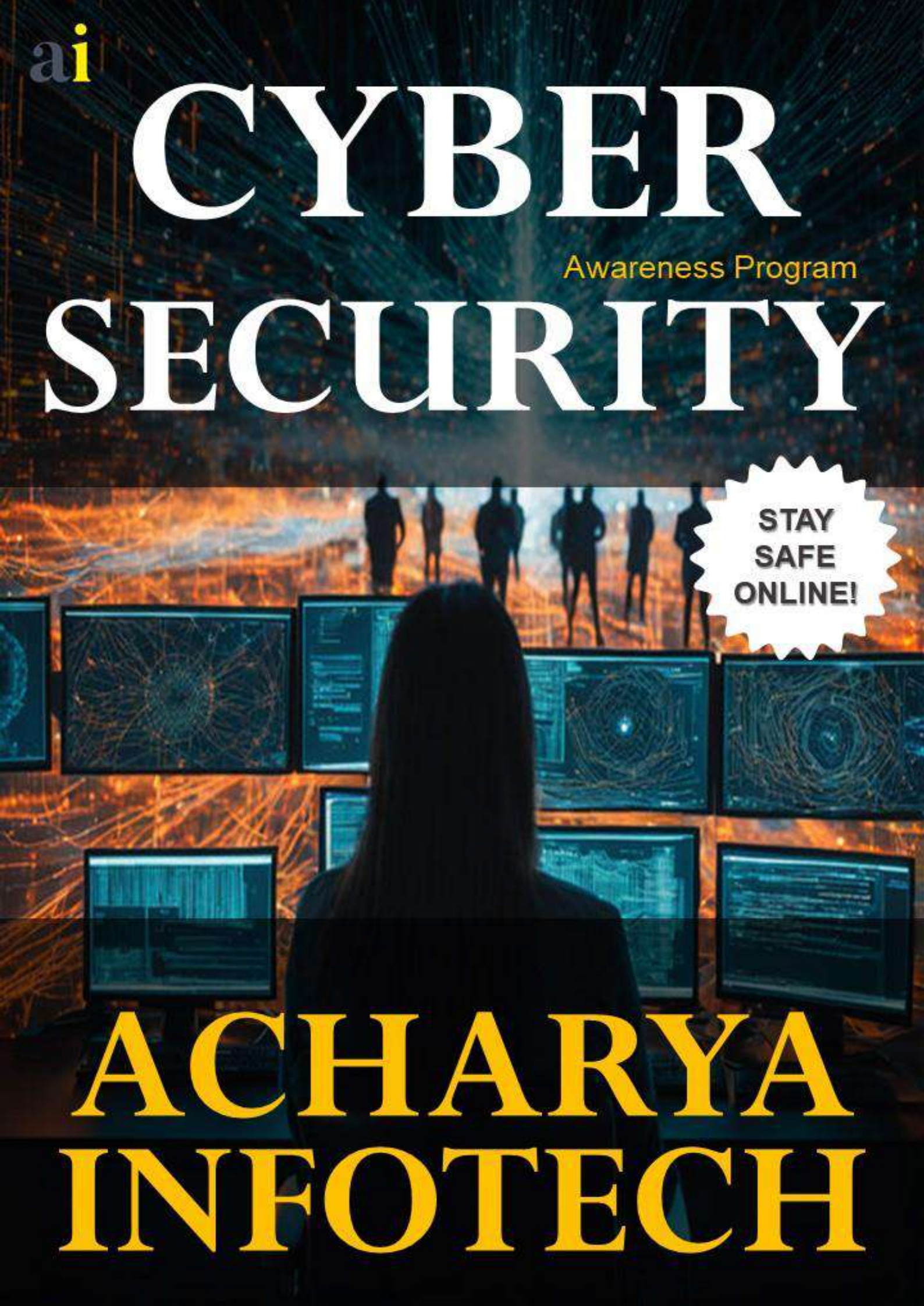
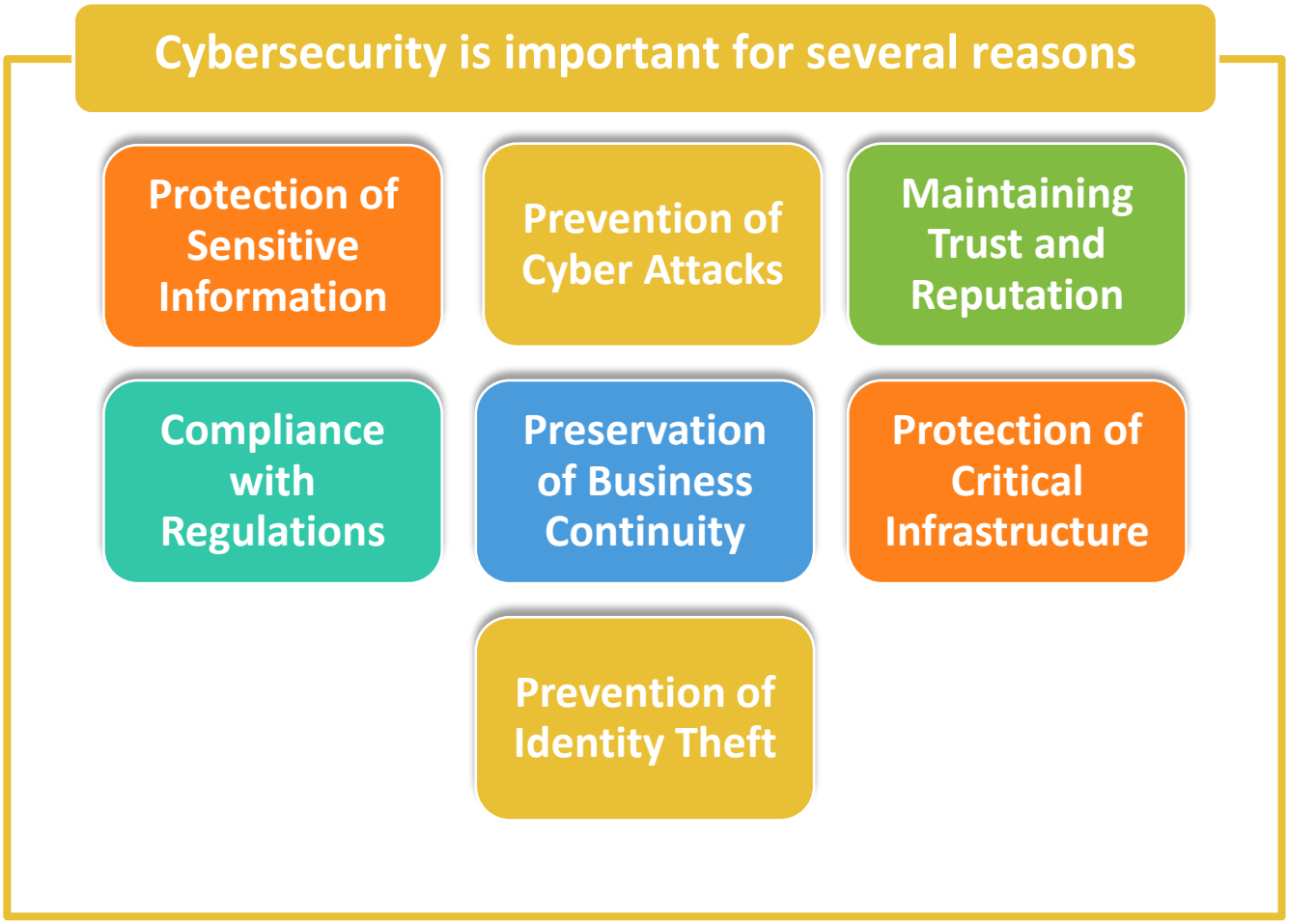

ai
CYBER
Awareness Program
SECURITY
STAY
SAFE
ONLINE!
ACHARYA
INFOTECH

Introduction to Cybersecurity

What is Cybersecurity?

Cybersecurity refers to the practice of protecting internet-connected systems, including hardware, software, and data, from cyber threats. These threats can come in various forms, such as hacking, malware, phishing, ransomware, and other malicious activities.

Why is Cybersecurity Important?



Real-life Examples of Cyber Threats

Understanding Online Risks

1 Identity Theft

Identity theft is a form of cybercrime in which someone wrongfully acquires and uses another person's personal information, typically for financial gain or to commit fraud. This stolen information may include the victim's name, Social Security number, date of birth, credit card numbers, bank account details, and other sensitive data.

2 Phishing Attacks

Phishing attacks are a type of cyber-attack where perpetrators attempt to deceive individuals into providing sensitive information, such as login credentials, financial details, or personal data. These attacks typically involve sending fraudulent emails, messages, or websites that appear legitimate and trustworthy to the recipient.

3 Malware and Viruses

Malware and viruses are both types of malicious software designed to disrupt, damage, or gain unauthorized access to computer systems or networks, but they have distinct characteristics:

1. Malware (malicious software): Malware is a broad term that encompasses various types of malicious software designed to perform harmful actions on a computer system or network. It includes viruses, worms, Trojans, ransomware, spyware, adware, and other types of malicious programs.

2. Viruses: Viruses are a specific type of malware that replicate themselves by infecting other files or programs on a computer. They attach themselves to executable files or documents and spread when the infected files are executed or opened.

4 Social Engineering

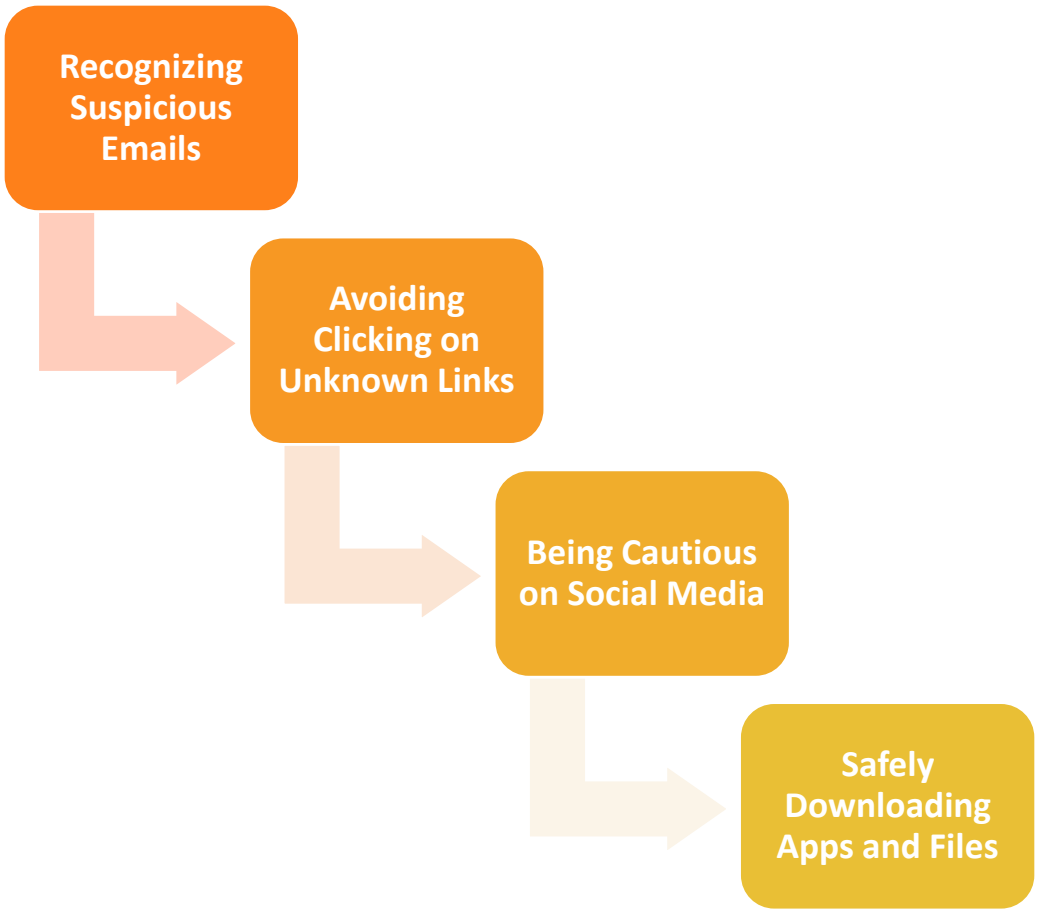
Social engineering is a technique used by cybercriminals to manipulate individuals into divulging confidential information, performing actions, or divulging information that compromises security protocols.

Protecting Your Devices

Follow these Instructions:

Safe Internet Practices

Follow these Instructions:



Social Media and Cyberbullying

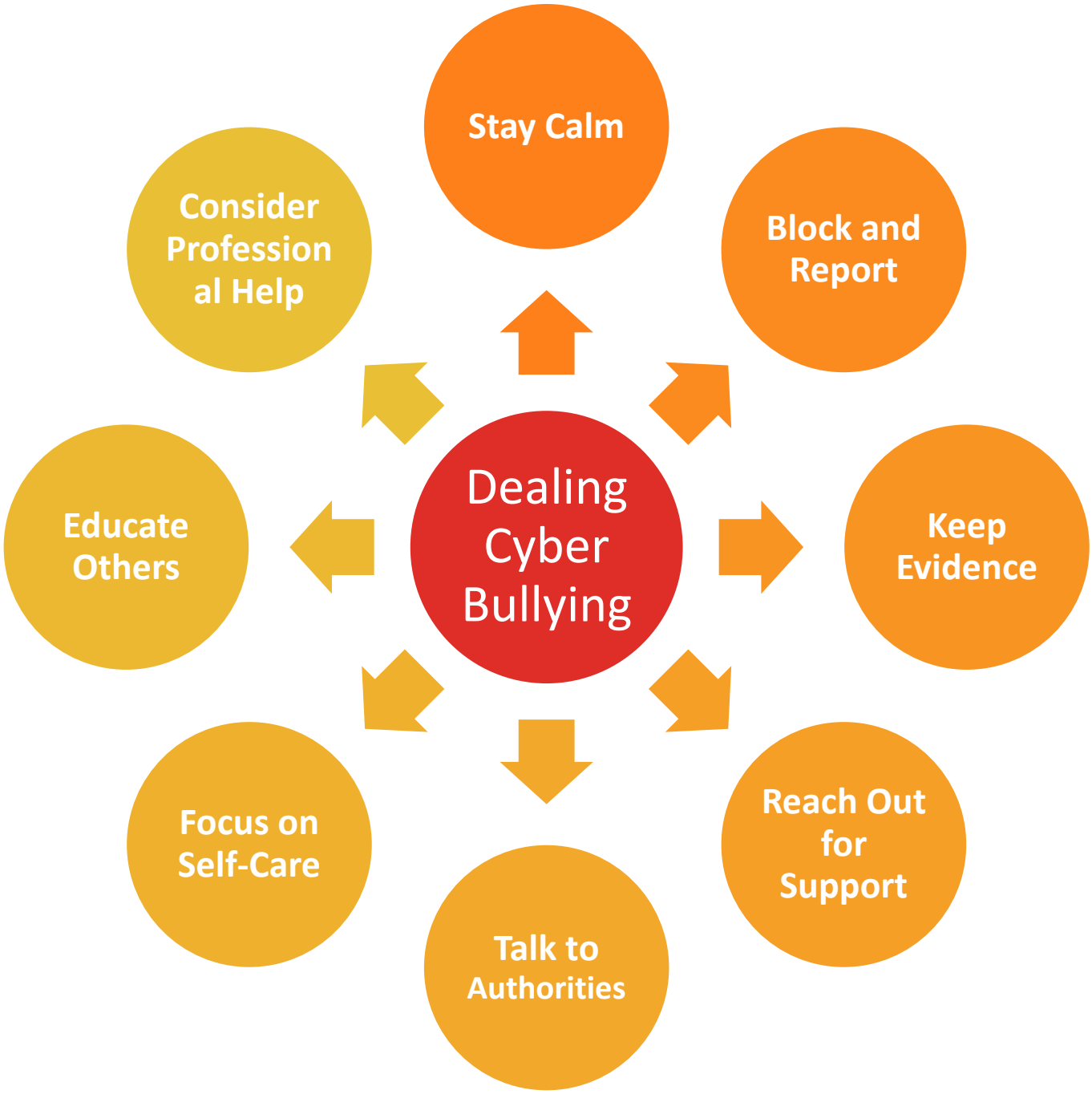
Cyberbullying involves using technology, such as social media, messaging apps, or online forums, to harass, embarrass, or harm others. This can include spreading rumours, sharing hurtful comments or images, or repeatedly sending threatening messages.

Recognizing Cyberbullying

Recognizing cyberbullying is crucial for identifying and addressing harmful online behaviour. Here are some key indicators to help recognize cyberbullying:

Dealing with Cyberbullies

Dealing with cyberbullies can be challenging, but there are strategies you can use to protect yourself and address the situation effectively. Here are some tips:



Protecting Your Online Reputation

Protecting your online reputation is essential in today's digital age. Here are some strategies to help safeguard your online image:

1. Think before you post: Before sharing any content online, consider how it may impact your reputation. Avoid posting anything that could be perceived as offensive, inappropriate, or damaging to your image.

2. Use privacy settings: Familiarize yourself with the privacy settings on social media platforms and adjust them to control who can see your posts and information. Limiting your audience can help protect your privacy and reputation.

3. Monitor Your Digital Footprint: Regularly monitor your online presence by searching for your name on search engines and social media platforms. If you come across any negative or unwanted content, take steps to address it promptly.

4. Be Selective About Friends and Connections: Be cautious about accepting friend requests or connections from individuals you don't know or trust. Adding people indiscriminately can expose you to potential risks and damage your reputation.

5. Secure Your Accounts: Use strong, unique passwords for your online accounts and enable two-factor authentication whenever possible. This helps prevent unauthorized access to your accounts and protects your personal information.

6. Think Twice Before Engaging in Online Arguments: Avoid getting involved in heated debates or arguments on social media. Engaging in online conflicts can escalate quickly and reflect poorly on your reputation.

7. Maintain Professionalism: Whether you're using social media for personal or professional purposes, always maintain a professional tone and demeanour. Avoid posting anything that could be construed as unprofessional or disrespectful.

8. Respond Wisely to Negative Feedback: If you receive negative feedback or criticism online, respond calmly and professionally. Address the issue constructively, and avoid getting defensive or engaging in arguments.

9. Regularly Update Your Privacy Settings: Stay informed about changes to privacy policies and settings on social media platforms, and update your settings accordingly. This helps ensure that you maintain control over who can access your information.

Be a responsible digital citizen

Being responsible digital citizens means engaging in online activities in a safe, ethical, and respectful manner. Here are some key aspects of responsible digital citizenship:

1. Respecting others: Digital citizens should treat others with respect and kindness in online interactions, avoiding cyberbullying, harassment, or spreading hate speech.

2. Protecting privacy: Responsible digital citizens should be mindful of their online privacy and take steps to protect their personal information from unauthorized access or misuse.

3. Promoting digital literacy: Digital citizens should strive to improve their digital literacy skills, including critical thinking, media literacy, and online safety awareness, to navigate the digital landscape effectively.

4. Fostering positive relationships: Building positive and supportive relationships online contributes to a healthy digital community. Digital citizens should engage in constructive dialogue, collaborate with others, and foster a sense of belonging and inclusivity.

5. Practicing cybersecurity: Responsible digital citizens should practice good cybersecurity habits, such as using strong passwords, keeping software up to date, and being cautious of phishing scams, to protect themselves and others from cyber threats.

6. Respecting intellectual property: Digital citizens should respect intellectual property rights, including copyrights, trademarks, and patents, and avoid unauthorized use or distribution of copyrighted materials online.

7. Contributing positively: Responsible digital citizens should use their online platforms and voices to contribute positively to society, whether by sharing valuable information, raising awareness about important issues, or advocating for social change.

8. Being critical consumers: Digital citizens should critically evaluate the information they encounter online, fact-check sources, and avoid spreading misinformation or disinformation that can harm individuals or society.

9. Modelling good behaviour: Responsible digital citizens should lead by example and model good online behaviour for others, especially younger generations, by demonstrating integrity, empathy, and ethical conduct in their online interactions.

10. Promoting digital citizenship education: Lastly, digital citizens should advocate for and support initiatives that promote digital citizenship education in schools, workplaces, and communities to empower individuals with the knowledge and skills needed to navigate the digital world responsibly.

By embodying these principles of responsible digital citizenship, individuals can contribute to creating a safer, more inclusive, and positive online environment for themselves and others.

Stay Safe Online.

We have

GREAT NEWS

Challenge Yourself!!

Participate in "Cyber Security Awareness Quiz" and get instant certificate on your mail ID.

https://forms.gle/JYNvRiG4NHTxZa

ACHARYA INFOTECH

+91 967 - 230 - 1234