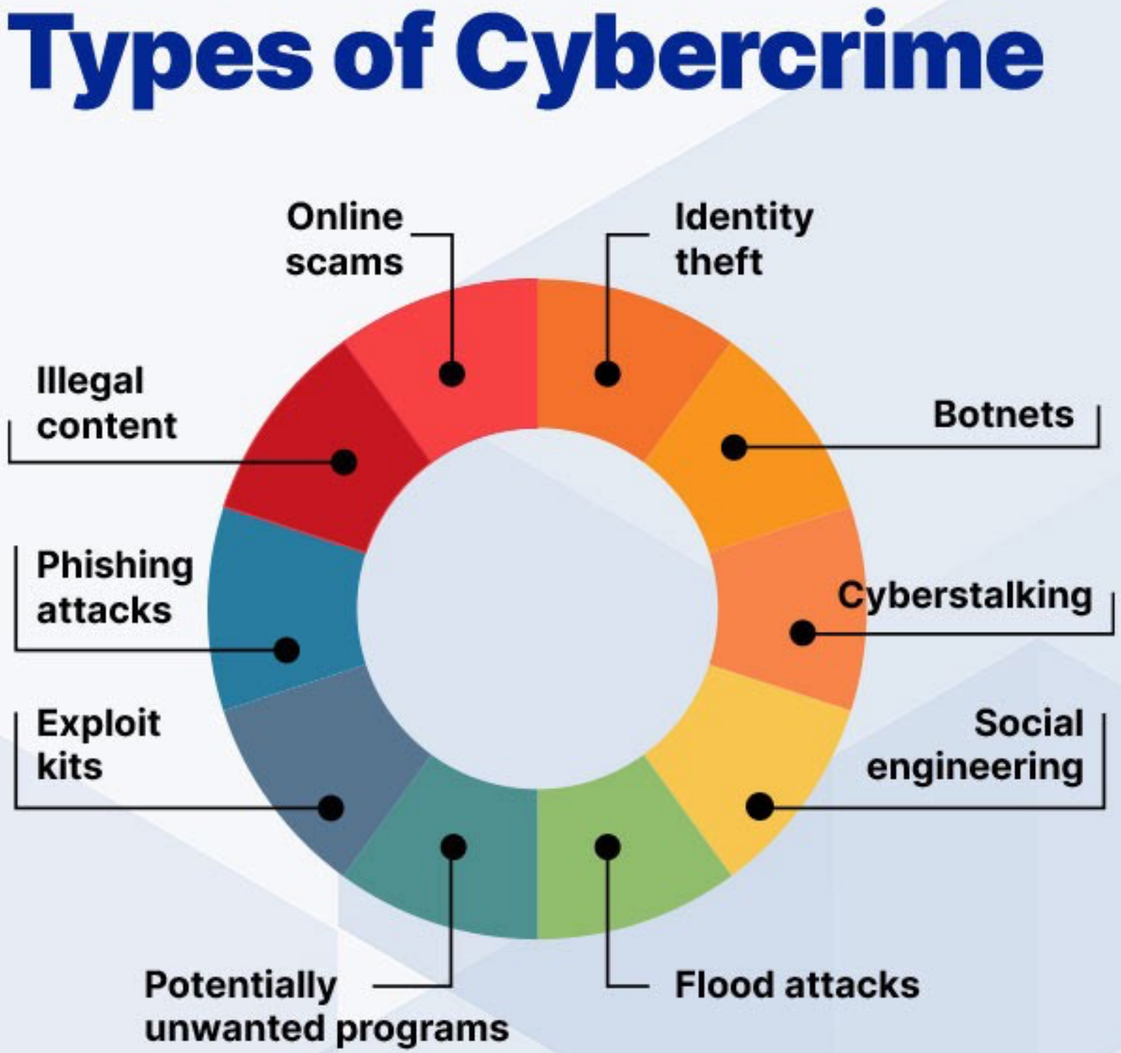
Developing and delivering security awareness training programs

Security Awareness Training

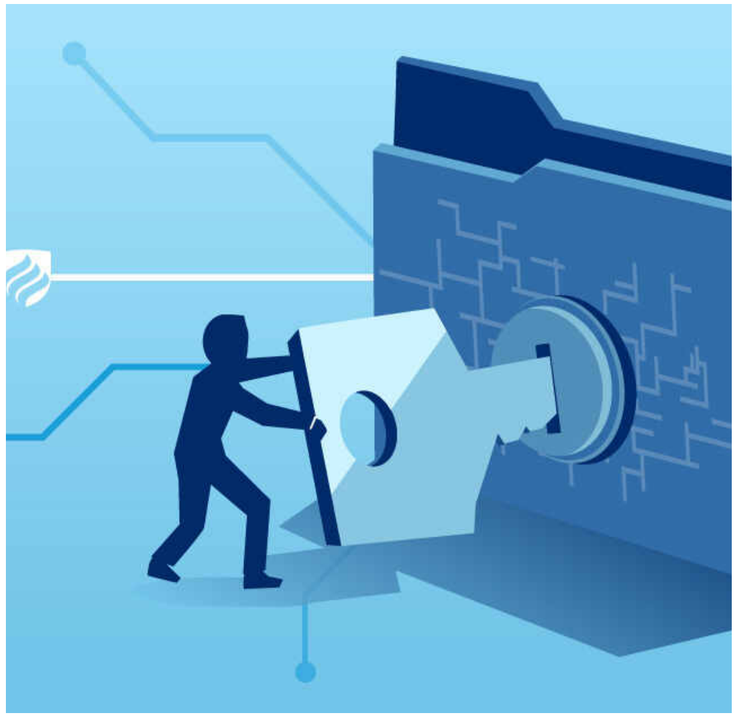
~ Team 8.1



Cybercrimes:

1. *Phishing*
2. *Malware attacks*
3. *Ransomware attacks*
4. *Identity theft*
5. *Online fraud*
6. *Data breaches*
7. *Distributed Denial of Service (DDoS) attacks*
8. *Social engineering attacks*
9. *Cyberstalking*
10. *Online harassment*
11. *Hacking*
12. *Intellectual property theft*
13. *Cyberbullying*
14. *Money laundering*
15. *Online scams*

Good security practices



✓	**Use strong and unique passwords**
	Create complex passwords using a combination of letters (uppercase and lowercase), numbers, and special characters
✓	**Enable two-factor authentication (2FA)**
	This adds an extra layer of security by requiring a second form of verification
✓	**Keep software up to date**
	Regularly update your operating system, web browsers, antivirus software
✓	**Be cautious of phishing attempts**
	Be skeptical of unsolicited emails, messages, or phone calls asking for personal information
✓	**Use secure Wi-Fi connections**
	Avoid using public Wi-Fi for sensitive activities such as online banking or accessing personal accounts

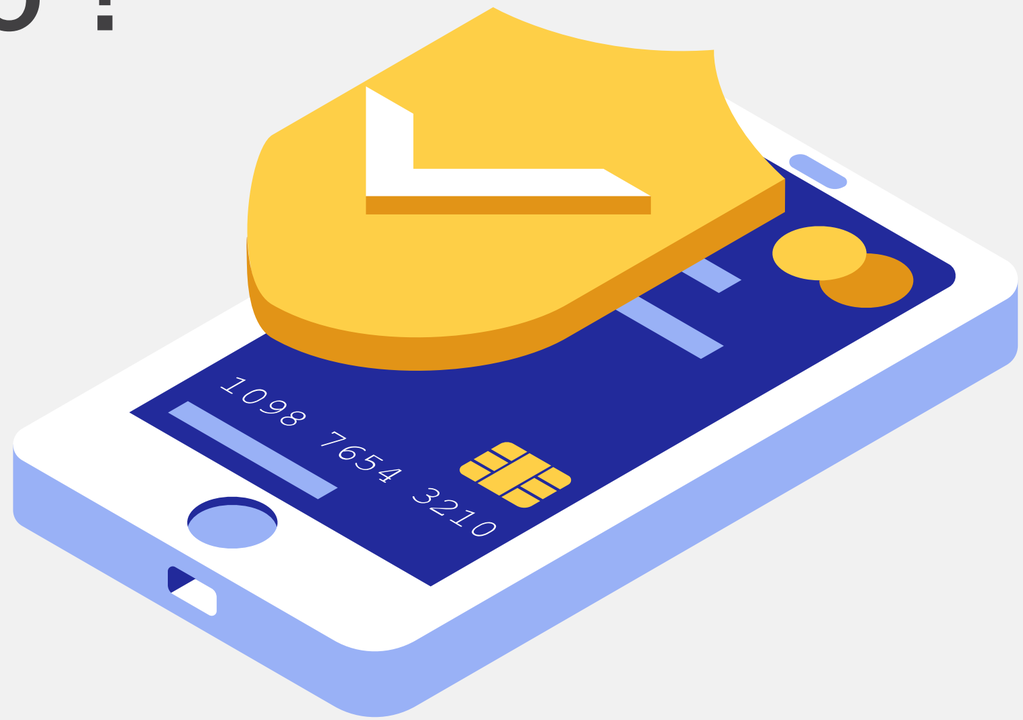
CREDIT/DEBIT CARD FRAUD:

These fraudulent activities aim to steal personal and financial information from unsuspecting individuals.

Card skimming	Online Shopping Fraud	Card-Not-Present (CNP) Fraud:
• Scammers use devices to capture credit or debit card information when you make a payment at an ATM, gas pump, or point-of-sale terminal. • They may install skimming devices or cameras to record your card details or PIN. • Always check for any suspicious attachments or loose parts before using such machines, and cover your hand when entering your PIN.	• When making online purchases, ensure you use reputable and secure websites. Look for "https://" in the website address, indicating a secure connection. • Avoid entering your card details on unsecured or suspicious websites, as they may collect your information for fraudulent purposes.	• CNP fraud occurs when card information is used for online or phone transactions without physical card presence. • Be cautious when sharing your card details over the phone or on online platforms. • Verify the website's security, use trusted vendors, and monitor your statements regularly for any suspicious activity.

what should victims do ?

- Many banks offer card blocking features and transaction alerts through mobile apps or online banking.
- Enable these features to receive real-time notifications about card usage and to block your card in case of loss or theft.



Also they should immediately report to the nearby cyber cell

INTERNET BANKING FRAUD:

These fraudulent activities are aimed at stealing personal and financial information related to online banking accounts.

Phishing

- A fraudster might send an email to a bank customer, posing as a bank representative.
- The email may claim that there is an issue with the customer's account and provide a link to a fake website that looks identical to the bank's official site.
- If the customer enters their login credentials on the fake site, the fraudster can capture the information and gain access to the customer's account.

Keylogger attack

- A user may unknowingly download a malicious software program, such as a Trojan horse or a keylogger, onto their device.
- The malware can record keystrokes and capture login credentials when the user accesses their online banking account.
- The fraudster can then use the stolen information to gain unauthorized access to the account and carry out fraudulent transactions.

Preventive measures

Monitor Account Activity:

Regularly review your bank statements and transaction history to detect any unauthorized activity. Report any suspicious transactions or discrepancies to your bank immediately.

Verify Requests:

Be cautious of any unexpected requests or changes related to your online banking account. Verify such requests directly with your bank through official contact channels before taking any action.

Educate Yourself:

Stay informed about the latest online banking fraud techniques and scams. Regularly educate yourself about best practices for online security and fraud prevention.

SMSHING:

SMShing: SMShing (SMS phishing) is a type of cyber attack where fraudsters use text messages (SMS) to deceive individuals into disclosing sensitive information or performing malicious actions.

Fake Messages:	Deceptive Techniques:	Red Flags:
• Fraudsters send text messages that appear to be from a legitimate source, such as a bank or a trusted organization. • These messages often contain urgent requests, offers, or alerts to trick recipients into taking immediate action.	• SMShing messages may contain links that direct users to malicious websites or prompt them to reply with personal information like passwords, account numbers, or verification codes. • Their goal is to gain access to sensitive data for fraudulent purposes.	• Be cautious of messages that create a sense of urgency, demand immediate action, or offer unrealistic rewards. • Poor grammar, spelling mistakes, or unfamiliar sender numbers can also indicate a potential SMShing attempt.

Preventive measures

Avoid clicking on links:

Do not click on links or open attachments in text messages, especially if they are from unfamiliar or suspicious sources. These links may lead to fraudulent websites or trigger malware downloads.

Verify Requests:

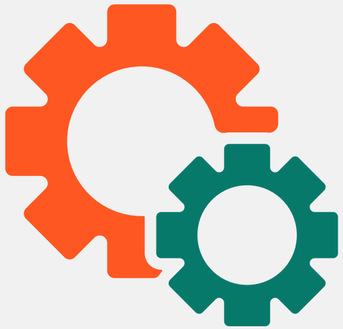
If you receive a text message asking for sensitive information or requesting action, such as providing account details or clicking a link, do not respond directly.

Register for SMS alerts:

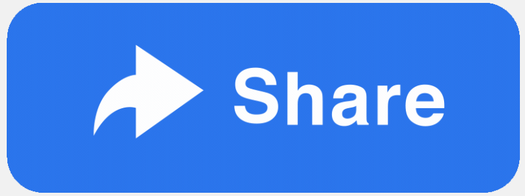
Consider signing up for SMS alerts from your bank or financial institution. This way, you can receive legitimate transaction notifications and quickly identify any unauthorized activity.

DIGITAL FOOTPRINT:

A digital footprint refers to the traces and information that individuals leave behind when they engage in online activities. It includes the data and information about an individual that is collected, stored, and shared online.



Permanent Nature:	Personal Information:	Social Media Privacy Settings:
• Digital footprints are often permanent and can be difficult to erase completely. • Information shared online, such as social media posts, comments, or photos, can be archived, shared, or retrieved even after deletion.	• Be mindful of the personal information you share online. • Avoid sharing sensitive details like your full name, address, phone number, social security number, or financial information in public or untrusted online platforms.	• Review and adjust the privacy settings on your social media accounts. • Limit the visibility of your personal information, posts, and photos to only trusted individuals or friends, rather than having them accessible to the public.



Online Reputation:	Oversharing:	Online Tracking:
• Your digital footprint contributes to your online reputation. • Employers, colleges, and others may assess your online presence to make judgments about your character and suitability. • Be mindful of the content you post and consider how it may be perceived by others.	• Avoid oversharing personal information or intimate details about your life online and keep your social media accounts private. • Fraudsters can exploit such information for identity theft, social engineering, or targeted attacks.	• Understand that various online services, websites, and advertising networks may track your online activities to gather data for targeted advertising. • Use browser settings or extensions to manage or block tracking, if desired.


Thank you!