Office-Principal
Govt. Jagannath Munnalal Choudhary Mahila Mahavidyalaya, Mandla, Madhya Pradesh

Towards Excellence…

Phone/Fax: 07642-252536 **Email:** hegjcgcman@mp.gov.in
Website: http://www.gjmcgirlscollegemandla.in
AISHE Code: C-33429 **College Code:** 3502

Report

Title of the Programme: 15 Days Certificate Course on "Cyber Crime"

The 15 Days Certificate Course was begun with the welcome speech by the Coordinator of the Course, Dr. Aradhna Dubey (Associate Professor, Home Science; Coordinator, IQAC) after that the patron of the institution and trainer of the course Dr. S.N. Khare in his speech added that there is the demand of time that we should be very careful while using the online facilities in this technical era. He also added that during the course, the participants would be made to know about some preventive measures while using mobile phones, laptops, computer systems for miscellaneous works.

During this course the students were made aware about the following domains of the Cyber Crimes through some news clippings and cuttings:

- Definition and Scope of Cybercrime.
- Historical overview of Cybercrime.
- Categories of Cybercrime (Hacking, Cyber Fraud, Cyber Bullying).
- Legal frameworks and international corporations in combating Cybercrime.
- Techniques and tools for Cybercrime investigation.
- Digital Forensics: collecting and analyzing digital evidence.
- Chain of custody and legal payments in Cybercrime investigations.
- Case studies and practical exercises in Cybercrime investigation.
- Understanding Cybersecurity principles.
- Common vulnerabilities and attack vectors.
- Strategies for preventing cybercrimes (e.g.- Security Awareness Training, Implementing cybersecurity measures.)
- Ethical considerations in cybersecurity and cybercrime.

Further during the course, the trainer elaborately explained the students about:
Cybercrime is criminal activity that either targets or uses a computer, a computer network or a networked device. Most cybercrime is committed by cybercriminals or hackers who want to make money. However, occasionally cybercrime aims to damage computers or networks for reasons other than profit. These could be political or personal.
Cybercrime can be carried out by individuals or organizations. Some cybercriminals are organized, use advanced techniques and are highly technically skilled. Others are novice hackers.

Types of cybercrime include:

- Email and internet fraud.
- Identity fraud (where personal information is stolen and used).
- Theft of financial or card payment data.
- Theft and sale of corporate data.
- Cyberextortion (demanding money to prevent a threatened attack).
- Ransomware attacks (a type of cyberextortion).
- Cryptojacking (where hackers mine cryptocurrency using resources they do not own).
- Cyberespionage (where hackers access government or company data).
- Interfering with systems in a way that compromises a network.
- Infringing copyright.
- Illegal gambling.
- Selling illegal items online.
- Soliciting, producing, or possessing child pornography.

Cybercrime involves one or both of the following:

- Criminal activity targeting computers using viruses and other types of malwares.
- Criminal activity using computers to commit other crimes.

Cybercriminals that target computers may infect them with malware to damage devices or stop them working. They may also use malware to delete or steal data. Or cybercriminals may stop users from using a website or network or prevent a business providing a software service to its customers, which is called a Denial-of-Service (DoS) attack.

Cybercrime that uses computers to commit other crimes may involve using computers or networks to spread malware, illegal information or illegal images.
Cybercriminals are often doing both at once. They may target computers with viruses first and then use them to spread malware to other machines or throughout a network. Some jurisdictions recognize a third category of cybercrime which is where a computer is used as an accessory to crime. An example of this is using a computer to store stolen data.

Examples of cybercrime:

I. Malware Attacks

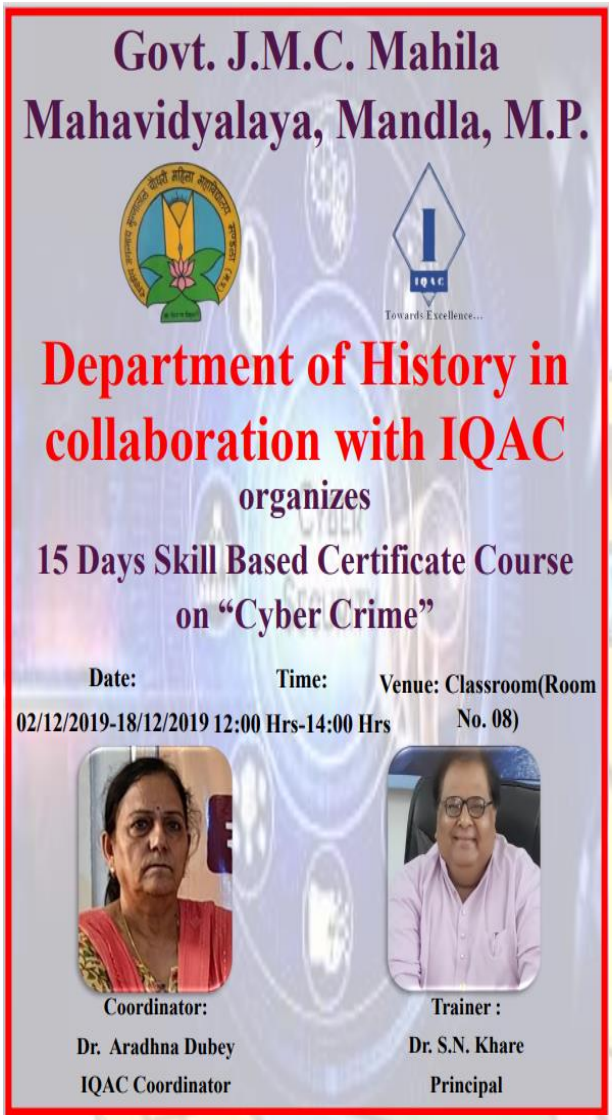
A malware attack is where a computer system or network is infected with a computer virus or other type of malware. A computer compromised by malware could be used by cybercriminals for several purposes. These include stealing confidential data, using the computer to carry out other criminal acts, or causing damage to data.

II. Phishing

A phishing campaign is when spam emails, or other forms of communication, are sent with the intention of tricking recipients into doing something that undermines their security. Phishing campaign messages may contain infected attachments or links to malicious sites, or they may ask the receiver to respond with confidential information.

III. Distributed DoS Attacks

Distributed DoS attacks (DDoS) are a type of cybercrime attack that cybercriminals use to bring down a system or network. Sometimes connected IoT (Internet of Things) devices are used to launch DDoS attacks.
A DDoS attack overwhelms a system by using one of the standard communication protocols it uses to spam the system with connection requests. Cybercriminals who are carrying out cyberextortion may use the threat of a DDoS attack to demand money. Alternatively, a DDoS may be used as a distraction tactic while another type of cybercrime takes place.



Protection against Cybercrimes:

1. Keep software and operating system updated-

Keeping your software and operating system up to date ensures that you benefit from the latest security patches to protect your computer.

2. Use anti-virus software and keep it updated-

Using anti-virus or a comprehensive internet security solution like Kaspersky Premium is a smart way to protect your system from attacks. Anti-virus software allows you to scan, detect and remove threats before they become a problem. Having this protection in place helps to protect your computer and your data from cybercrime, giving you piece of mind. Keep your antivirus updated to receive the best level of protection.

3. Use strong passwords-

Be sure to use strong passwords that people will not guess and do not record them anywhere. Or use a reputable password manager to generate strong passwords randomly to make this easier.

4. Never open attachments in spam emails-

A classic way that computers get infected by malware attacks and other forms of cybercrime is via email attachments in spam emails. Never open an attachment from a sender you do not know.

5. Do not click on links in spam emails or untrusted websites-

Another way people become victims of cybercrime is by clicking on links in spam emails or other messages, or unfamiliar websites. Avoid doing this to stay safe online.

6. Do not give out personal information unless secure-

Never give out personal data over the phone or via email unless you are completely sure the line or email is secure. Make certain that you are speaking to the person you think you are.

7. Contact companies directly about suspicious requests-

If you are asked for personal information or data from a company who has called you, hang up. Call them back using the number on their official website to ensure you are speaking to them and not a cybercriminal. Ideally, use a different phone because cybercriminals can hold the line open. When you think you've re-dialed, they can pretend to be from the bank or other organization that you think you are speaking to.

8. Be mindful of which website URLs you visit-

Keep an eye on the URLs you are clicking on. Do they look legitimate? Avoid clicking on links with unfamiliar or URLs that look like spam. If your internet security product includes functionality to secure online transactions, ensure it is enabled before carrying out financial transactions online.

9. Keep an eye on your bank statements-

Spotting that you have become a victim of cybercrime quickly is important. Keep an eye on your bank statements and query any unfamiliar transactions with the bank. The bank can investigate whether they are fraudulent.

A good antivirus will protect you from the threat of cybercrime. Learn more about Kaspersky Premium.

The certificate course was wrapped up after distribution of the course completion certificates by the trainer of the programme Dr. S.N. Khare (Professor, Department of History) and the coordinator of the course Dr. Aradhna Dubey (Coordinator, IQAC) among the enrolled students.

The number of enrolled as well as the benefitted students was 72.

Trainer and Coordinator
Dr. Aradhna Dubey
(Associate Professor, Home Science)
Coordinator. IQAC

Principal
Govt. Jagannath Prasad Chaudhary
Mahila Mahavidyalaya,Mandla (M.P.)

Principal
Govt. J.M.C. Mahila
Mahavidyalaya,
Mandla. M.P.