पेंशन निधि विनियामक और
विकास प्राधिकरण
बी–14/ए, छत्रपति शिवाजी भवन,
कुतुब संस्थागत क्षेत्र,
कटवारिया सराय, नई दिल्ली–110016
दूरभाष : 011–26517501, 26517503, 26133730
फैक्स : 011–26517507
वेबसाईट : www.pfrda.org.in

PENSION FUND REGULATORY
AND DEVELOPMENT AUTHORITY
B-14/A, Chhatrapati Shivaji Bhawan,
Qutub Institutional Area,
Katwaria Sarai, New Delhi-110016
Phone : 011-26517501, 26517503, 26133730
Fax : 011-26517507
Website : www.pfrda.org.in

No.: PFRDA/33/1/1/0001/2021-ICS INTRDY 01 November 2021

To,

All NPS Subscribers & Stakeholders

Subject: Pension Cyber Spotlight – Newsletter for the Quarter ending September 2021

As the economy is becoming more digitized, Cyber security incidents have also grown manifold with adoption of Digitalization and extensive use of Emerging Technologies such as Internet of Things (IOT), Artificial Intelligence (AI) and Cloud. The pandemic has further exacerbated the vulnerabilities with remote working becoming ubiquitous across organizations and digitalization penetrating the Financial Intermediation activities with rise of digital payments and personal investment through mobile application/online mode becoming the *new normal*.

The *data breaches, cyber jacking, ransomware attacks and deep fakes* across the world have shown the need for creating awareness and up-skilling among NPS Subscribers and the critical stake holders to protect their pension wealth, prosperity and reputation.

2. '**PENSION CYBER SPOTLIGHT**' The Quarterly Cyber Security and Technology Newsletter of PFRDA has been compiled and 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 *priced assets*.

3. **'Pension Cyber Spotlight – Volume 2'**, has been attached at Annexure for the benefit of the stakeholders. This edition marks the **Cyber Security Awareness Month of October** and aims to brief the Financial Industry and Pension Sector stakeholders on the cyber-security issues and the latest financial technology developments.

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

Yours Sincerely,

K Mohan Gandhi

Chief General Manager

pfrda
Azadi Amrit Mahotsav
CYBER SECURITY
We Evolve. We Secure.
Cyber Security Awareness Month
VOL 2 | OCTOBER 2021

PENSION CYBER SPOTLIGHT

CYBER SECURITY IS EVERYONE'S RESPONSIBILITY

PFRDA'S CYBER SECURITY AND TECHNOLOGY NEWSLETTER

CHAIRMAN'S DESK

Cyber Security is now part of every individual's life. Digital adoption and increased connectedness have made safeguarding our digital assets and identities a shared responsibility. With the objective to bring Cyber Security to the main stage and make organisations and individuals aware, month of October is globally marked as the National Cyber Security Awareness Month (NCSAM). This is an initiative towards ensuring better cyber hygiene and to incorporate stronger security measures.

I am elated that 2nd volume of Pension Cyber Spotlight on the theme of 'Cyber Security Awareness' has been conceptualised in a lucid way for the benefit of the crores of NPS, APY subscribers.

- Shri Supratim Bandyopadhyay

WHOLE TIME MEMBER (LAW) 'S MESSAGE

Cyber Security is a collective responsibility of the government, organisations, employees, consumers and citizens at large to stay cyber safe. Cyber Security is to be seen as adding value to the overall organisation and not as a cost. Following the best cyber security practices and ensuring the data is safe, builds the trust of the public in the organisations.

Being ready for the new cyber reality requires multidimensional approach taking organisations and the public as a single ecosystem. Pension Cyber Bulletin is one the initiatives of PFRDA towards a continued effort of building informed ecosystem of subscribers and intermediaries.

- Shri Pramod Kumar Singh

FOCAL POINT

Cyber Security Awareness

Since the year 2004, Cyber Security Awareness month is being observed around the world. Over a period of time, Cyber Security Awareness is becoming more and more relevant with the evolving reality of cyber security threats. Cyber Security Awareness is now of prime importance to ensure safer and secured online / digital roadmap of the country. While Cyber Security to digital world is equivalent to the breathing for the living world, this month is earmarked specifically to keep reminding us all regardless of us being computer users from large enterprises or as individual computer users, we all have certain role to play in securing the digital assets used by us.

This edition of Pension Cyber Spotlight has been crafted carefully to focus on enhancing the awareness of the readers in understanding, identifying and managing cyber security.

COMMON CYBER THREATS FACED BY ORGANISATIONS AND PUBLIC

Malware

Software maliciously spread with intention to gain unauthorised access to your digital assets. Most cyber crimes succeed using this method.

Social Engineering

Attempts to trick users to give away sensitive information or transfer money to fraudulent accounts.

Digital Frauds

Committed by cyber criminals with intention to abuse unaware computer users. This results in financial losses to sensitive information disclosure causing harm.

Ransomware

Specialized form of Malware designed to target specific computer systems and lock data or hardware making it un-usable to the owner (victim). Ransom demands are made to release the same.

HOW CAN YOU BETTER PROTECT YOUR DIGITAL ASSETS?

Stay Up to Date

Update applications (apply patches) to latest versionand set security softwares to run regular scans.

Protect your Account

Enable Multi Factor Authentication

Secure Password

Construct using unique combination of numbers, alphabets (upper case & lower case) and special characters and special characters.

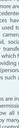
Use secured networks

Never connect to unsecure or open Wi-Fi for sensitive information sharing and financial transactions.

PHISHING IN SPOTLIGHT

Phishing is a method deployed to lure users in giving away sensitive personal information using deceptive e-mails and websites. This includes information like PIN, Credit Card Numbers, Account details and passwords.

HOW TO IDENTIFY THE TYPE OF PHISHING ATTACK?



Being aware of the threat is the first step towards not being spoofed!

Email Phishing

Mass emails masked as being from genuine sources, sent to trick recipients into revealing personal information such as passwords, credit card details, PINs etc. These are general attempts, sometimes without knowing the user.

Spear Phishing

These are sofisticated attempts which target high value victims or organisations. This method is highly personalised with the attackers crafting information specific to the recipient by referencing a file name or conference that only few known to recipient are privy to.

Whaling

Attack aimed at the high profile individual within organisations, stolen information is believed to highly valuable. Whaling references to corporate terms, legal subpoenas or customer complaints.

Vishing

Stands for voice phishing. The victims receive calls that are disguised as communications from a financial institutions. The attack convinces the victims to reveal personal confidential information.

SMS Phishing

SMS Phishing is a cyber attack that uses SMS/text messages to deceive victims. It usually contains a website link for providing details. Its more succesful than email phishing as people tend to respond more to texts than to emails.

DON'T TAKE THE BAIT!

Do not open suspicious emails claiming to be from known sources.

Never share personal or financial information over the internet.

Before entering sensitive details make sure the site's URL begins with "https" and a closed lock icon next to it.

MY DEVICE, MY CYBER SECURITY

HOW TO SECURE YOUR PHONE?

Mobile phones have changed the way of communication. For over 2.5 decades, mobile phones devices have become more and more feature rich and due to which gained unprecedented popularity and acceptance by masses. Mobile devices have almost replaced all supporting gadgets that we were used to. Apart from the contact list, other things like watch, camera, music, video entertainment, games, calculator, email, social media, banking and finance access systems, money transfer systems etc, etc, etc. are all packed in the Mobile device which fits in the pocket of the user. All these facilities, while making it much better to use, providing rich experience, also leads to consolidating all the sensitive personal data of users (personal photographs and family messages, social media, bank statements, etc.), facilities such as storing passwords and credit card details.

Research indicates that on an average, 80+ Mobile Apps are installed by the users. However, many Apps are designed to acquire many permissions at the time of installation. Users are negligent to this fact and allow all the permissions. Similarly open and free Wi-Fi networks are facilitated by many to attract the users. These networks are not necessarily set-up with all controls required to safeguard the users' data. Hence it is prudent that users understand their responsibility and follow certain discipline while using mobile devices and packing it with critical and sensitive information. While celebrating this month of October 2021 as Cyber Security Awareness Month, few tips on good practice that users should be aware are given here below:

- Always secure the mobile device with authentication mechanism. It can range from biometric lock (using fingerprint or face) to Passcode / PIN which user needs to set and remember.
- Never connect on open / free Wi-Fi while doing financial transactions or sending important information on email.
- Always have some antivirus installed and keep it active. Cost of personal data is very high as compared to cost of antivirus software license.
- Never download Mobile Apps from any unknown source. Always download it from Google Play Store or Apple iStore.
- Always review the permissions acquired by the Mobile App after installation. Disable all the unnecessary permissions (Why would a Game App need to have permission to access contacts and camera as well read permission to your files?).
- Never handover the mobile to any stranger to make any calls. Even if you need to help anyone in distress, dial the number yourself and allow such person only to talk. Make sure that you are around and carefully watching while he / she is talking.
- Always remember that not all SMS and social media posts are genuine. They may carry links and tempting offers which leads to user clicking the links resulting in their data theft or locking out the data followed by demand for ransom.
- Never ignore the Mobile App update notifications. As and when the App has an update, apart from the new features, they also have patches to plug any remaining / discovered later loop holes /vulnerabilities in the mobile App.
- Always be careful while using Bluetooth file transfer with relatives or friends. Make sure that they too have the antivirus installed.
- Never answer calls from unknown numbers (especially international numbers) when you are not expecting any call from someone whose mobile number is not stored in your contact. Further, never press any key combinations, if the callers asks you to do so. Certain combinations are used to take full control of your mobile.
- Always block the access to the storage area / files on the mobile, while connecting to charging stations in public areas like cafeteria, multiplexes, malls and airports. Carry your own charger instead of using such cables embedded in the charging stations.

For Feedback/Suggestions

Mail to:

Shri Mohan Gandhi
CGM
k.mohangandhi@pfrda.org.in

Shri Daulath Khan
DGM
daulath.khan@pfrda.org.in

Vignesh.c
Assistant Manager
Vignesh.c@pfrda.org.in

PFRDA appreciates NSDL CRA for their support.