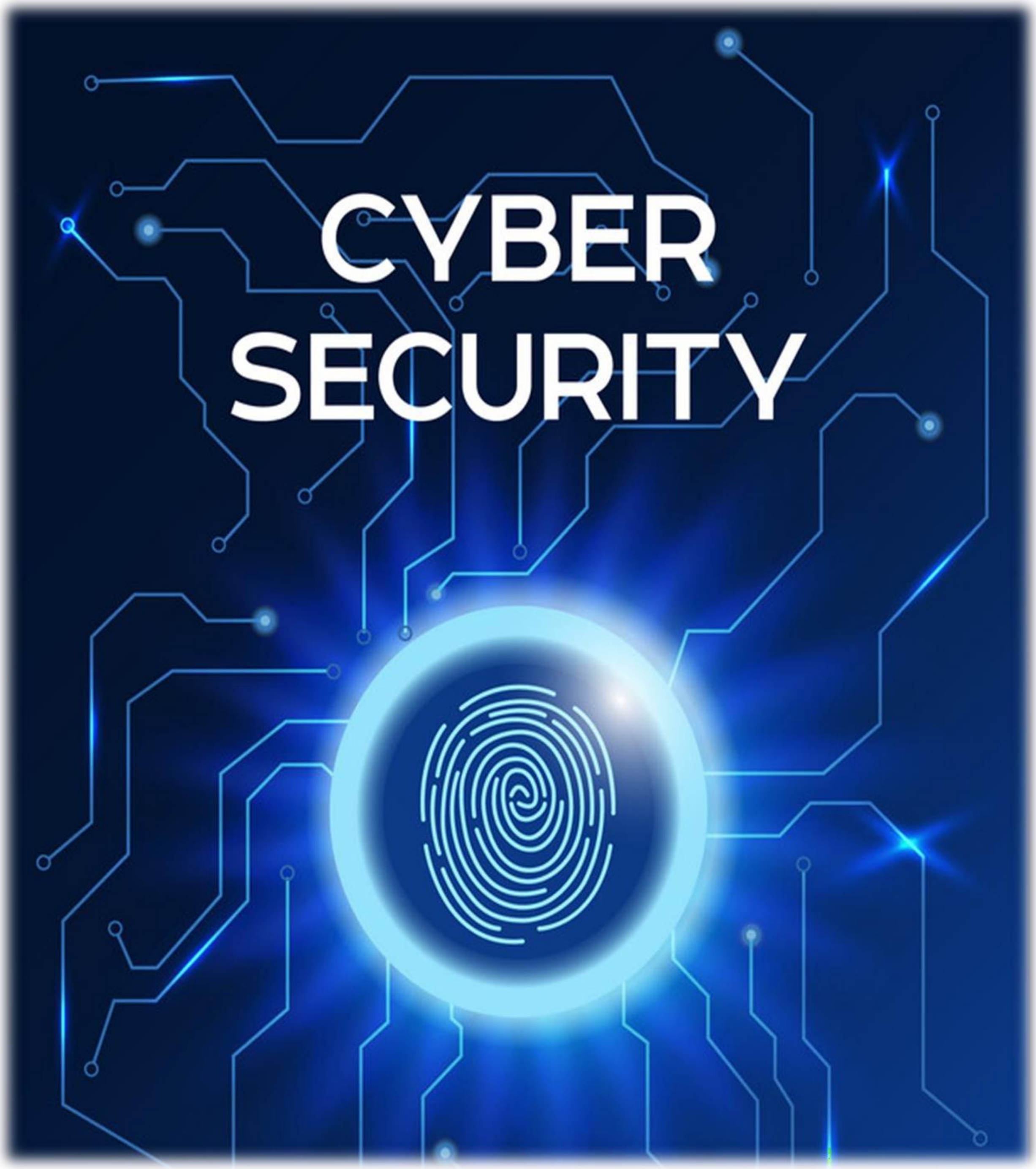
UTKAL UNIVERSITY



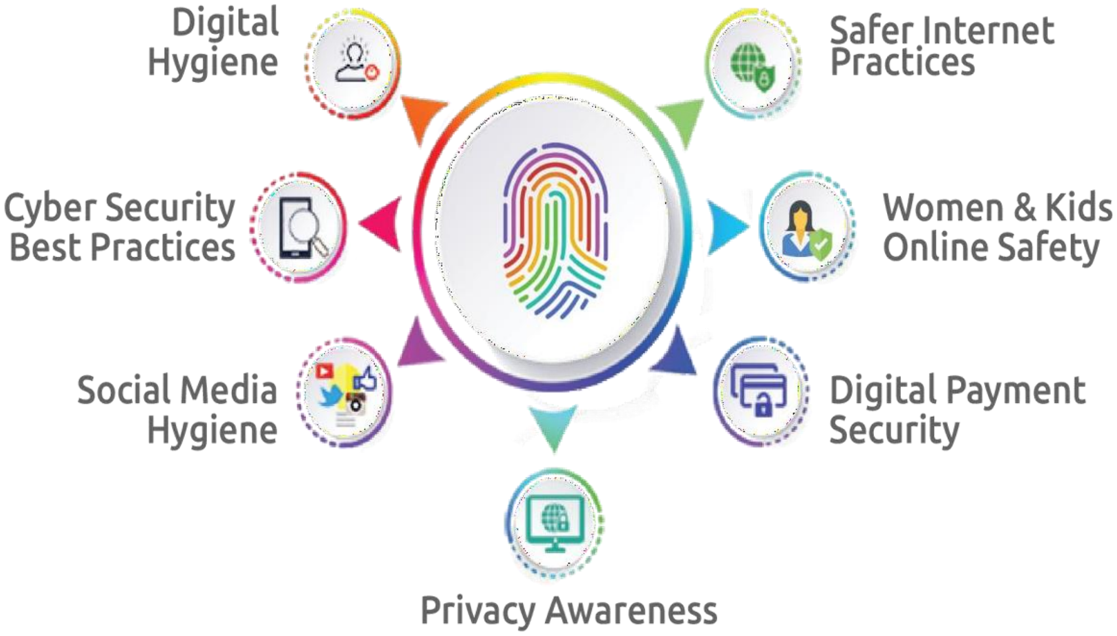
CYBER SECURITY

CYBER SECURITY

Compiled By:

Dr. Mrutyunjaya Panda, Associate Professor, Utkal University
Dr. Sanjaya Kumar Sarangi, Academic Coordinator, Utkal University

In day-to-day life, everyone is leading their life with technology. Our daily life depends on technology. So, nowadays everybody knows the internet and is aware of it. The Internet has everything that a man needs in terms of data. So, people are becoming addicted to the Internet. The percentage of the population using the internet is increasing day by day. National security is in some way getting dependent on the internet. But the new technologies that have arrived also brought unusual threats and Cyber-Crime is one such concept. Cyber-Crime is a crime that uses a computer for an attack like hacking, spamming, etc.



Cyber Security & Forensics

Due to the surge in Internet astuteness and exponential growth in IT infrastructure in recent times, the attackers try to find ways and means to invade critical infrastructure and pose an immense threat to people or organization by securing sensitive information from credit card, transactions through smartphones or any other financial intelligence.

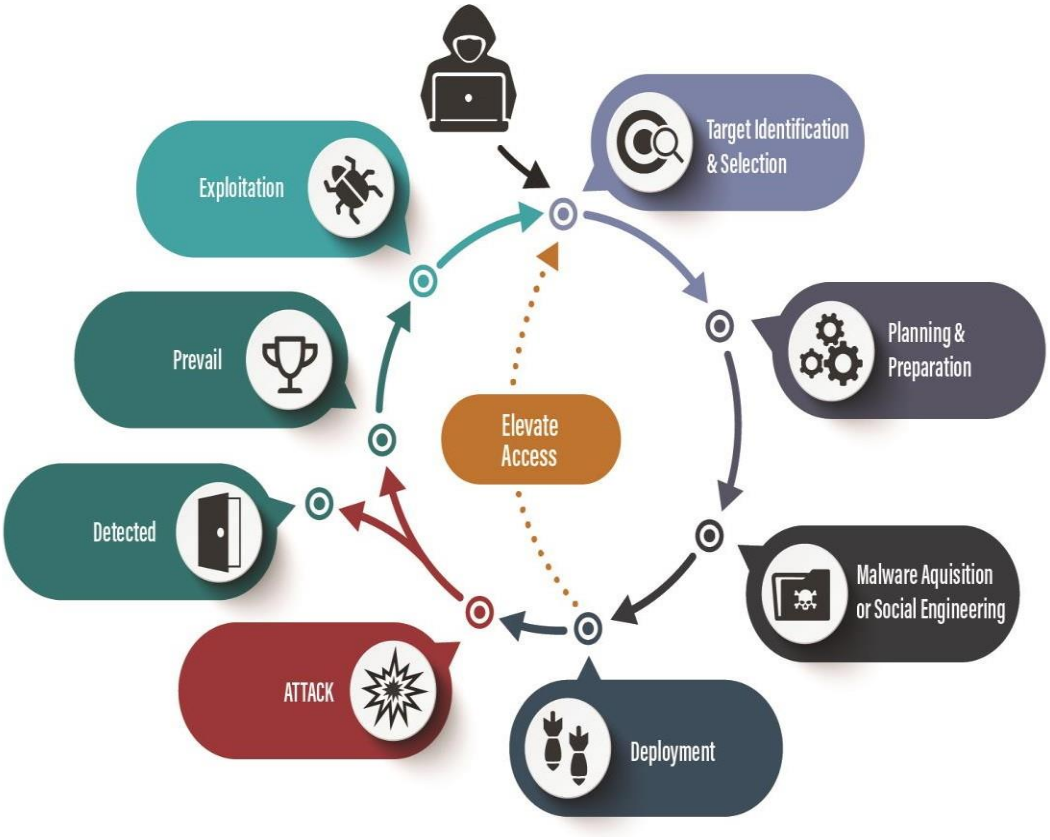
Smartphone attacks are growing in multiple folds nowadays. At the same time, with the growth of 4G and upcoming 5G services, the future of smart education, smart cities, smart homes, smart healthcare, and intelligent transportation systems which depend heavily on billions of connected IoT (Internet of Things) devices are vulnerable to cyber threats due to non-availability standard regulation. Due to this lack of organization and regulation at the present time, manufacturers often inadvertently vessel malware in IoT devices which allows hackers to manipulate the connected cameras or hold smart homes to ransom through cyber threats. Further, as most of these IoT traffic are not encrypted, so there is always a chance for the cybercriminals to penetrate through the 5G network to malfunction the network devices and system which may pose threats to national security. It can also be envisioned from the recent cyber-attacks during 2016, how the cybercriminals could stall the internet services of Amazon, Wall Street Journal, Twitter and CNN etc.,using DDOS (Distributed Denial of Service) attack and caused huge financial losses to them.

Hence, In order to make our IT infrastructure resilient against these cyber threats now and in the future, awareness amongst the general public and all the stakeholders of the Utkal University about the menace of Cyber Securityis the need of the hour.

In the following sections, information is shared to understand the basics of cyber security and its causes, types of cyber-crime and their countermeasures by all stakeholders of the University to identify and prevent cyber threats.

A. Introduction about Cyber-crime:

Cyber-crime is nothing but all illegal activities which are carried out using technology. Cyber-criminals hack user's personal computers, smartphones, personal details from social media, business secrets, national secrets, important personal data, etc with the help of the internet and technology. Hackers are the criminals who are performing these illegal, malicious activities on the internet. Though some agencies are trying to tackle this problem, it is growing regularly and many people have become victims of identity theft, hacking, and malicious software. Let's find out more about cyber-crimes.



B. Causes of Cyber Crime:

To earn a huge amount of money, Cyber-criminals always choose an easy way. Banks, casinos, companies, and, financial firms are prosperous organizations, and their target centers where an enormous amount of money runs daily and have diplomatic information. It's very difficult to catch those criminals. Hence, the number of cyber-crimes is increasing day by day across the globe. We require so many laws to protect and safeguard them against cyber-criminals since the devices we use every day for businesses and communication might have vulnerabilities that can be exploited. We have listed some of the reasons:

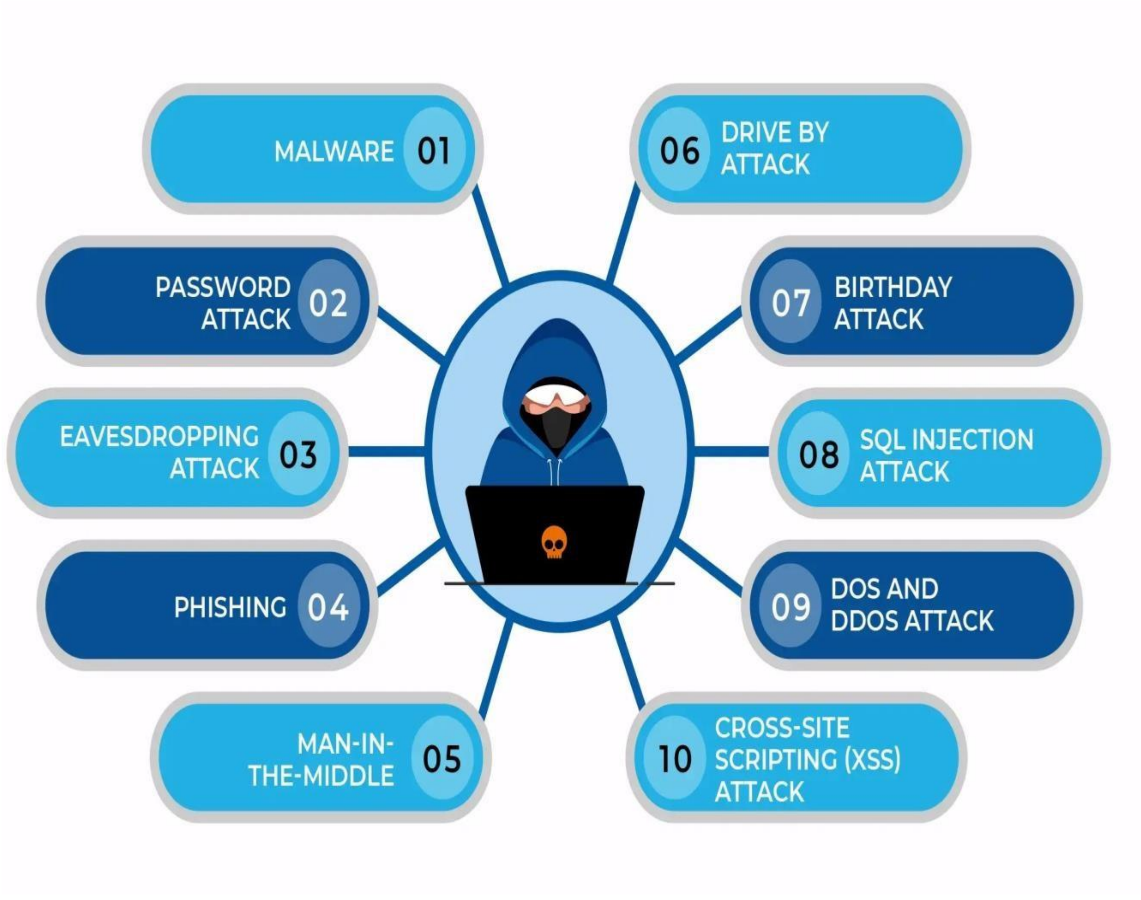
1. **Easy to access computers:**
   Since technology is complex, it has become very difficult to protect the computer from viruses and hackers. There are so many possibilities for hacking when we safeguard a computer system from unauthorized access. Hackers can steal access codes, retinal images, advanced voice recorders, etc.which can mislead the bio-metric systems easily and can be utilized to get past many security systems by avoiding firewalls.

2. **Size to store computer data in comparatively small space:**
   The computer has a distinctive feature of storing data in a very small space. Due to this, people can steal data very easily from any other storage and use this for their purpose.

3. **Complexity of Code:**
   The computers can run on operating systems and these operating systems are programmed with millions of codes. There might be mistakes in the code. The human brain is defective so they can commit mistakes at any stage. The cybercriminals take advantage of these loopholes.

4. **Negligence of the user:**
   Human beings always neglect things. So, if we make any negligence in protecting our computer system it leads the cyber-criminals to access and control over the computer system.

5. **Loss of evidence:**
   Hackers always make sure to clear any evidence i.e. log data related to the attack. So, Loss of evidence has turned into an evident problem that disables law enforcement to go beyond the investigation of cybercrime.



C. Types of cyber-crimes which are explained below:

1. **Hacking:**
   It defines sending illegal instructions to any other computer or network. In this case, a person’s computer is hacked so that sensitive information can be retrieved. The criminal uses a variety of software to break into a person’s computer and the person may not know that his computer is being accessed from a remote location. Government websites are strong prey for hackers. Ethical hacking is different from this and is used by many organizations to check their Internet security protection.

2. **Children's pornography and their Abuse:**
   The internet is being enormously used to abuse children. This is a type of cybercrime where criminals exploit minors through chat rooms with the intention of child pornography. The Cybersecurity sector of each nation is spending an excess of time supervising chat rooms frequently visited by children with the belief of minimizing and preventing child abuse and soliciting.

3. **Plagiarism or Piracy or Theft:**
   This crime happens when a person disobeys copyrights and downloads music, movies, games, and software. There are even peer sharing websites that stimulate software piracy and many of the other websites are now being aimed by the FBI. Nowadays, the judicial system is addressing the cyber-crime and there are so many laws that stop people from illegal downloading. Film producers and directors frequently become a martyr of this crime.

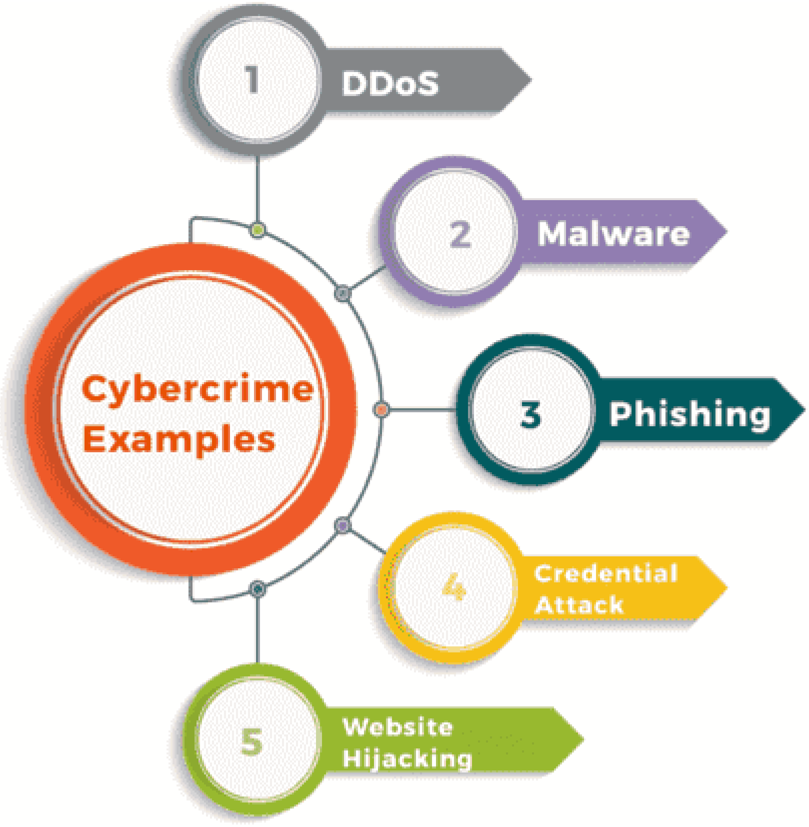
4. **Cyber Stalking:**
   This is an online harassment where the victim is exposed to a cascade of online messages and emails. Typically, these stalkers know their victims and instead of offline stalking, they will use the Internet to stalk. Although, if they notice that cyber-stalking is not having the effect which they have desired, then they begin offline stalking along with cyber-stalking to make sure that victim’s survival is more depressed.

5. **Cyber Terrorism:**
   Cyber terrorism is also known as information wars and can be defined as an act of Internet terrorism which contains cautious and large-scale strikes and disturbances of computer networks using computer viruses or the physical attacks using malware to strike individuals, governments and other organizations. The aim of terrorists is to produce a sense of terror in the brains of the victims. Maintaining this idea in mind, it enhances a simple way to modify the cyber-attacks for a financial or egotistical and achieve from acts of cyber terrorism. Cyber terrorists drive with the aim of harm and demolition at the forefront of their activities like a vanguard.

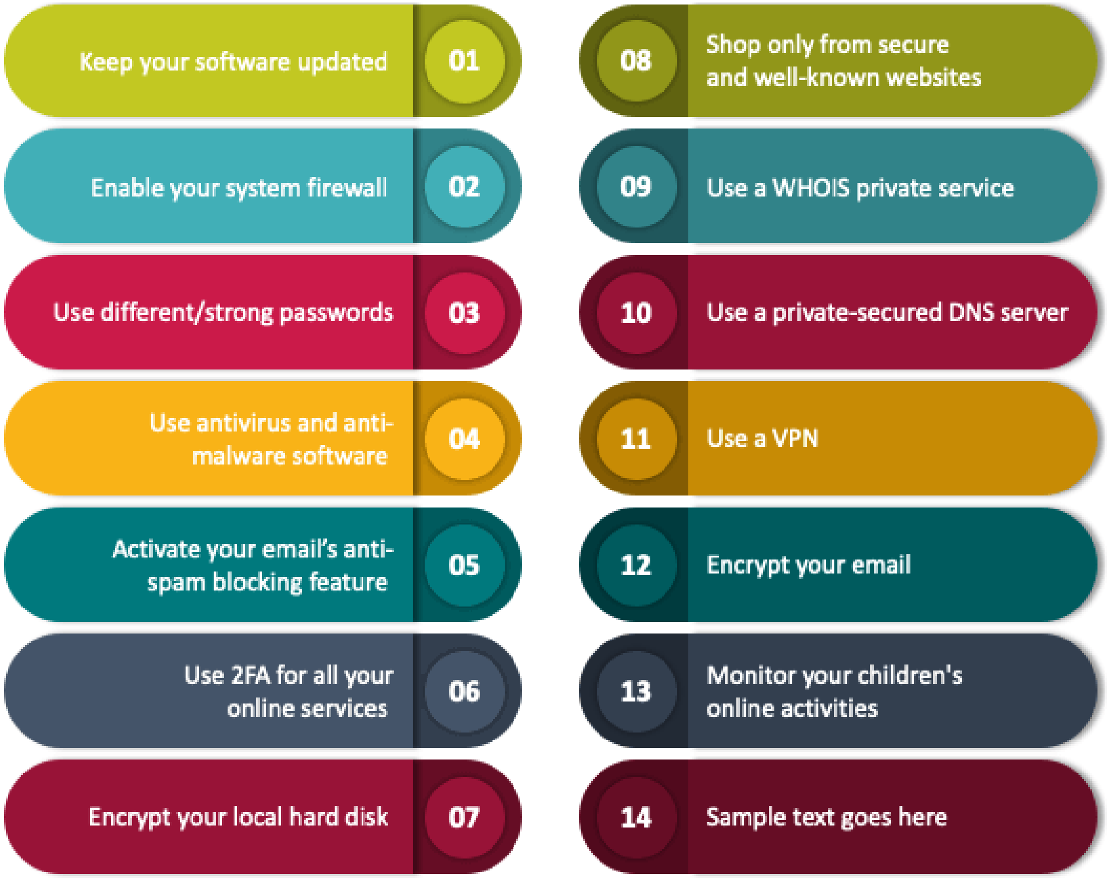
6. **Identity Theft:**
   This is a major problem with the people who are using the Internet and technology for cash transactions and banking services. In this cyber-crime, a criminal retrieves data about a person's bank account, credit cards, Social Security, debit card and the other diplomatic information to drain money or to purchase things online in the victim's name. This can result in vital economic losses for the victim and even in damaging the victim's credit history.

7. **Computer Vandalism:**
   This is a type of malicious action that involves the destruction of computers and data in different ways and certainly disrupting businesses. The computer vandalism involves the installation of malicious programs which are designed to perform damaging tasks such as deleting hard drive data or remove login credentials. Computer vandalism differs from viruses which hold themselves to the existing programs.

8. **Malicious Software:**
   This software based on the Internet or programs that are used to disturb a network. The software is used to acquire access to a system to loot diplomatic information or data or causing destruction to the software which is present in the system.



D. How to prevent Cyber-Crime?



01 Keep your software updated

02 Enable your system firewall

03 Use different/strong passwords

04 Use antivirus and anti-malware software

05 Activate your email's anti-spam blocking feature

06 Use 2FA for all your online services

07 Encrypt your local hard disk

08 Shop only from secure and well-known websites

09 Use a WHOIS private service

10 Use a private-secured DNS server

11 Use a VPN

12 Encrypt your email

13 Monitor your children's online activities

14 Sample text goes here

To prevent cyber-crime successfully, set up multidimensional public-private collaborations between law enforcement organizations, the information technology industry, information security organizations, internet companies, and financial institutions. A far apart from the real world, Cyber-criminals do not combat one another for predominance or authority. Rather, they do their tasks together to enhance their abilities and even can help out each other with new opportunities. Therefore, the regular ways of fighting the crime cannot be used against these cyber-criminals.

There are some ways to prevent cyber-crimes are explained below:

1. **By Using Strong Passwords:**
   Maintaining different password and username combinations for each of the accounts and withstand the desire to write them down. Weak passwords can be easily broken. The following password combinations can make password more prone to hacking:
   - Using keyboard patterns for passwords. e.g. – wrtdghu
   - Using very easy combinations. e.g. – sana1999, jan2000
   - Using Default passwords. e.g. – Hello123, Madhu123
   - Keeping the password the same as the username. e.g. – Sanu Sanu

2. **Keep social media private:**
   Be sure that your social networking profiles (Facebook, Twitter, YouTube, etc.) are set to be private. Once be sure to check your security settings. Be careful with the information that you post online. Once if you put something on the Internet and it is there forever.

3. **Protect your storage data:**
   Protect your data by using encryption for your important diplomatic files such as related to financial and taxes.

4. **Protecting your identity online:**
   We have to be very alert when we are providing personal information online. You must be cautious when giving out personal IDs such as your name, address, phone number, and financial information on the Internet. Be sure to make that websites are secure when you are making online purchases, etc. This includes allowing your privacy settings when you are using social networking sites.

5. **Keep changing passwords frequently:**
   When it comes to passwords, don’t stick to one password. You can change your password frequently so that it may be difficult for hackers to access the password and the stored data.

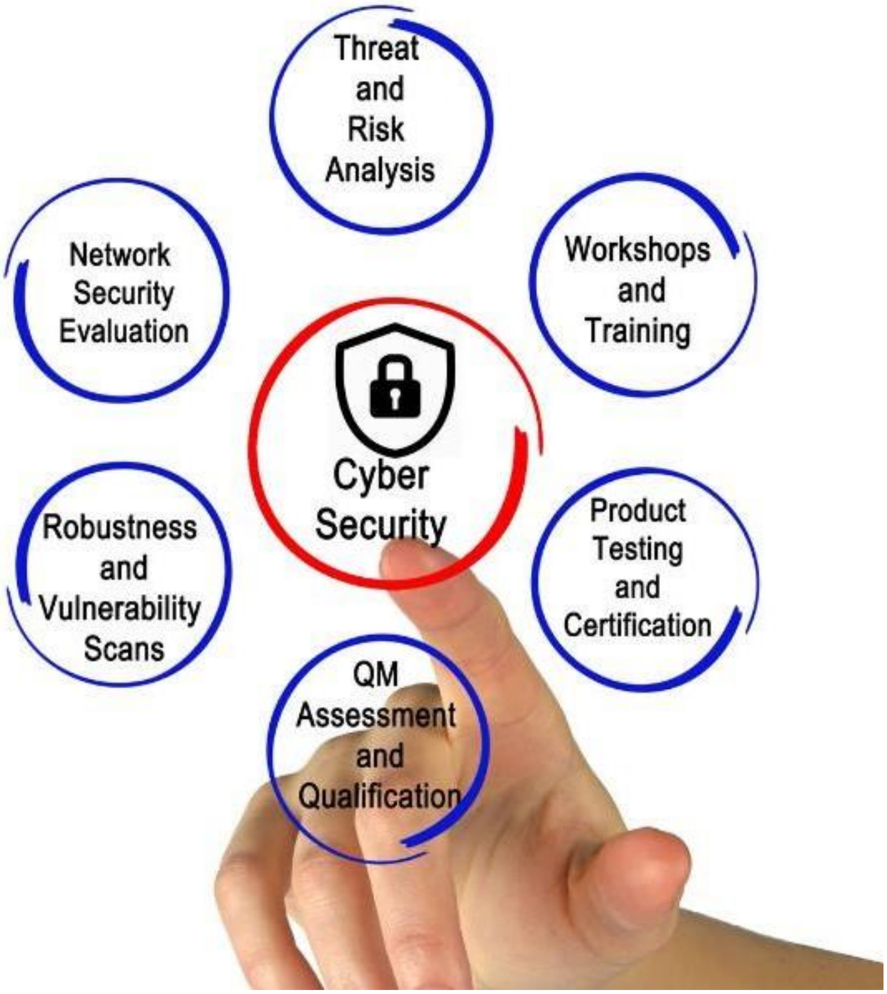
6. **Securing your Phones:**
   Many people do not know that their mobile devices are also unsafe for malicious software, such as computer viruses and hackers. Make sure that you download applications only from trusted sources. Don’t download the software /applications from unknown sources. It is also pivotal that you should keep your operating system up-to-date. Be sure to install the anti-virus software and to use a secure lock screen as well. Otherwise, anybody can retrieve all your personal information on your phone if you lost it. Hackers can track your every movement by installing malicious software through your GPS.

7. **Call the right person for help:**

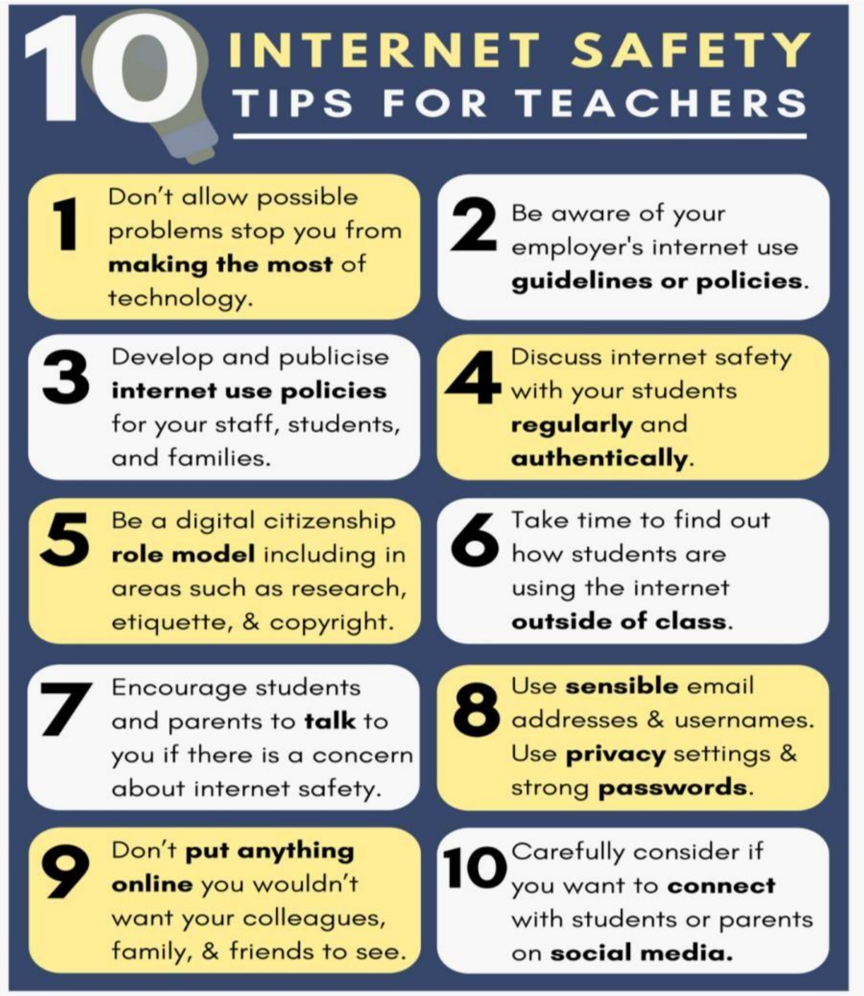
   Try not to be nervous if you are a victim. If you come across illegal online content such as child exploitation or if you think it's a cyber-crime or identity theft or a commercial scam, just like any other crime report this to your local police. There are so many websites to get help on cybercrime.

8. **Protect your computer with security software:**

   There are many types of security software that are necessary for basic online security. Security software includes firewall and antivirus software. A firewall is normally your computer's first line of security. It controls who, what and where is the communication is going on the internet. So, it's better to install security software which is from trusted sources to protect your computer.


Threat and Risk Analysis
Network Security Evaluation
Workshops and Training
Cyber Security
Robustness and Vulnerability Scans
Product Testing and Certification
QM Assessment and Qualification

E. Cyber-security Tips for Teachers



10 INTERNET SAFETY TIPS FOR TEACHERS

1 Don't allow possible problems stop you from **making the most** of technology.

2 Be aware of your employer's internet use **guidelines or policies**.

3 Develop and publicise **internet use policies** for your staff, students, and families.

4 Discuss internet safety with your students **regularly** and **authentically**.

5 Be a digital citizenship **role model** including in areas such as research, etiquette, & copyright.

6 Take time to find out how students are using the internet **outside of class**.

7 Encourage students and parents to **talk** to you if there is a concern about internet safety.

8 Use **sensible** email addresses & usernames. Use **privacy** settings & strong **passwords**.

9 Don't **put anything online** you wouldn't want your colleagues, family, & friends to see.

10 Carefully consider if you want to **connect** with students or parents on **social media.**

Now that you have an understanding of the cyber threats that educators face today, you mightbe wondering, what do I need to do to ensure myself, my school and my students are safe? Here are five steps you can follow to help prevent these attacks, provided by the Texas Computer Education Association:

Encrypt Your Data: Hackers today can obtain classroom data by intercepting it while actively in transit. By protecting your data using encryption, you can prevent cyber attackers from stealing the data that you send and receive.

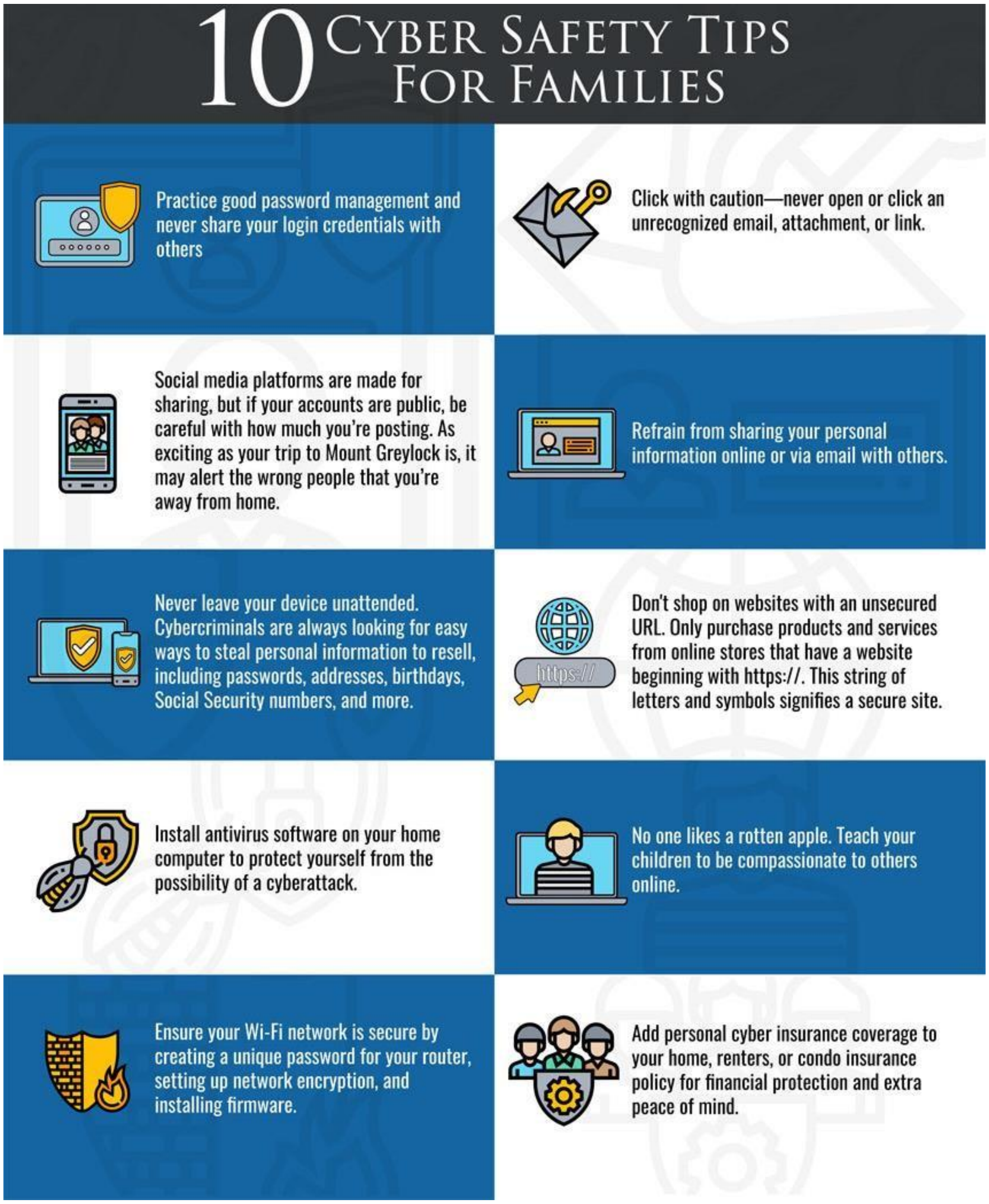
Comply with Your Institution's Cyber Protocols: It is very likely your school already has cyber-security measures in place to protect users. It is important to follow these provisions and contact your IT or Cyber-security department if an issue arises.

Safeguard Your Devices From Physical Attacks: Always log out of your computer when you step away. To keep passwords safe, try to avoid writing them down or entering your credentials within view of someone else.

Back up Your Data: If your work or institution requires the storage of student data, it is important to back it up to prevent attackers from targeting this private data in Ransomware-style attacks where you may be locked out until a ransom is paid.

Practice Good Password Management: It’s easy to take shortcuts when it comes to passwords. A password management program such as LastPass can help you to maintain unique passwords for all of your accounts.

F. Cyber-security Tips for Parents and Children



10 CYBER SAFETY TIPS FOR FAMILIES

Practice good password management and never share your login credentials with others

Click with caution—never open or click an unrecognized email, attachment, or link.

Social media platforms are made for sharing, but if your accounts are public, be careful with how much you’re posting. As exciting as your trip to Mount Greylock is, it may alert the wrong people that you’re away from home.

Refrain from sharing your personal information online or via email with others.

Never leave your device unattended. Cybercriminals are always looking for easy ways to steal personal information to resell, including passwords, addresses, birthdays, Social Security numbers, and more.

Don’t shop on websites with an unsecured URL. Only purchase products and services from online stores that have a website beginning with https://. This string of letters and symbols signifies a secure site.

Install antivirus software on your home computer to protect yourself from the possibility of a cyberattack.

No one likes a rotten apple. Teach your children to be compassionate to others online.

Ensure your Wi-Fi network is secure by creating a unique password for your router, setting up network encryption, and installing firmware.

Add personal cyber insurance coverage to your home, renters, or condo insurance policy for financial protection and extra peace of mind.

As a parent, you are your child’s best protection against online threats like those mentioned above. Here are five steps that you can start following with your child today:

Teach Passwords and Privacy: Help your children password-protect all devices and online accounts. Teach them why creating strong passwords is important, how to create them and never to share them.

Monitor and Communicate: Communicate what comprises an acceptable, respectable (to themselves and others) online post and take the time to monitor your child’s online activity as often as possible.

Protect Identity and Location: Disable photo geo-tagging on your Android or iPhone and remind your child not to share any personal info online like age, school, address, phone number, last name or any personally identifiable data.

Use Secure Wi-Fi: Ensure that your home’s Wi-Fi includes encryption and a strong password to restrict outside access, and only share your password with those that you know and trust.

Utilize Parental Controls: Many kids are given their first tablet or internet-connected device before they can fully comprehend the power in their hands. Try using built-in parental control features to start taking precautions and monitor their usage as early as possible.

G. Cyber-security Tips for Students

Today’s cyber hackers are constantly discovering new exploits and strategies to compromise users. Here are five cyber-security best practices to help protect yourself from them:

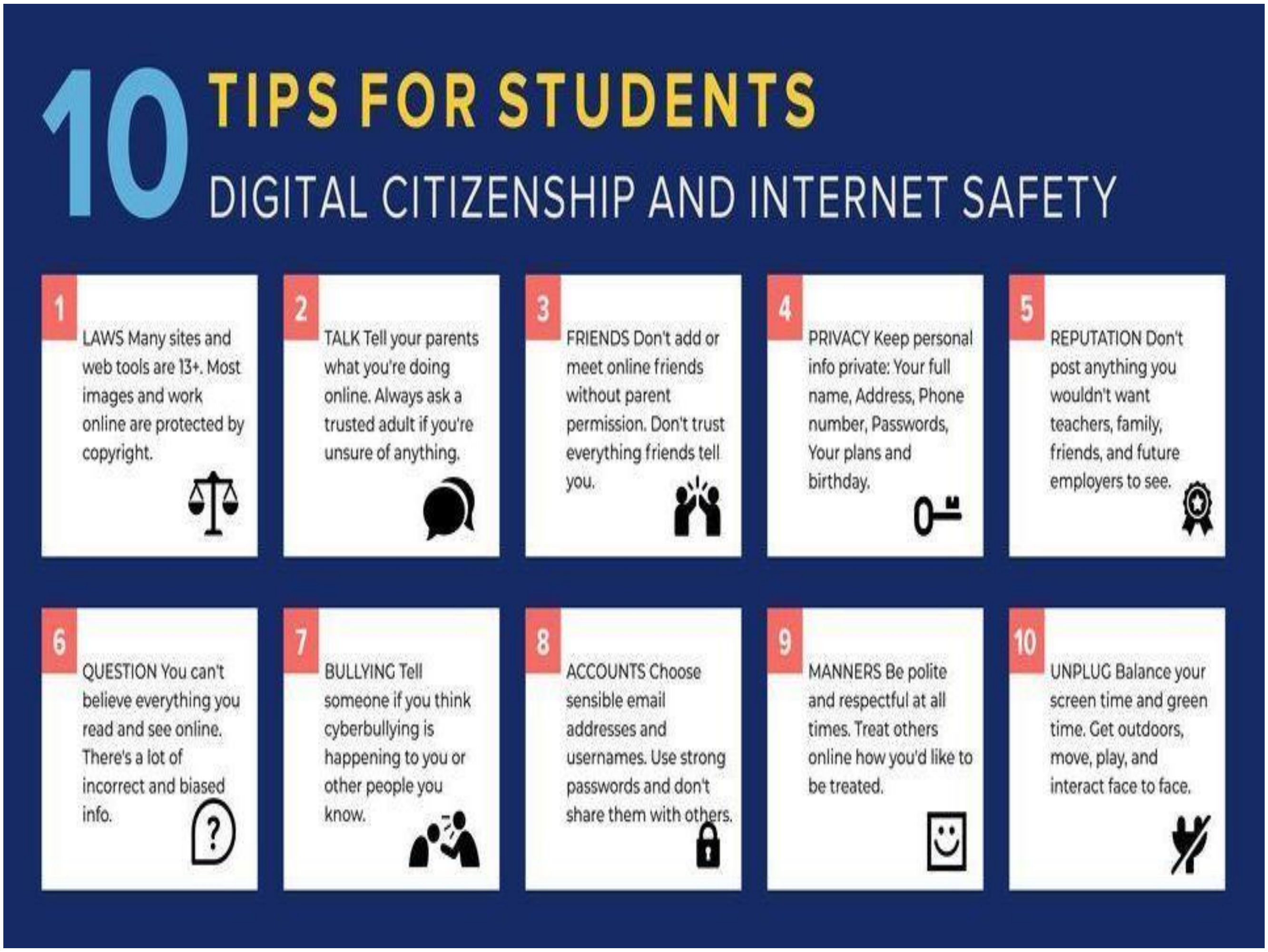
Avoid Sharing Personal Information: Be mindful about the information you divulge online — such as school names, email addresses, home addresses and telephone numbers.

Invest in Virus Protection: Ensure you have antivirus protection with anti-phishing support installed on all devices (desktops, laptops, tablets, etc.). Set it to update automatically and run virus scans at least once a week.

Keep Software Up-to-Date: Be sure to keep your operating system, browser software, and apps fully updated with patches. Even new machines can have out-of-date software that can put you at risk.

Be on the Guard for Phishing: Do not open email attachments from untrusted sources. You may be expecting emails from group members or teachers, but use caution when opening any attachments.

Be Careful What You Click: Avoid visiting unknown websites or downloading software from untrusted sources. These sites can host malware that will install (often silently) and compromise your computer.



10 TIPS FOR STUDENTS

DIGITAL CITIZENSHIP AND INTERNET SAFETY

1 LAWS Many sites and web tools are 13+. Most images and work online are protected by copyright.

2 TALK Tell your parents what you're doing online. Always ask a trusted adult if you're unsure of anything.

3 FRIENDS Don't add or meet online friends without parent permission. Don't trust everything friends tell you.

4 PRIVACY Keep personal info private: Your full name, Address, Phone number, Passwords, Your plans and birthday.

5 REPUTATION Don't post anything you wouldn't want teachers, family, friends, and future employers to see.

6 QUESTION You can't believe everything you read and see online. There's a lot of incorrect and biased info.

7 BULLYING Tell someone if you think cyberbullying is happening to you or other people you know.

8 ACCOUNTS Choose sensible email addresses and usernames. Use strong passwords and don't share them with others.

9 MANNERS Be polite and respectful at all times. Treat others online how you'd like to be treated.

10 UNPLUG Balance your screen time and green time. Get outdoors, move, play, and interact face to face.