SMART COLLEGE
We are different.

FCI

FACULTY OF CRIME & INVESTIGATION
SEPTEMBER ISSUE

NEWSLETTER

CYBER FRAUD

IN THIS ISSUE:

1. CONCEPT & TYPE OF CYBER FRAUD
2. CHARACTERISTIC OF CYBER FRAUD
3. CASES OF CYBER FRAUD
4. CYBER FRAUD CASES IN MALAYSIA
5. PREVENTION STRATEGIES OF CYBER FRAUD

CONCEPT AND TYPE OF CYBER FRAUD

MS HAKIMAH

>>> CONCEPT OF CYBER FRAUD

CYBER FRAUD IS THE CRIME COMMITTED VIA A COMPUTER WITH THE INTENT TO CORRUPT ANOTHER INDIVIDUAL'S PERSONAL AND FINANCIAL INFORMATION STORED ONLINE.

TYPE OF CYBER FRAUD <<<

CYBERCRIMES IN GENERAL CAN BE CLASSIFIED INTO FOUR CATEGORIES:

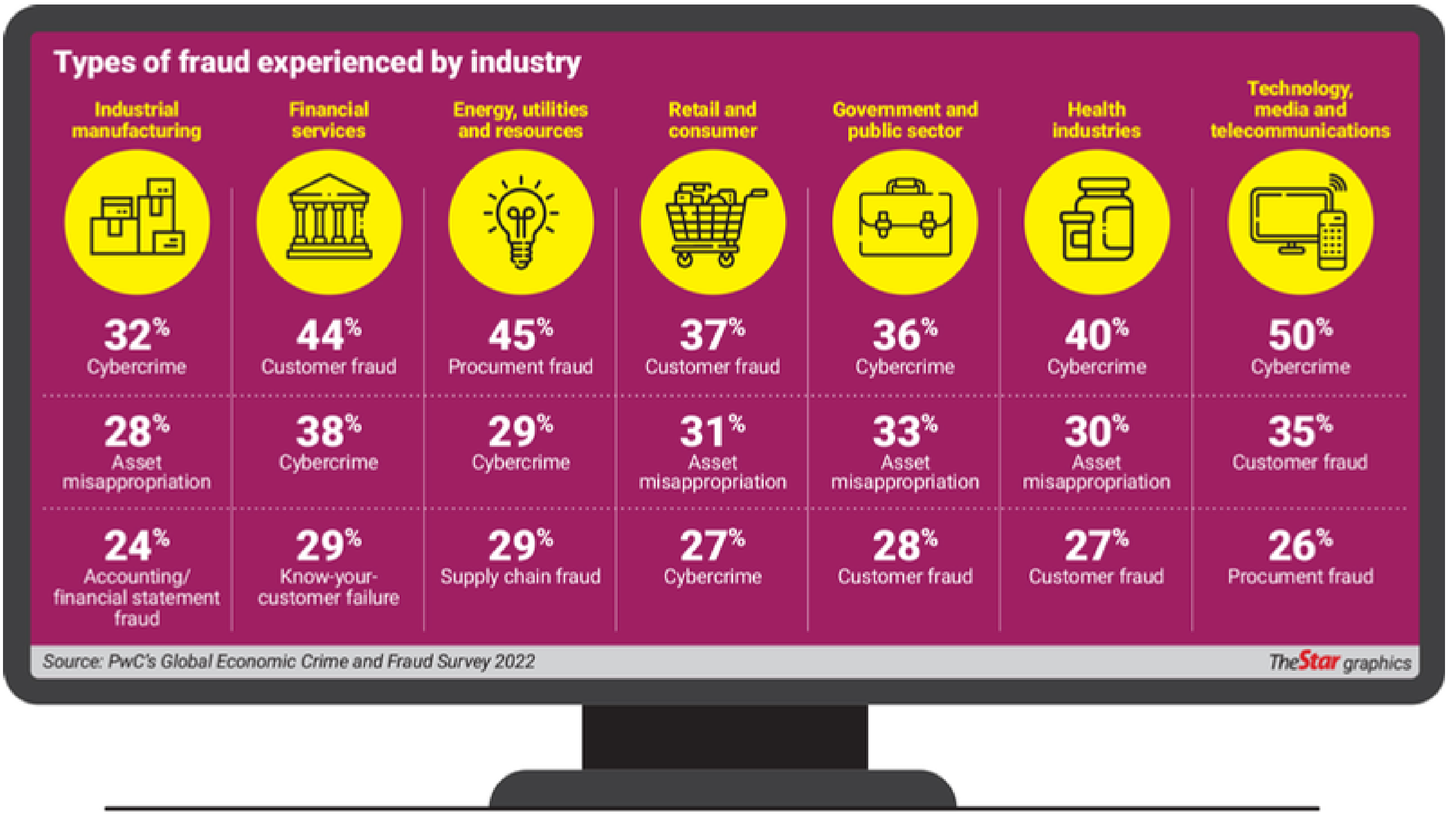
1. INDIVIDUAL CYBER CRIMES:
   - TARGETING INDIVIDUALS.
   - EXAMPLES: PHISHING, SPOOFING, SPAM, CYBERSTALKING, AND MORE.

2. ORGANISATION CYBER CRIMES:
   - TARGET ORGANIZATIONS. USUALLY, THIS TYPE OF CRIME IS DONE BY TEAMS OF CRIMINALS
   - EXAMPLES: MALWARE ATTACKS AND DENIAL OF SERVICE ATTACKS.

3. PROPERTY CYBERCRIMES:
   - TARGETS PROPERTY LIKE CREDIT CARDS OR EVEN INTELLECTUAL PROPERTY RIGHTS.
   - EXAMPLES: COMPUTER VANDALISM, TRANSMISSION OF HARMFUL PROGRAMS, AND UNAUTHORIZED POSSESSION OF COMPUTERIZED INFORMATION.

4. SOCIETY CYBERCRIMES:
   - THIS IS THE MOST DANGEROUS FORM OF CYBERCRIME AS IT INCLUDES CYBER-TERRORISM.

<<< CYBER FRAUD IN MALAYSIA <<<



Types of fraud experienced by industry

Industrial manufacturing	Financial services	Energy, utilities and resources	Retail and consumer	Government and public sector	Health industries	Technology, media and telecommunications
32% Cybercrime	44% Customer fraud	45% Procument fraud	37% Customer fraud	36% Cybercrime	40% Cybercrime	50% Cybercrime
28% Asset misappropriation	38% Cybercrime	29% Cybercrime	31% Asset misappropriation	33% Asset misappropriation	30% Asset misappropriation	35% Customer fraud
24% Accounting/ financial statement fraud	29% Know-your-customer failure	29% Supply chain fraud	27% Cybercrime	28% Customer fraud	27% Customer fraud	26% Procument fraud

Source: PwC's Global Economic Crime and Fraud Survey 2022

TheStar graphics

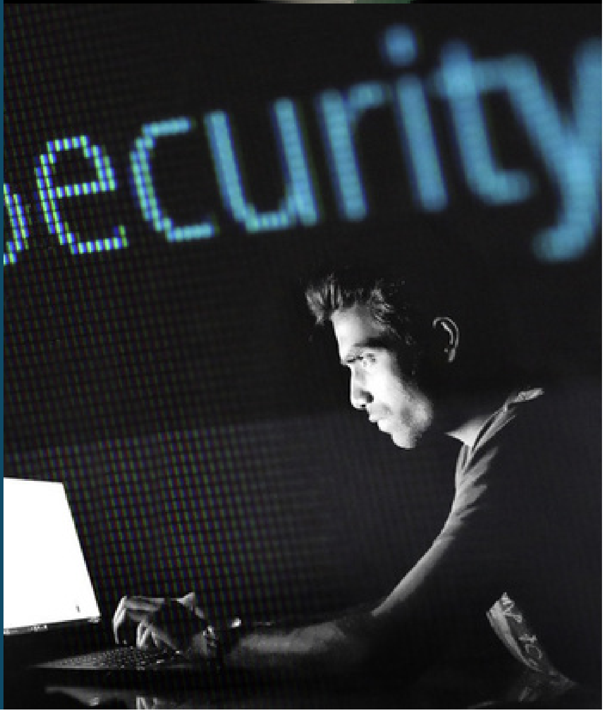
CHARACTERISTIC OF CYBER FRAUD

MS SHALINI

As the internet develops, cybercrime also increases. People who want to engage in illicit behavior now have additional opportunities because to the growth of the Internet and computer technology. In addition to causing a sharp spike in the prevalence of crime, the development of technology and online communication has also led to the appearance of what seem to be certain new types of criminal activity. Law enforcement agencies, as well as the legal systems, face problems from both the rise in the frequency of crime and the potential introduction of new types of crime. The following features apply to cybercrime:

Characteristics of Cyber Crime

- Commission of an illegal act using a computer, its systems, or applications
- Unlawful acts wherein the computer is either a tool or a target or both
- Crimes Perpetrated in Computer Environment
- Criminals are young and smart with technology
- Trans-National /Inter State criminals
- Jurisdiction Issues
- Strong Audit trail
- Mostly non violent crimes
- Veil of Anonymity
- Sometimes difficult to work out



WANNACRY 2017
‘A PERFECT RANSOMWARE STORM’

MS SHIVA

What is WannaCry?

The WannaCry ransomware attack was a worldwide cyberattack in May 2017 by the WannaCry ransomware crypto-worm, which targeted computers running the Microsoft Windows operating system by encrypting data and demanding ransom payments in the Bitcoin cryptocurrency.

How did WannaCry attack happened ?

The attack began on Friday, 12 May 2017, with evidence pointing to an initial infection in Asia at 07:44 UTC. The initial infection was likely through an exposed vulnerable SMB port, rather than email phishing as initially assumed. Within a day the code was reported to have infected more than 230,000 computers in over 150 countries.

Organizations that had not installed Microsoft's security update from May were affected by the attack. Those still running unsupported versions of Microsoft Windows, such as Windows XP and Windows Server 2003 were at particularly high risk because no security patches had been released since May 2014 for Windows XP and July 2015 for Windows Server 2003. A Kaspersky Lab study reported, however, that less than 0.1 per cent of the affected computers were running Windows XP, and that 98 per cent of the affected computers were running Windows 7. In a controlled testing environment, the cybersecurity firm Kryptos Logic found that it was unable to infect a Windows XP system with WannaCry using just the exploits, as the payload failed to load, or caused the operating system to crash rather than actually execute and encrypt files. However, when executed manually, WannaCry could still operate on Windows XP.

Sources: https://www.csoonline.com/article/563017/wannacry-explained-a-perfect-ransomware-storm.html

ONLINE SELLER USING STOLEN IDENTITY ARRESTED FOR CYBERCRIME CASE

MS ZURAIDA

PHILIPPINE NATIONAL POLICE

Regional Anti-Cybercrime Unit 9

Camp Gen. Eduardo B. Batalla, JRT Lim Boulevard, Zamboanga City

www.facebook.com/PNP.ACG.RACU9 racu9.pnpacg@gmail.com +63 998 598 8106

On July 20, 2022 at around 12:10 PM, operatives of the Eastern District Anti-Cybercrime Team (EDACT) arrested a male suspect from Mandaluyong City for using stolen credentials of innocent victims to commit an online scam.

The suspect, identified as Christian O. Sanchez, Jr., posted on Facebook Marketplace the sale of an IPhone 7 mobile phone for Three Thousand Nine Hundred Pesos (Php3,900.00). The victim sent a message to the suspect about his interest to buy the said phone. They closed a deal wherein the phone will be shipped via Lalamove courier. The suspect demanded to pay half of the amount of the phone to push through with their transaction. Further, as proof that the transaction was legit, the suspect asked the victim to send two valid identification cards with a "selfie" while holding the said IDs. When the payment has been made and the IDs were sent, the suspect blocked the victim.

Prior to the arrest, the victim was surprised to learn that his identity and pictures were already circulating online, and had been tagged as a "scammer" on Facebook Marketplace. This prompted him to report the matter to EDACT who immediately launched an entrapment operation after engaging the suspect who was still offering the sale of various gadgets online using the victim's stolen identity. The suspect was arrested at the instance of withdrawing the payment from the victim through a remittance center.

Seized from the possessions of the suspect are: a) three pieces of Php1,000.00 and Php200.00 bills as boodle money; b) one unit of Oppo A5s mobile phone; and c) one identification card.

The suspect will be facing charges for violation of Section 4 (b) 3 (Computer-related Identity Theft) of RA No. 10175 (Cybercrime Prevention Act of 2012).

The suspect will be turned over to Pasig CPS after the conduct of inquest proceedings.

"Muli po kaming nagpapaalala sa ating mga kababayan na huwag pong ibigay sa ibang tao ang ating mga Identification Cards at iba pang pagkakakilanlan dahil nagagamit po ito ng mga cybercriminals upang isakatuparan ang kanilang masamang hangarin. I also commend the efforts of our personnel who engaged the suspect which resulted in his immediate arrest. I am also encouraging all those who had fallen victims by this cybercriminal to immediately report to any PNP-ACG office and lodged a complaint against the arrested suspect."- PBGEN BOWENN JOEY M MASAUDING, THE OFFICER-IN-CHARGE OF PNP-ACG said.

Sources: https://acg.pnp.gov.ph/main/press-releases/468-online-seller-using-stolen-identity-arrested-for-cybercrime-case.html

CYBER FRAUD CASES IN MALAYSIA

MS FARAH

POLICE: 2,079 CASES OF ONLINE FRAUD DETECTED IN JOHOR INVOLVING LOSSES OF OVER RM71M IN 2023 SO FAR

JOHOR BARU, Sept 17 — Online fraud cases in Johor increased by 15.5 per cent to 2,079 cases from January 1 to September 16, compared to 1,800 cases in the same period last year.

Johor Police chief Datuk Kamarul Zaman Mamat said a total loss of RM71.857 million was recorded during the same period this year compared to RM57.026 million last year.

He said most of the cases involved online purchases (485 cases), followed by non-existent investments (382), phone scams (368 cases), job offers (361 cases) and non-existent loans (338 cases).

“A total of 478 out of 2,079 cases were reported by victims to the National Scam Response Centre (NSRC),” he said in a statement today.

Kamarul Zaman called on the public to be more vigilant when conducting dealings online to avoid becoming a victim of fraud.

Police: 2,079 cases of online fraud detected in Johor involving losses of over RM71m in 2023 so far

Kamarul Zaman said the public should first check the phone number and bank account used by the suspect through the “Semak Mule” application provided online by the Commercial Crime Investigation Department (JSJK).

“The public is also urged to always follow JSJK’s social media pages such as on Facebook, Instagram and TikTok to find out the latest modus operandi of commercial crimes.

“If you have become a victim of fraud, please immediately call the NSRC at 997 so that early action can be taken to block the outflow of money from the suspect’s account,” he said.

Sources-BERNAMA, official of Ministry of Communication and Digital

PREVENTION STRATEGIES OF CYBER FRAUD

MS AZLINDA

Preventing cyberattacks effectively requires a comprehensive approach that addresses various aspects of cybersecurity. Here are 10 steps to help you enhance your cybersecurity posture:

Step 1: Incorporate Zero Trust Inspection

Implement a zero-trust security model that verifies and authenticates every user and device trying to access your network or resources.

Utilize encryption and multi-factor authentication (MFA) to enhance security.

Continuously assess the risk, frequency, and impact of potential threats to prioritize security efforts.

Step 2: Outsource Protection Needs to a Cybersecurity Firm

Consider outsourcing your cybersecurity needs to specialized firms with expertise in dealing with cyber threats.

Cybersecurity firms can provide round-the-clock monitoring and incident response, which can be challenging for businesses with limited budgets.

Focus on your core business while professionals handle cybersecurity.

Step 3: Encrypt Data When Sharing or Uploading Online

Use encryption techniques to protect data during transfers, such as Secure Sockets Layer (SSL) or Transport Layer Security (TLS) for website communication.

Choose cloud storage services that offer end-to-end encryption to safeguard your data.

Safeguard decryption keys to prevent data loss.

Implement a Virtual Private Network (VPN) or network encryption via control panel settings to secure data transfers and online interactions.

PREVENTION STRATEGIES OF CYBER FRAUD

MS AZLINDA

Step 4: Regularly Update Software and Systems

Keep all software, operating systems, and applications up to date with the latest security patches.

Enable automatic updates whenever possible to ensure timely protection against known vulnerabilities.

Step 5: Educate and Train Employees

Conduct cybersecurity awareness training for employees to teach them about common threats and safe online practices.

Encourage employees to use strong, unique passwords and enable MFA for their accounts.

Step 6: Implement Network Security Measures

Utilize firewalls, intrusion detection systems (IDS), and intrusion prevention systems (IPS) to monitor and protect your network.

Segment your network to limit lateral movement for attackers.

Step 7: Perform Regular Vulnerability Assessments

Conduct routine vulnerability assessments and penetration testing to identify and remediate weaknesses in your systems and applications.

Step 8: Develop an Incident Response Plan

Create a detailed incident response plan outlining the steps to take in the event of a cyberattack.

Test and refine the plan regularly to ensure it remains effective.

Step 9: Backup Data Regularly

Implement a robust data backup strategy to ensure you can recover quickly from data loss or ransomware attacks.

Store backups offline or in an isolated environment to prevent them from being compromised.

Step 10: Monitor and Audit Activity

Continuously monitor network and system logs for suspicious activity.

Set up alerts for potential security incidents and investigate them promptly.

Remember that cybersecurity is an ongoing process, and threats constantly evolve. Regularly reassess your security measures and adapt them to the changing threat landscape to effectively prevent cyberattacks.

HTTPS://WWW.KNOWLEDGEHUT.COM/BLOG/SECURITY/PREVENT-CYBER-ATTACKS#HOW-TO-PREVENT-CYBER-ATTACKS-EFFECTIVELY?%C2%A0[IN-10%C2%A0STEPS]%C2%A0

FACULTY OF CRIME & INVESTIGATION

ACTIVITIES

A VISIT TO ORPHANAGE

The lecturers and staff of FCI and the students from DCI 19 went to visit the orphanage at Rumah Kebajikan Anak Yatim dan Asnaf An-Naafi. We went for a visit and also to handover the donation from SMART College and surrounding committees. The donation involves monetary,clothes and toys. The student also conducted several activities for the orphans to get to know them better.

FACULTY OF CRIME & INVESTIGATION

ACTIVITIES

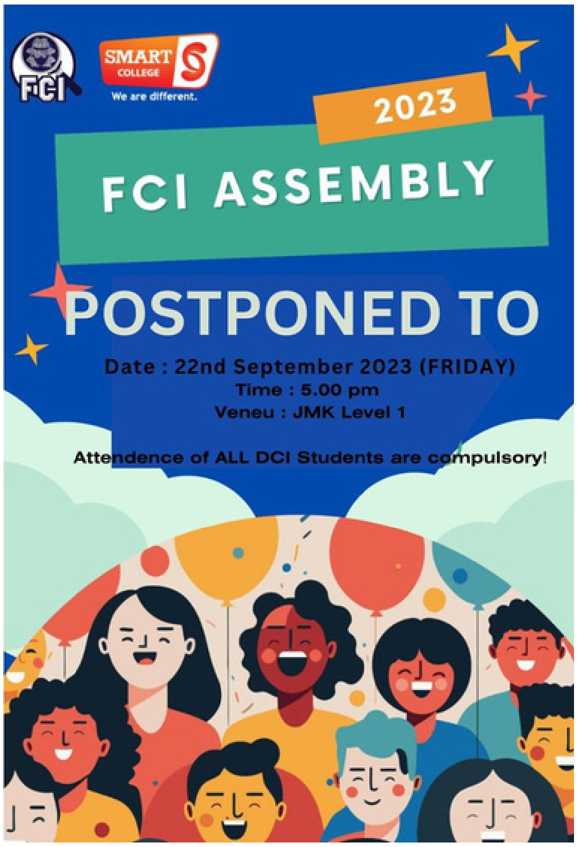
BOOTH FOR HARI MALAYSIA

The students from DCI 20 participated in the booth opening for Hari Malaysia . They prepared and sold several types of food. They also managed to get second place in the booth category for the most sales.

FACULTY OF CRIME & INVESTIGATION

ACTIVITIES

FCI ASSEMBLY



2023

FCI ASSEMBLY

POSTPONED TO

Date : 22nd September 2023 (FRIDAY)

Time : 5.00 pm

Veneu : JMK Level 1

Attendence of ALL DCI Students are compulsory!

The lecturers, staff and students of FCI gathered at JMK to attend the assembly with Head Of Department (HOD), Mr. Sevakumar. The lecturers, staff and students were briefed regarding several matters and activities that will be conducted for the next few months.

FACULTY OF CRIME & INVESTIGATION

STUDENT ACTIVITIES

INTER-FACULTY SPORT DAY

The students of FCI involved in the inter-faculty sport day. They participated in badminton, futsal, and netball. FCI managed to become the winner for the inter-faculty sport day competition for year 2023.

FACULTY OF CRIME & INVESTIGATION

STUDENT ACTIVITIES

Gathering: Ms Azlinda & DCI 14

The lecturers, staff and students from DCI 14 went for gathering at level 1 of SMART college before they went for their internship. They gathered to eat various kind of delicious food prepared by students. Besides, students and lecturers did an exchange gift event as token of appreciation to each others

FACULTY OF CRIME AND INVESTIGATION

Monthly Newsletter

FCI TEAM

MS HAKIMAH
MS LINDA
MS SHIVA
MS SHALINI
MS ZURAIDA
MS FARAH
MS WAHIDA

FOLLOW US ON

SOCIAL MEDIA

FACEBOOK : SMART COLLEGE CRIME AND INVESTIGATION DEPARTMENT

INSTAGRAM : FACULTY_OF_INVESTIGATION

HASHTAG : #FACULTYCRIMEANDINVESTIGATION