GURU GOBIND SINGH INDRAPRASTHA UNIVERSITY

Guru Gobind Singh Indraprastha University

(A State University established by the Government of NCT of Delhi)
Sector 16-C, Dwarka, New Delhi 110078

University IT Services Cell

[Room No. D-412, Phone: 011-25302746, Email: uits@ipu.ac.in]

Ref: GGSIPU/UITS/.336....

Date:...13-03-2023

CIRCULAR

An email received through Office of Registrar from All India Council for Technical Education regarding promotion of cyber hygiene / cyber security / prevention of cybercrime with details of (1) **Cyber Security Do's and Don'ts and (2) User Guide – 10 Steps to Protect your personal data**.

The same is attached with this circular as the ready reference.

All employees and students of University are requested to follow the above laid guidelines in day to day activities.

Prof. Pravin Chandra
(Incharge, UITS)

Copy for information & compliance of circular to:-

1. All Deans, Directors and Branch Heads, GGS Indraprastha University
2. AR to Vice Chancellor - For Kind Information to the Hon'ble Vice Chancellor
3. AR to Registrar - For Kind Information to worthy Registrar
4. UITS – To upload on University
5. Guard File

Pushpendra K. Mishra
(System Administrator, UITS)

University IT Service
GGS Indraprastha Un
Dwarka 16C, New Delhi-75

CYBER SECURITY DO'S AND DON'TS

✓ BEST PRACTICES AGAINST PHISHING

- Periodic Individual awareness
- Think before you CLICK
- Practice good cyber hygiene practices both
- Use Multi-Factor Authentication (MFA)
- Verify a website's legitimacy
- Check all online accounts including social media regularly
- Keep Browser up to date
- Beware of Pop-Ups
- Never disclose Personal Information
- Use genuine and updated software
- Use updated antivirus
- Report the incident

✓ CYBER SECURITY DO'S

- Use complex passwords.
- Change your passwords at least once in 45 days.
- Use multi-factor authentication, wherever available.
- Save your data and files on the secondary drive (ex: d:\).
- Maintain an offline backup of your critical data.
- Keep your Operating System and BIOS firmware updated with the latest updates/patches.
- Install enterprise antivirus client and ensure that the antivirus client is updated with the latest virus definitions, signatures and patches.
- Use authorized and licensed software only
- Ensure that proper security hardening is done on the systems
- When you leave your desk temporarily, always lock/log-off
- When you leave office, ensure that your computer and printers are properly shutdown.
- Keep your printer's software updated with the latest updates/patches.
- Setup unique passcodes for shared printers.
- Use a Hardware Virtual Private Network (VPN) Token for connecting privately to any IT assets located in the Data Centers.
- Keep the GPS, Bluetooth, NFC and other sensors disabled on

your computers and mobile phones. They maybe enabled only when required.

- Download Apps from official app stores of google (for android) and apple (for iOS).
- Before downloading an App, check the popularity of the app and read the user reviews. Observe caution before downloading any app which has a bad reputation or less user-base, etc
- Use a Standard User (non-administrator) account for accessing your computer/laptops for regular work.
- Observe caution while opening any shortened uniform resource locator (URLs) (ex: tinyurl.com/ab534/). Many malwares and phishing sites abuse URL shortened services.
- Observe caution while opening any links shared through SMS or social media, etc., where the links are preceded by exciting offers/discounts, etc., or may claim to provide details about any current affairs. Such links may lead to a phishing/malware webpage, which could compromise your device.
- Report suspicious emails or any security incident to incident@cert-in.org.in

✓ CYBER SECURITY DON'TS

- Don't use the same password in multiple services/websites/apps.
- Don't save your passwords in the browser or in any unprotected documents.
- Don't write down any passwords, IP addresses, network diagrams or other sensitive information on any unsecured material (ex: sticky/post-it notes, plain paper pinned or posted on your table, etc.)
- Don't save your data and files on the system drive (Ex: c:\ or root).
- Don't upload or save any internal/restricted/confidential government data or files on any non-government cloud service (ex: google drive, dropbox, etc.).
- Don't use obsolete or unsupported Operating Systems.
- Don't use any 3rd party anonymization services (ex: Nord VPN, Express VPN, Tor, Proxies, etc.).
- Don't use any 3rd party toolbars (ex: download manager, weather tool bar, askme tool bar, etc.) in your internet browser.

10 A USER'S GUIDE: WAYS TO PROTECT YOUR PERSONAL DATA

1 Don't click that link!

What to do: Don't click untrusted links in emails. Instead, type the URL you want directly into the browser.

Why: According to Microsoft, phishing is still the number one favorite method of cyber-attacks.

2 Use two-factor authentication

What to do: Use a second factor for logging into accounts.

Why: If you have a robust two or multi-factor in place, you are much less likely to lose personal data due to phishing.

3 Delete recorded conversations

What to do: Regularly delete any recorded conversations used by your personal assistant.

Why: There have been cases where Alexa revealed personal data to unknown persons without consent.

4 Keep it clean — delete old files

What to do: Make sure you keep data replication to a minimum. Delete old files you don't use.

Why: There can never be 100% security, but reducing the places that can be compromised helps lessen your risk.

5 Be less social

What to do: Minimize the amount of personal data you have on social media platforms.

Why: Information like your pet's name or mother's maiden name is sometimes used to recover account logins. Don't give hackers an easy way into your online accounts!

6 Don't sync for sync's sake

What to do: Disable automatic file and media sharing whenever possible.

Why: A lot of devices set up cloud syncing when you first configure the device. Check if you really want to store these data in the cloud.

7 Keep off the beaten track

What to do: Disable location tracking on each app.

Why: A recent study of almost 1 million Android phones demonstrated that apps regularly harvested tracking data.

8 Let sleeping Bluetooth lie

What to do: If you are not using Bluetooth, switch it off.

Why: Bluetooth vulnerabilities can allow data to be siphoned off your device.

9 Encrypt stored data

What to do: Encrypt any data you store on hard drives and use an email encryption tool if you share personal data.

Why: Encryption is a layer of protection that can prevent lost or stolen data from being exposed.

10 Patch your devices

What to do: Keep your computers and mobile devices patched and up to date.

Why: Software vulnerabilities allow malware to infect your device, which can steal data and login credentials.

AICTE

G20 भारत 2023 INDIA