PENSION FUND REGULATORY AND DEVELOPMENT AUTHORITY

PENSION CYBER SPOTLIGHT

VOL 3| FEB 2022

PFRDA'S CYBER SECURITY AND TECHNOLOGY NEWSLETTER

CHAIRMAN'S DESK

Social Media sites have connected people like never before and have seen rapid adoption in the past decade. This growth has meant sharing of personal information and data giving new avenues for cyber threats and privacy issues. The 3rd edition of Pension Cyber Spotlight throws light on the timely theme of Social Media and Cyber Security emphasising on 'Responsible Use' to protect self and society. All the very best to ICS dept and other intermediaries are welcome to provide contents from diverse fields., for the bulletin .

MEMBER'S MESSAGE

It is the 3rd issue of Cyber Spotlight and in each bulletin diverse areas of Cyber Security issues are covered for the benefit of stake holders. Cyber threats have now become a question of 'When' and not 'If' they will occur. With technology and data becoming ubiquitous across organisations and individuals, it is imperative to lessen risk. Cyber Insurance is emerging as an integral part of the risk mitigating strategy. In this regard, Pension Cyber Spotlight looks to address the question of 'Why Cyber Insurance?' for organisations as well as for individuals.

FOCAL POINT

SOCIAL MEDIA AND CYBER SECURITY

"being socially responsible …being responsibly social".

SOCIAL MEDIA

It is a platform (website or mobile app) which facilitates dialogue and remote connectivity to friends and relatives. It is also a medium for many businesses to promote themselves to masses. However, Social Media is a double edged sword. Unless handled properly, it can cause lot of harm to people. Not going in to the social aspects and behavioural changes caused to human kind due to percolation of Social Media, we will dwell upon discipline to protect ourselves from Cyber / Digital Security aspect of Social Media. Let us understand a few important terms causing harmful nuances to our life.

Profile Hijacking:

Did you ever imagine that someone could be having equal or more interest in your social media profile as much as your financial assets? Social media profiles have become an attractive target for many to fulfil their harmful intentions. Someone can hijack and misuse your profile to spread social unrest or send threatening messages to someone else. As your profile is used, the consequences of such act and burden of proving innocence would rest upon you. Therefore,

1) Update your passwords and security settings regularly. Wherever platform offers two / multi-factor authentication, activate it.

2) Never give account or page credentials to anyone who emails or direct messages you, especially if they claim to be customer support from the network itself.

3) Accept any connection request only after verifying that it is genuine, even if such connection request comes through a friend's recommendation, because you may not know if your friend's social media account is hijacked.

4) Never give permission to any and every app to post anything on social media on your behalf. Few such apps could take your consent right in the initial set-up. Keep reviewing the permissions given to / obtained by your app.

Fake Profiling:

Cyber fraudsters identify a soft target and create a social media profile using the identity and personal details like name, photograph etc. (It is easy to download your photograph from your social media) of such target, without their knowledge. This is called a fake profile creation. Further, such fake profiles are used to connect with the people in friend list of such person whose fake profile is used. Those who accept such friend request, are reached out and attempts are made to scam them out of money or threaten them of harmful consequences if they do not do as instructed by the fraudster. Therefore,

1) Verify the friend / connection request, especially if it is repeat request from someone already in your friend / contact list. Fake profiles would have very less pictures and posting history. It would also have far less connections.

2) Never ignore such requests by just not accepting it. Inform to the friend / associate whose social media profile is being used to connect with you again. If possible, inform the common friends.

3) Block such request and report it to the social media platform administrator. All social media platforms provide you such facility.

4) Never respond to any queries or pass on any information to messages that you may receive from such fake social media profile after or before you reject their connection request.

Cyber Bullying:

Social media is a very easy way to connect with anyone. However, that means that anyone can send any message to anyone as long as the sender knows the digital location (also termed as Handle or Page) of the person. Cyber-bullying is a method used to send messages which are either threatening or intimidating the receiver causing psychological distress. Therefore, to protect yourself.

1) Never allow access to open public for posting comments on your social media handle /page.

2) Always look the profile and limit it to only whom you have allowed in your connection / friend list.

3) Never bring out your frustration about anyone known to you, by posting such comments on social media.

4) Craft the language of your comments to ensure that they do not lead to social unrest against anyone.

Cyber Stalking:

If your profile is not private, people can get private information about you on social media. Cyber-Stalking defined in plain language is, “Persistent, unwarranted and unwanted contact with someone, primarily with intention of knowing more about the person and using that information to harm the person in on or the other way”. With the capabilities of Social Media, the risk of physical world contact has been eliminated for such stalkers. Without being identified or disclosing location, stalkers can easily track anyone on social media.
Therefore,

1) Never accept friend / connection request from people not known to you.

2) Always check if any friend / connection request is indeed genuine. If in doubt, call the person on confirming if such request is sent.

3) Never disclose unnecessary and personal information on Social Media. This platform is to have seamless contact with your friends and relatives and not a diary or calendar to log each and every event of your life.

4) Always use one to one messenger services if you have to pass on your contact coordinates like mobile or email ID to your social media friend / connection.

Image Tarnishing:

Using one or multiple of above methods, fraudster could attempt to tarnish your image. Social media platform does not have demarcation of personal and professional personas. On social media, your personal friends and office colleagues could be in common friend / contact list. Any comments / that you may put or any comment on which you respond would be mostly visible to all in your contact list. Therefore, while posting any comments / responding to any comments, it is necessary to exercise caution so that either ways it does not impact / affect your personal or professional reputation. On the other side, if someone could get access to your social media account or allowed to post on your profile, it becomes very easy for anyone to tarnish your image within your contact list. The extreme end could be digitally manipulating your photographs and posting it leading to a very awkward situation for you. Therefore,

1) Always be alert and cautions about what information and photographs you post on social media.

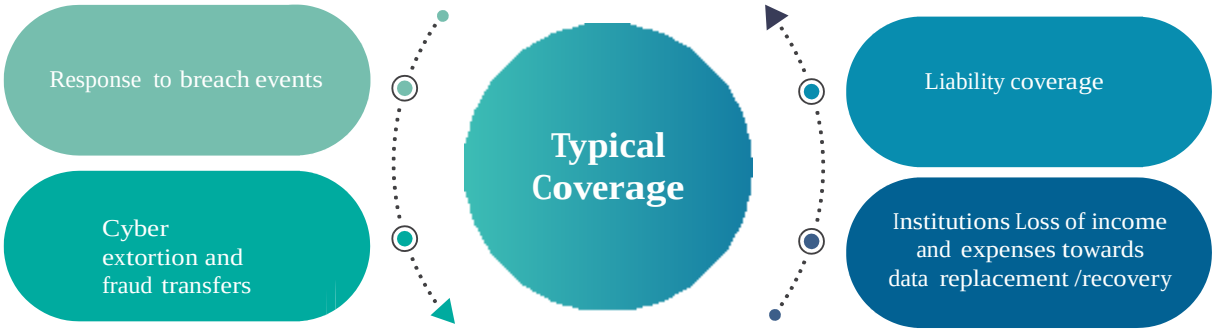
2) Never put anything in great elaboration making it easy to decipher much more information about your life (including places, relatives etc.). If you attend a wedding in family and feel like posting a selfie, one or two is sufficient. No need to post an entire album.

3) Always ensure that your camera or GPS does not have auto-posting feature enabled

4) Your family time and your outings are your private moments. Never post in elaboration as others really don't need to know your plans of travel and places you are about to visit.

SPOTLIGHT ON 'CYBER INSURANCE'

Cyber Insurance is becoming the need of the hour with cyber-attacks and cyber frauds increasing exponentially. The enhanced digitalisation especially post Covid 19 onset has increased the vulnerabilities of both institutions and individuals. Response, Recovery and Rebuilding from cyber-attacks entails significant monetary and time costs for organisations and individuals. Cybersecurity Insurance is typically designed to offset losses from potential cybercrimes such as ransomware, malware, DDoS attacks etc. and may include the cost of lawsuits and investigations arising from loss of critical information or data.



The cost of Cyber-Risk insurance policy depends on several factors such as vulnerability of the sector, for example: Financial Sector, Critical Infrastructure like Power and Healthcare, for its immense sensitive data. The premium will also be influenced by cyber preparedness of the organizations.

HOW CYBER INSURANCE CAN IMPROVE THE CYBER POSTURE OF COUNTRY?

Cyber insurance has an associated benefit of pushing organizations to invest in preventive measures by strengthening their cyber defence capabilities. Companies may be motivated to invest in capacity building of human resource and engage professionals for robust cyber security policy design and implementation. This may help bring down their cost of cyber risk insurance.

The India Perspective

With increasing volume and value of cyber-frauds and cyber-crime cases, there has been increased adoption of cyber insurance policies in India. Report by DSCI found that demand for cyber insurance grew by 40% in 2018. With increased cyber-attacks on personal computer networks since Work From Home due to covid-19 outbreak and enhanced risks with increased exposure to digital world, individuals are also in need for Cyber-Risk insurance. A 'Guidance Document on Product structure for cyber insurance' has been set out by insurance regulator in the direction of protecting individuals. This changing scenario of cyber threat has government and regulators working towards building a cyber-risk resilient digital world.

NEWS

Log4J Vulnerability

Log4j vulnerability called 'Log4Shell' detected recently is being considered as one of worst cybersecurity flaws, which if exploited by hackers can grant them access and control of an application. This is serious, as Log4j is a common logging library used in Java based applications and servers all over the world. While security patches have been released and cyber security firms are on constant vigil, threat of Log4J exploitation continues to persist due to its ubiquitous use.

GUIDELINES FOR CYBER SECURITY IN POWER SECTOR RELEASED BY INDIA

First time a comprehensive guideline for cybersecurity has been formulated in power sector. CEA has framed the guidelines under the Central Electricity Authority (Technical Standards for Connectivity to the Grid) (Amendment) Regulations, 2019. It lays down a cyber-assurance framework, mechanisms for security threat early warning, vulnerability management and response among others.

Major guidelines include Procurement of Information and Communication Technology based products from Trusted sources, appointment of CISO at each entity, and it requires entities to set up procedure for identification and reporting of threat to CERT-In within 24 hours.

PHISHING ATTACKS: MOST IMPERSONATED BRANDS

Recent report by Checkpoint research finds in its analysis of phishing emails that Microsoft continues to be most imitated brand. WhatsApp, LinkedIn and Facebook have made the list of ten (10) impersonated brands for the first time this year. Attackers aim to steal people's personal data by impersonating the above brands. To be secure from such phishing attacks one needs to be aware of mechanisms used by cyber criminals and follow the best practices.

QUIZ TIME: KNOW YOUR AWARENESS LEVEL

Remember what you read in the last bulletin (Vol No 2)? If not, read it before attempting the following Questions.

Multiple choice Quiz

1) Vishing is a form of

a. Email Phishing
b. Voice Phishing
c. Phishing using SMS
d. Desiring of some specific thing

2) Phishing attempts are made to extract

a. Personal credentials
b. Sensitive personal information
c. Financial information
d. All the above

3) Ransomware is deployed for

a. Stealing information from your storage
b. Destroying data on your storage
c. Encrypting data on your storage
d. None of the above

4) Cyber Security Awareness Month is observed every year in

a. November
b. August
c. January
d. October

5) Research indicates that on an average, users have _____apps on their smart phones

a. 76 apps
b. 80 apps
c. 84 apps
d. 88 apps

True of False Quiz

1) As a good practice to be followed in Information Security, I will always keep my smart phone equipped with Anti-Virus.

2) Considering humanitarian behaviour, I will always help any stranger by allowing him to use my smart phone.

3) Because my family members want, I will download any and every interesting app / game apps on my smart phone.

4) I will always connect to the free WIFI available during travel, because I am sincere to the work I have to do for my organisation.

5) I will always lock my smart phone with PIN or password to ensure that it is never misused if I leave it un-attended.

For Feedback/Suggestions

Mail to:

Sh. Mohan Gandhi, CGM
k.mohangandhi@pfrda.org.in

Sh. Daulath Ali Khan, DGM
daulath.khan@pfrda.org.in

Sh. Vignesh C, AM
vignesh.c@pfrda.org.in

PFRDA appreciate Protean CRA for their support