CYBER SAFETY

safe and responsible use of information and communication technology

What is Cyber Safety

- Cyber safety refers to safe and responsible use of Internet, to ensure safety and security of personal information and not posing threat to anyone else's information.

Safely Browsing The Web

- These days we must know the threats while browsing the web. Safe browsing on web needs you to know many things like:
  - What are possible dangers?
  - How to avoid these?
  - How to virtually conduct yourself while browsing web
- **You must remember, not every site you visit is safe. Whatever you post or do online is visible to others. Not everything you see or is promised online is true.**

Identity Protection while using Internet

- We surf internet for a variety of reasons, from using social media, buying and selling goods, to exchanging information.
- When we give private data to businesses and other Internet users (such as while filling online form or making payment online), we trust them to use that information for legitimate purposes.
- These information can be used for harmful reasons like hacking, stalking an identify fraud.
- Identity fraud is when personal details that have been accessed or stolen are used to commit fraudulent acts posing as someone else with stolen identity

Solution of Identity Fraud

- Most common solution to this is :
  - Private Browsing Or
  - Anonymous Browsing

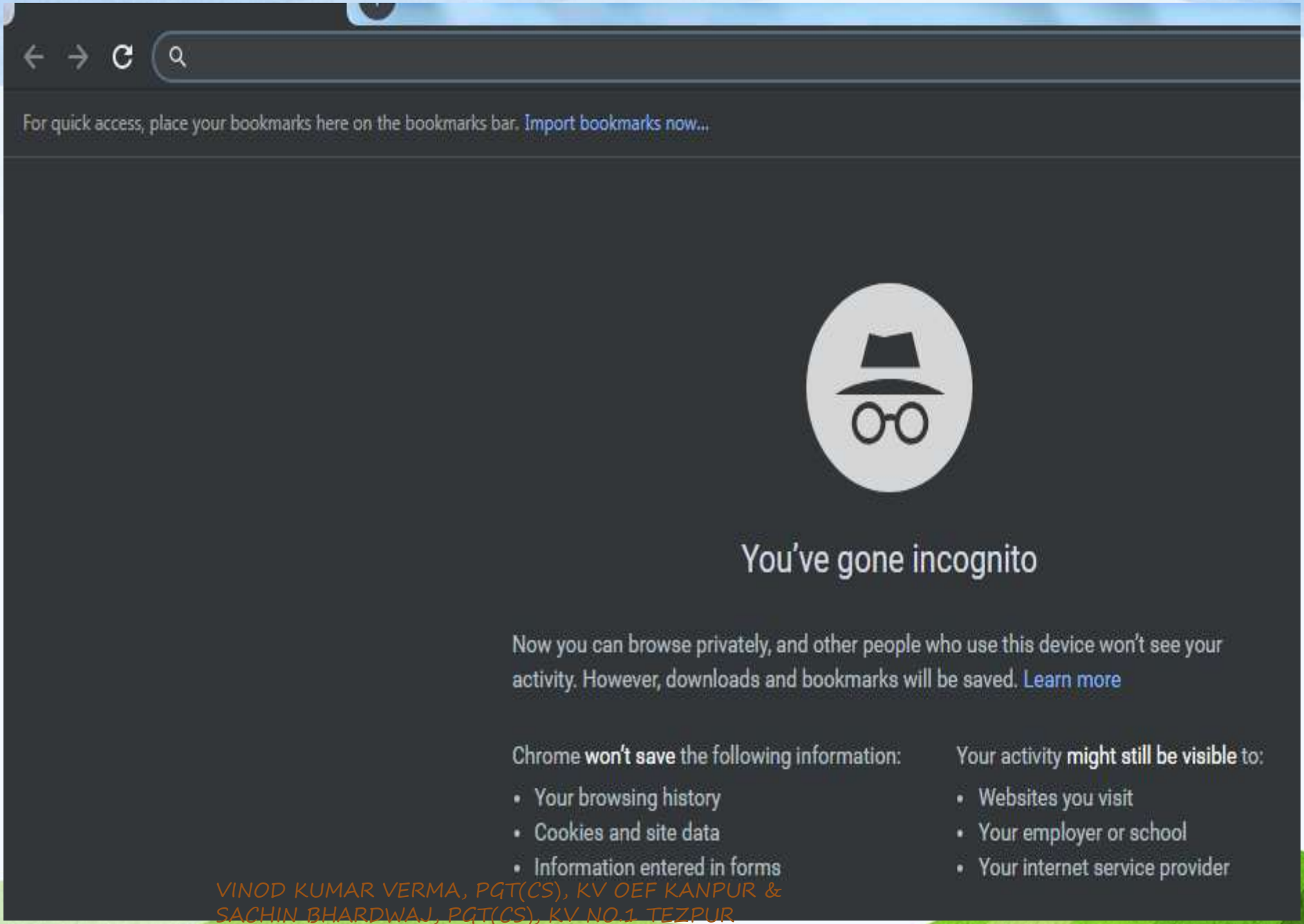
Before we understand this, let us talk about what happens when we browse the internet...

Anonymous Browsing

- All the ways discussed earlier of identity leakage is resolved by either ANONYMOUS OR PRIVATE BROWSING.
- **ANONYMOUS BROWSING** : allows users to view websites without revealing any personnel information of user like IP address, machine type, location. An anonymous browser lets users access websites anonymously. It can also be as a tool for government, journalists and everyday security-conscious surfers.

Private Browsing

- There are other ways to use internet without revealing our search history and sharing our data :
  - **Incognito Browsing** : opens up a version of the browser that will not track you activity. Its particularly useful if you are entering sensitive data like bank details into the browser as it can minimise the risk of our information being saved to that computer. In Google chrome, just press : **CTRL + SHIFT + N to open in incognito mode**


For quick access, place your bookmarks here on the bookmarks bar. Import bookmarks now...
You've gone incognito
Now you can browse privately, and other people who use this device won't see your activity. However, downloads and bookmarks will be saved. Learn more
Chrome won't save the following information:
• Your browsing history
• Cookies and site data
• Information entered in forms
Your activity might still be visible to:
• Websites you visit
• Your employer or school
• Your internet service provider

Private Browsing

- **Proxy** : act as a middlemen between your computer and the website you want to access. Now the tracking website will get the IP address and information that belongs to the proxy site, so you are effectively getting the same content from another source without getting to know your browsing details
- **Virtual Private Network (VPN)** : is a method to add security and privacy to private and public networks like Wi-Fi hotspot and the Internet. VPNs are most often used by corporation to protect sensitive data. VPN were originally meant for business employees working offsite to gain access to shared drive.

Confidentiality of Information

- Internet is a public platform. The sites you visit, the products you search, the posts that you put on social media are all visible to public. But there must be some information like Credit Card Details, Bank Details which you do not want to make public i.e. you want to keep this information confidential.

Practices to Ensure Confidentiality of Information

1. **Use Firewall wherever possible** : we must secure our system such that only authentic users can connect to it. Firewall is one very good solution for this. Firewall is a program/hardware that monitors all communications and traps al illicit packets. Most OS now comes with firewall preinstalled. We must install Firewall that can monitor both incoming and outgoing communication and traps the illicit ones.

Practices to Ensure Confidentiality of Information

2. **Control browser setting to block tracking** : as we know that website can track our surfing on their site by IP address, to minimise these threats we can turn our default settings to exclude third party cookies since they can be used to build up detailed profiles of our surfind pattern over time.

In Google Chrome : Open settings, -> Privacy and Security -> Content Settings-> Cookies -> "Enable" Block Third party cookie.

Practices to Ensure Confidentiality of Information

3. **Browse privately wherever possible:** to avoid the tracking as discussed earlier try to browse anonymously or privately.

4. **Be Careful while posting on Internet :** When you post anything to public Internet such as social networking site like Instagram or Facebook etc. newgroup, mailing list or chat room you generally give up rights to the content and any expectation or privacy or confidentiality is useless. So never post crucial information like you personal details such as address, mobile phone numbers, bank details, credit card details. Etc. on public internet sites.

Practices to Ensure Confidentiality of Information

5. **Ensure Safe sites while entering crucial Information** : while entering or giving crucial information like Passwords, Bank Details always ensure the website is working on https not on http. https means website is Secure i.e. Secure Socket Layer. For e.g. (next slide)

Closed Lock Pad (Secure Connection)

VINOD KUMAR VERMA, PGT(CS), KV OEF KANPUR &
SACHIN BHARDWAJ, PGT(CS), KV NO.1 TEZPUR

Practices to Ensure Confidentiality of Information

6. **Carefully handle emails** : while opening emails, make sure you know the sender. Never open email of unknown or if by curiosity/accidentally opened the mail never click on any link inside it or open any attachment. It may lead to you fraudulent site, or trap for you or may be a Trojan, which will act as a Spy in you computer for sending information to the sender without your knowledge.

Practices to Ensure Confidentiality of Information

7. **Avoid using Public Computer** : Always try not to use the public computer specially if you have to deal with your crucial data. But if it is an urgency then do remember:

- ✓ Browse privately
- ✓ Never save your login information (ID/Password)
- ✓ Avoid entering sensitive information
- ✓ Don't leave computer unattended with sensitive information on screen
- ✓ Disable the features that stores passwords
- ✓ Properly logout before you leave the computer
- ✓ Erase history and traces of your work i.e. clear history and cookies
- ✓ Look for any suspicious device connected to computer

Cyber Crime

- Is any criminal offense that is facilitated by, or involves use of electronic communications of information system including any electronic device, computer or the Internet.
- It involves the terms like : **Phishing, Credit Card Frauds, illegal downloading, industrial espionage, child pornography, cyber bullying, cyber stalking, cyber terrorism, creation and /or distribution of viruses, spam** and so on

Cyber Trolls and Bullying

- It refers to a person who purposely post opposing, sarcastic, demeaning or insulting-comments about something or someone with an aim of targeting a person online. The provocative messages posted this way are also called trolls. It is a cyber crime and is a form of cyber bullying.

Cyber Bullying

- Harassing, demeaning, embarrassing, defaming, or intimidating someone using modern technologies like internet, cell phones, instant messengers, social networks etc. is called Cyber Bullying.

Cyber Stalking

- It is a kind of online harassment wherein the victim is subjected to barrage of online messages and emails.
- Typically these stalkers know their victims instead of resorting to offline stalking, they use the internet to stalk.
- A cyber stalker relies upon the anonymity afforded by the Internet to allow to stalk their victim without being detected

Cyber Stalking

- Cyber Stalkers often do this to trouble their victims:
  - They collect all personal information about their victims
  - The stalker may post this information on any obscene or illegal website posing as if the victim is posting this information
  - People of all kind from nook and corner of the world, start calling the victim as his/her residence/workplace for many filthy/obscene reasons
  - Some stalker subscribe the email account of victim to illegal websites because of which victim starts receiving such kind of unsolicited e-mails.

Cyber Stalking

- Cyber Stalkers often do this to trouble their victims:
  - Some stalkers keep on sending repeated e-mails asking for various kinds of favors or threaten the victim.
  - Stalkers follow their victim from board to board.
  - Stalkers will almost always make contact with their victims through email having friendly or threatening content. The stalker many times uses multiple names when contacting the victim.

Spreading Rumors Online

- People often think that they can make a fake profile with some different name and do anything online and will not be caught. Through such fake profile, people sometimes indulge in posting false information on social media, or comment could hurt others or spread rumors that may trigger panic or hurt religious sentiments of other people resulting into clashes and even riots
- Spreading rumors online is a cyber crime and it may invite a fine with imprisonment extendable up to three years.

Reporting Cyber Crime

- If any cyber crime happens, one must report it firstly to parents, school authorities and then to police.
  - The local police stations can be approached for filing complaints just as the cybercrime cells specially designation with the jurisdiction to register complaint
  - In addition, provisions have now been made for filing of E-FIR in most of the states
  - In addition, the ministry of Home Affairs is also launching a website for registering crimes against women and children online including cybercrimes

Common Social Networking Sites

- **Facebook :** it is a platform where you can share your ideas in form of posts, share photos, videos etc.
- **Twitter :** micro blogging site which allows to post very small messages up to 280 chars.
- **LinkedIn :** social network for professionals. Provides features to make profiles look sort of detailed resumes, with sections for work experience, education, volunteer work, certifications, awards etc.
- **Instagram :** on of the most popular social networks for online photo sharing. Offer features like sharing real-time photos and short videos while on the go.

Appropriate usage of Social Networks

- Whatever we do online – post something or visit friends pages or search something etc leaves a permanent footprints called digital footprints and it remains for years storing trails of your online activities.
- We are using this platform for personal reasons and visible to anyone who looks for it, this might not cause any problem now BUT sometimes later it can pose potential problems when it comes to matter like – taking admissions in higher education or looking for job or even when looking for a life partner
- These days many universities look for digital footprints of applicant students before giving them admissions, similarly employers may look for digital footprint of candidates and so on.

What you should know?

- While using social networking sites, you should know about what the **right online behaviors are** and **what is considered a cybercrime**
- If anyone thinks by making fake profile he/she can do such activity without being caught he/she is certainly mistaken. Modern technology tools can find anyone online using IP address, locations etc. So one must not indulge in these activities at all

Digital Footprints

- Are the records and traces individuals leave behind as they use the Internet.
- Your interaction on social media, your friend circle on social media sites, site you visits, online purchase, location visited through Facebook check-ins. etc. all make up your Digital Footprints.

Privacy Settings

- When you start social media, you should not go with default privacy settings. Rather it is always a good idea to set-up privacy settings yourself by using Account Settings. Through privacy settings you can control :
  - **Who all can see what you have posted**
  - **Who all can send requests to you**
  - **What all information about you is visible to others, even to you contacts etc.**

What you should do – Usage Rules

1. Be Authentic : Be honest about your identity
2. Use a Disclaimer : if you are associated with any institution / organization and you are sharing you personal views about something, do make it clear that these are you personal vies and you do not represent any institution/organization.
3. Don't Pick Fights Online : don't pick fight online if you do not like anyone's comments on your post.

What you should do – Usage Rules

4. Don't use Fake names or Pseudonyms : never pretends to be someone else.

5. Protect Your Identity : while you should be honest about yourself, BUT you should never provide or post personal information online. These information can be used to conduct fraud or crime.

6. Does your Information / Post pass the publicity test ? : if your post is not acceptable for face-to-face conversation, over the telephone then it is NOT ACCEPTABLE for a social networking site too.

What you should do – Usage Rules

7. Respect you audience : sometimes school/college students talk in slang or use some abusive words which they find okay within their small group. But these things must not be posted online because it would not be acceptable in you connected world.

8. Respect other's Sentiments : you should always respects others' privacy and be considerate for topics that may be considered sensitive – such as politics and religion.

What you should do – Usage Rules

9. Monitor Comments : most people who maintain social media sites welcome comments – it builds credibility and community. You should prefer to review and approve comments before posting them on you site. This way you will ensure quality oF comments