A Brief Report on the Workshop on Cyber Awareness and Cyber Hygiene Practices

July 7th, 2023, IBS Auditorium

On July 7th, 2023, the IBS auditorium was abuzz with distinguished panellists, experts, and enthusiasts discussing the crucial issue of cyber awareness and cyber hygiene practices. The focus was on understanding the legal and technical perspectives of cybercrime prevention, along with the nuances of data privacy.

From Left to right : Mr. Abhishek, Mr. Praveen, Mr. Ramesh, and Prof. Shailendra

Discussion Overview

The discussion kicked off with the keynote speaker, Dr. L.S. Ganesh, Vice Chancellor of the ICFAI Foundation for Higher Education outlining the importance of cyber hygiene in today's increasingly digital world. This was followed by two enlightening panel discussions that delved into different aspects of cybercrime prevention and data privacy issues.

Dr. L.S. Ganesh, Vice Chancellor, IFHE, giving the inaugural address

Dr. Shailendra Singh Bisht, Prof. Marketing and Strategy at IBS Hyderabad, welcoming the panel members

Panel 1

The first panel comprised of the following members from the Society of Cyberabad Security Council (SCSC).

1. Mr. Abhishek Kumar, Joint Secretary - Cyber Security and Principal Group Manager, Cyber Security, Microsoft.
2. Mr. Praveen Tangella, Alliant Group

3. Inspector Mr. Ramesh, Cyber Crimes Police Official

Mr. Rajendra Prasad and Mr. Bhanu Murthy of SCSC were instrumental in getting the speakers to the IBS campus. This session was moderated by Prof. Shailendra Singh Bisht.

Mr. Abhishek Kumar and Mr. Praveen spoke about the enterprise aspect of Cyber Security. According to Mr. Abhishek the individual is the weakest link in the Cyber Crime chain. He also specified how *phishing* was the greatest threat 20 years ago and still is. As far as prevention is concerned, one needs to be aware of the different ways in which such crimes can happen. They spoke about how malware can sit in between the email interaction of a CFO and CEO. The malware can trigger an email requesting the CFO to transfer money to a particular bank account. The CFO would see this as an order from the CEO but in fact it is the malware doing its thing and siphoning of money.

Mr. Ramesh provided examples of different types of complaints from individuals. According to him greed is behind individuals providing all their details and getting lured by fraudsters. He spoke about how a small place called Nuh in Haryana produces thousands of fraudsters. Job related scams where the victim is promised a job with high salary were also talked about. Once the victim accepts the job, he/she is asked to transfer some amount of money for creating ID or for processing papers. Once the money is transferred, the scammers can't be traced. There are cases of extortion where a video call is made via WhatsApp and the victim blackmailed to fork out money.. He also urged the participants never to share their smartphones with anybody including close friends. They might call people from the opposite sex and later the owner of the smartphone might be blackmailed into giving money to the perpetrator of the crime.

The session ended with a vote of thanks by Sanjay Fuloria.

Panel 2

The second panel comprised of:

1. Dr. Md. Akbar Khan, Associate Professor, Faculty of Law, IFHE.
2. Dr. Ritu Chhabra, Assistant Professor, Faculty of Law, IFHE.
3. Dr. P. Pavan Kumar, Assistant Professor, Faculty of Science and Technology, IFHE.

This discussion focused on the legal aspects of data privacy, legal aspects of cyber-crime, and the technical aspects of cyber security.

Dr. Md. Akbar Khan cited various provisions in the Indian law which deal with data privacy. He was of the opinion that law follows technology and not the other way round. Individuals need to be careful while using technology as it is a necessary evil. The data protection laws in Europe such as General Data Protection Regulation (GDPR) are leading the way. India is lagging but it has a bill ready to be discussed in the parliament.

The General Data Protection Regulation (GDPR) is a regulation in EU law on data protection and privacy for all individuals within the European Union (EU) and the European Economic Area (EEA). It came into effect in May 2018 and requires businesses to protect the personal data and privacy of EU citizens for transactions that occur within EU member states. The regulation also applies to companies outside the EU that offer goods or services to individuals in the EU. The GDPR seeks to give individuals more control over their personal data and simplify the regulatory

environment for international business by unifying the regulation within the EU.

In the legal realm, Dr. Ritu Chhabra, a cyber law expert at the Faculty of law at IFHE , highlighted how laws and regulations can play a vital role in preventing cybercrime. Emphasis was placed on vigilance at the level of the individual. She gave an example of how a family while going on a vacation posted pictures of their house. This invited undue attention from thieves and they promptly stole a lot of stuff from their house. Publicly sharing your whereabouts is a strict no-no.

The panel also discussed the ongoing challenges of jurisdiction in cybercrime, as criminals often operate across borders, making it tough to apprehend and prosecute them. The audience was informed about the need for harmonizing cyber laws globally to ensure more effective enforcement.

From left to right : Prof. Md. Akbar Khan, Prof. Ritu, Prof. Pavan Kumar, and Prof. Sanjay

On the technical front, Prof. Pavan Kumar, a faculty member at the Faculty of Science and Technology at IFHE , discussed the different forms of cyber threats, such as phishing, malware, ransomware, and Denial-of-Service (DoS) attacks. They underscored the importance of keeping software and systems updated to patch vulnerabilities that could be exploited by hackers.They also highlighted the importance of robust encryption in safeguarding data, secure backup practices, and the use of secure networks. Practical advice included using strong, unique passwords for different accounts and implementing multi-factor authentication where possible.

Panel 2 members

He also drew attention to the technical aspects of data privacy, such as anonymization and pseudonymization techniques, privacy by design, and the critical role of data protection officers in organizations. The importance of knowing one's digital rights and how to exercise them effectively was underscored.

CEDT members with the DOT Club

The discussions ended with Ms. Aditi from the DOT club thanking all the participants.

As per both the panel members, here are some simple preventive strategies to maintain online security:

Prof. Venugopal, Director IBS Hyderabad, addressing the workshop attendees.

1. **Use Strong, Unique Passwords:** This is your first line of defence. Make sure your password is a combination of letters (upper and lower case), numbers, and special characters. Avoid common words or phrases and never use personal information that might be easily guessed or found online. Use a different password for each of your online accounts.
2. **Enable Multi-Factor Authentication (MFA):** MFA is a method of verifying a user's identity by using multiple verification methods. This could be something the user knows (password), something the user has (security token or a mobile device), or something the user is (biometric verification). If one method is compromised, the attacker still has at least one more barrier to breach.
3. **Regularly Update Your Software and Devices:** Software updates often include patches for security vulnerabilities that have been discovered since the last version was released. Keep your operating system, apps, and devices updated to protect yourself against these vulnerabilities.
4. **Use Secure Networks:** Be cautious when using public Wi-Fi. Unsecured networks can expose your device to others on the same network, leaving your data vulnerable. If you have to use a public Wi-Fi, avoid accessing sensitive information, such as bank accounts, or use a trusted virtual private network (VPN).
5. **Install a Reliable Antivirus Software:** Antivirus software can protect your device from malware by detecting, quarantining, and eliminating it. Choose reliable software and keep it updated to ensure it can protect against the latest threats.
6. **Be Wary of Phishing Scams:** Phishing scams often come in the form of emails or messages trying to get you to click on a link or provide personal information. Be wary of unexpected emails or messages, especially those that ask for personal information.
7. **Backup Your Data Regularly:** Regular backups can save your valuable data if you ever fall victim to a ransomware attack or if your device crashes. You can backup your data to an external hard drive or a cloud-based service.
8. **Educate Yourself:** Stay informed about the latest cyber threats and how you can protect against them. Cybersecurity is a rapidly changing field, and the more you know, the better you can protect yourself.
9. **Privacy Settings:** Review and adjust privacy settings on your social media accounts, applications, and other online platforms to control what information you are sharing and with whom.
10. **Think Before You Click:** Be cautious when downloading new applications or clicking on links,

especially from unknown sources. Some of these can contain malware or direct you to fraudulent sites.

Remember, the best defence against cyber threats is a combination of these strategies. Stay vigilant and make cybersecurity a priority to help protect your online activities.

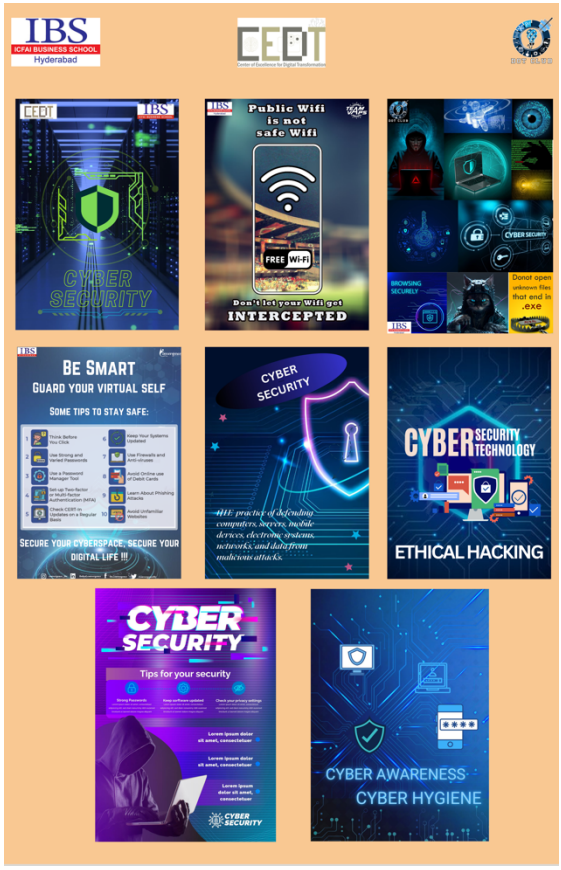
Poster Competition for IBS Hyderabad Students

A poster competition on "Cyber Awareness and Cyber Hygiene" was conducted prior to the event day. A total of 18 posters were displayed during the event.

Posters submitted by IBS Hyderabad students

Conclusion and Audience Response

The panel discussion concluded with a question and answer session, during which attendees had the opportunity to interact with the experts.



The event was a resounding success, providing a comprehensive understanding of cybercrime prevention and data privacy issues from both legal and technical aspects.

Attendees left the discussion with a greater appreciation for the complexity of the cybersecurity landscape and a clearer understanding of how to implement effective cyber hygiene practices. The discussion reinforced the notion that each of us, as users of digital technology, has a role to play in combating cybercrime and protecting privacy. This event served as a sobering reminder that in an increasingly interconnected world, vigilance, education, and awareness are key to navigating the cyber world safely and responsibly.

This report was prepared by CEDT on July 8th, 2023.