CENTRAL KYC RECORDS REGISTRY

CKYC/2022/03 Date : January 27, 2022

To: All entities registered with Central KYC Records Registry (CKYCRR)

Dear Sir / Madam,

Sub: Cyber Security Advisory – Precautionary Measures

Due to the outbreak of COVID-19, many employees are currently working from home. This has resulted in an increased dependency on digital communications manifold and many operations may be under remote monitoring mode.

This is the time when cyber-attacks generally peak as the attackers try to utilize the paranoia around such pandemics and hence, we request all of you to be very wary and careful. The most common scams and possible attacks are as follows:

Social Engineering Attacks - You may receive bogus emails that appear to be from legitimate sources containing malicious links. These links, if clicked may lead to your devices being infected with malware.

Ransomware Attacks – Applications from unknown sources that claim to provide a much-needed utility. Once installed, the app asks for various permissions which it claims are needed to be able to deliver notifications and then installs ransomware due to which you cannot access your phone as it forces a change in the phone's lock screen password.

Phishing Attacks - Phishing emails which claim to be from legitimate sources and generally contain a malicious link. Once clicked, it requests the victim for their financial and tax information, bank details and PII.

Protection Measures

1. Do not click on links or download attachments from unknown sources.
2. Always verify the security of a website – Check the site has been secured using HTTPS /Check for a website privacy policy / Use a website safety check tool such as Google Safe Browsing / Do a WHOIS lookup to see who owns the website.

3. Pay close attention to the spelling of an email or web address, if there are any inconsistencies, delete immediately.
4. Ignore and delete emails with poor grammar and formatting.
5. Question the validity of any email that asks you to submit personal or financial information.
6. Do not download apps from untrusted and unfamiliar sites.
7. Pay close attention to the permissions requested by an app and think twice before you grant access to sensitive information such as your address book or access to your photo library.
8. Use a Secure Wi-Fi connection while connecting to office environment. Avoid the use of public Wi-Fi. With an insecure connection, people in the near vicinity can snoop your traffic. Place the Router in the Center of Your Home. Change default passwords on you home Wi-Fi router.
9. Use strong passwords/passphrases to login to your personal desktops/laptops.

i. A strong password should be between 12-15 characters long, a mix of uppercase and lowercase letters and include numbers or symbols. For extra security, a passphrase can be created which is a password composed of a sentence or combination of words. The first letter of each word will form the basis of the password and letters can be substituted with numbers and symbols to add a further line of defence.

ii. Use separate logins for home system for work purpose.

iii. Ensure not to reuse passwords across the web.

iv. Consider the use of a password manager to maintain the security of multiple accounts.

v. When choosing a password/passphrase, avoid the use of:

a. Your name in any form or any abbreviations

b. The name of close relatives or pets

c. Birth dates or anniversaries.

d. Famous quotes

10. Ensure your laptops/systems are updated with latest anti-virus versions and patches.

11. Remember to back up all important files regularly. Disk encryption is an option available in most operating systems. In many cases it is optional that can be enabled as and when required.

12. Don't click on COVID-19 related messages with attachments. Don't forward them to family or friends.

13. Be wary of websites that start "Coronavirus" or "Covid." E.g. Do not install or click on apps like "coronavirusapp.site." which supposedly tracks virus outbreaks. Downloading such applications will infect your systems/phones with ransomware.

14. Seek legitimate information from authentic government, university, hospital and news sites with names you know.

15. Think carefully about letting family and friends use a computer that's also now used for work.

Disclaimer:

a. The information contained in this notice has been extracted from regulatory and public forums and has been published only as guidance to reporting entities. As the future course of events with regards to these threats are not known, members are advised to keep a close watch on their systems to identify timely detection and remediation of this threat.

b. Members shall act upon this notice at their own discretion after conducting appropriate impact/risk analysis to their specific environment.

c. Please note that other exploit kits are also widely in circulation and available for download for free on the Internet and there are possibilities of attack vectors other than this threat which may exist/emanate. It is critical to perform a self-assessment against these zero-days/ exploit kits released in the wild in a controlled environment.

d. This notice is for informational purpose only

For and on behalf of **C**entral **KYC R**ecords **R**egistry

Helpdesk Contact Details:

Email: helpdesk@ckycindia.in
Phone: 022 61102592 / 022 26592595