social networking account?
a) Never keep your password with any relevant names
b) Keep written records of your passwords
c) Keep records of your password in audio format in your personal cell-phone
d) Passwords are kept smaller in size to remember

3. Which is correct with regard to log4j?
a) It is a vulnerability in java libraries.
b) It is a security feature of chrome browser
c) It is the latest cloud service
d) None of the above

4. Which of the following is a benefit of cyber insurance?
a) It prevents cyber attack
b) It detects cyber-attack in real time
c) It compensates for the loss incurred due to cyber attack
d) It reduces the likelihood of the attack.

Contributors:

- Sh. Srinivas Yadav - CISO, KFintech,
- Sanchita Jaiswal
- Vignesh C
- Giraj Yadav

Editorial Team:

- K Mohan Gandhi
- Daulath Ali Khan

Design Courtesy:

- Protean

FOR FEEDBACK/SUGGESTIONS
dept-cybersecurity@pfrda.org.in