Gujarat National Law University

Gujarat National Law University

GNLU PRESS NOTE No. 08/2021

Workshop on "Digital Literacy and Online Safety"

Gandhinagar, February 20, 2021: GNLU Centre for Women and Child Rights organized a Workshop on "Digital Literacy and Online Safety."

The workshop was organized under the "We Think Digital" initiative of Cyber Peace Foundation in collaboration with the National Commission for Women and Facebook and conducted by Ms Janice Verghese of Cyber Peace Foundation.

Ms Janice focused on Understanding Data and Digital Footprints, Responsible Online Behaviour, Misinformation and Cybercrime and Redressal and said that being safe and protecting yourself, your data and privacy online is extremely important.

She said one should be careful while giving permissions to any application. She said, "People tend to give unnecessary permissions while installing applications. It makes their data vulnerable. To function, most of the Apps do not need access to your location and no app needs access to your messages. You should never give access to your Messages as messages contain One-Time Passwords (OTPs) for financial transactions and if one can access your messages, and therefore OTPs, you can become a victim of financial fraud."

She advised the participants to be extra careful while selling their devices (phones or laptops). She said people generally opt for the "Factory Reset" option and believe that their data is erased. But, the "Factory Reset" does not delete the data permanently; it only creates an illusion that the data is deleted. The data remains on the device and can be recovered with the appropriate software. "You should use Bit Erasing Apps, a software-based method of overwriting the data that aims to destroy all data on a device by using zeros and ones to overwrite data onto all sectors of the device. By overwriting the data on the storage device, the data is rendered unrecoverable and achieves data sanitization.

She said that one can browse the net for information on unsecured websites (HTTP) but should never enter any data on such websites. "Before you enter any personal data on a website, make sure it is a secured website – HTTPS – Hypertext Transfer Protocol Secure - that protects the integrity and confidentiality of data."

To guard against phishing, never click on a link received from an unknown source. If you receive an offer that is too good to be true, it probably is. If someone offers you an unbelievably huge discount, you are perhaps being lured into a phishing attempt.

If you face a problem during online shopping and you need to lodge a complain, look for the customer helpline number on the app itself or the official website. Never google search for the same. If you google search the number, you are likely to reach a fraudulent platform and may end up losing money.

If you become a victim of a cybercrime, you should preserve as much evidence as possible – save the URL, IP Address, take a screenshot and never delete messages – and lodge a complaint with a local police station or a cybercrime police station. If you want to complain online, make sure you are lodging your complaint on the official government website ending with nic.in or gov.in. If you lodge your complaint on any other website, chances are that they may harm you further in the guise of helping you!

She gave the following tips for the protection of users, users' data & Privacy Online:

1. Always Enable 2-Factor-Authorisation
This is available on almost all social media and adds an extra layer of safety to your account. Every time a new device is used to access your account with the correct password, the account holder will be notified with a special code. This not only makes your account safe, but it also alerts you when an outsider is trying to get into your account.

2. Regularly Check Login Activity
Also known as "Authorised Logins" or "Recently Used Devices", this is a list of every device, browser and website that has access to or has accessed your account. From this list, you should always remove unknown entities if you see them as well as clear out past devices. This is a great way to see who could have access to your data and account.

3. Be Smart With Your Passwords
There are two parts to this. First, a password should never be a name, birthday, phone number or anything basic. Such passwords can be cracked in mere seconds. Plus, they are very easy to guess! Your password should be complex and meaningless! Secondly, never share your password with anyone no matter who. They can be easily misused. Never use the same password for multiple accounts.

4. Turn off Location Access & "Background App Refresh"

Many applications ask for location permissions and most of us set it as "Always allowed", which isn't safe. Either deny all location services or allow them only when you use the application. This prevents third-party platforms from tracking your location even when you are not using the application. Turning off "Background App Refresh" makes sure the applications and browsers aren't running throughout the day and using your data without your active knowledge.

5. Use Unique Privacy Features on Various Platforms

Each application and social media platform has its unique privacy protection features that must be used. Explore them in the platform's privacy and safety settings. Here are a few things you can do on various platforms to stay safe online:

- Facebook: Use the "Lock My Profile" option
- Instagram: Turn off "Activity Status"
- Snapchat: Don't show yourself on "Snap Map"
- WhatsApp: Enable "End-to-End Encryption" and turn off "Live Location" when not in use
- For most platforms: Avoid linking one account (Facebook, Google, Apple etc) to log into multiple accounts.

6. Make Downloads From Trusted & Verified Sources

Using the Play Store and App Store is your safest bet as there are very little chances that downloads from these platforms will have viruses, Keyloggers or Spyware. Downloading things from random websites can lead to malware or data theft

7. Be Careful While Posting & Sending Pictures of Yourself

This is a given. Be very careful while sending and uploading pictures of yourself. The images should be such that even if they were leaked publicly, no harm would be done to you or your reputation. When it comes to sexting, avoid it at all costs. Even if you're sending pictures to a trusted person, they can be leaked.

9. Keep Updating Your Applications

Keep your devices and applications updated. With new versions come new and improved updates. These make your devices less susceptible to attacks and new viruses.

10. Report Inappropriate Content Immediately

If you notice anything fishy, inappropriate or abnormal, report it immediately! Most social media platforms have efficient and quick response teams.

Dr Asha Verma, Assistant Professor of Law and Head, GNLU's Centre for Women and Child Rights proposed a vote of thanks.

Media Contact:
Ashok Shah
Email: 9909960240, 8849110049