कर्मचारी भविष्य निधि संगठन
EMPLOYEES' PROVIDENT FUND ORGANISATION
(श्रम एवं रोजगार मंत्रालय, भारत सरकार)
(MINISTRY OF LABOUR & EMPLOYMENT, GOVT. OF INDIA)
राष्ट्रीय डाटा केंद्र /NATIONAL DATA CENTRE
1st Floor, Bhavishya Nidhi Bhawan, Plot No.23, Sector-23, Dwarka,New Delhi-110075
www.epfindia.gov.in

सत्यमेव जयते

CISO/Security/2022/ 1182 Date: 18.05.2022

CYBER SECURITY ADVISORY No 2022/01: PASSWORD SECURITY BEST PRACTICES

1. **Introduction**. A password represents a shared secret between the end user and the system they are authenticating. The system cannot differentiate the real user from another user who also knows the password. Thus, it is essential that users keep their password private. Stolen, weak or reused passwords are prominent reasons for data breaches worldwide.

2. **Best Practices**. The following best practices should be followed by all IT asset users and data owners: -

(a) Ensure a strong and unique password for all accounts.

(b) All passwords to be treated as sensitive and classified information.

(c) Use combination of upper case & lower case, letters, numbers and symbols in password.

(d) Never reuse password on multiple account.

(e) Do not use any information in password that can be found out in social media profiles (like DoB, name, etc.)

(f) Avoid using dictionary words and commonly used passwords.

(g) Never share password with anyone.

(h) Avoid password recycling.

(i) Always change vendor supplied default password and remove or disable unnecessary default accounts before installing a system on the network.

(j) Never text or email password.

(k) Do not use the same password for official and personal accounts.

(l) Avoid saving passwords to a computer.

(m) Do not provide user id or password on any page popping up by clicking on a hyperlink received through email.

(n) Use Multifactor authentication.

(o) Always decline the use of " Remember Password" feature of applications (browsers, email clients, messengers etc)

(p) Do not reveal a password on questionnaires or security forms.

(q) Do not speak about a password in front of others.

(r) Password should never be written down.

(s) Password must be changed atleast every 45 days.

(t) Some suggested ways to construct a strong password are as follows: -

(i) A secure password not only consist of letters, but also use numbers and special characters. For example, "i" will become "!", an "o" turns into a "0" and "s" is written as "$". This way, the simple term "Microsoft" changes to the substantially harder word "M!cr0$0ft".

(ii) The longer the password, the harder it is to crack.

(u) Obtain and install endpoint protection (antivirus, anti-malware, anti-spyware and firewall software) and make sure it is active and automatically updated online or take necessary steps to keep it updated.

2. **Conclusion**. An employee's failure to comply with the above guidelines regarding password security can lead to many major issues like data breaches, loss of sensitive information, account takeovers, exposure to malware, insider threats, reputational damage etc. It is emphasized that the most effective control against fraud is a well-informed user. The end user at EPFO must maintain confidentiality of login password and ensure security of information entrusted to their care.

3. For information and strict compliance please.

(Rahul Modgil)
Chief Information Security Officer

To,

1. PPS to CPFC
2. FA & CAO, CVO
3. ALL ACC/ ACC (HQ) in Head Office and NDC
4. ALL ACC/ ACC (HQ) Incharge of Zones
5. Director, PDUNASS
6. ALL RPFCs Incharge of Regional Offices & NDC
7. CTO
8. OICs of District Offices