

Cyber Crimes &



VIII International Online Faculty Development Program
On
Creativity, Innovation and Institution Building

Dr. Priyanka Kacker

Assistant Professor
Institute of Behavioural sciences,

GFSU

NAAC ACCREDITED 'A' GRADE



विद्यया अमृतं अश्नुते

**Gujarat Forensic
Sciences University**

Knowledge | Wisdom | Fulfilment

Cyber Security Threats Scenario

- 92% of the Indian youth was found to have shared private information online despite being aware that this is risky.
- 53% of youngsters trust the virtual world and interact with strangers
- 51% of those polled did not care about their online privacy at all
- Two out of three polled youngsters had some experience with cyber-bullying and
- an overwhelming number said they would not know what to do if they were harassed online.

Two Aspects:

1. Victim of Cyber Crime

- Direct
- Indirect

2. Cyber Crime Offender

Few Questions

- Do you know all the features of your smart phones/smart TV/Apps installed in your mobile/Computer?
- Are you using trial version of Anti-Virus and other soft wares?
- Do you read terms and conditions before installing any software/app in your comp/mobile phone?

Few Questions

- Do you share your password with your spouse/family members/Children?
- Do you use free Wi-Fi frequently?
- Have you ever been a victim of Cyber Crime?

A close-up photograph of a computer keyboard. The central focus is a light blue key with the words "Cyber crime" printed in a bold, black, sans-serif font. The key is slightly raised and has a soft shadow. Surrounding it are several dark grey keys with white symbols: an equals sign, a left arrow, a delete key, a bracket/brace key, a quote key, a question mark key, and a shift key with an upward arrow symbol. The lighting is soft, highlighting the texture of the keys.

**Cyber
crime**

Cyber crimes

- Crime committed using a computer and the internet to steal data or information.
- Illegal imports.
- Malicious programs.

Cyber crime Cybercrime is nothing but where the computer used as an object or subject of crime.

CATEGORIZATION OF CYBER CRIME

- The Computer as a Target
- The computer as a weapon

Types of cyber crimes

Types of Cyber Crimes

1. Hacking
2. Salami Attack
3. Malware dissemination
4. Software Piracy
5. Forgery
6. Obscene or Offensive Content
7. Pornography
8. Cyber Sex
9. Fraud
10. Phishing
11. Spoofing
12. Spam
13. Denial of Service
14. Threatening
15. Net Extortion
16. Cyber Terrorism
17. Drug Trafficking
18. Cyber Warfare
19. Cyber Stalking
20. Cyber Defamation
21. IRC Crime

Types of Cyber Crimes

COVID 19 Special Frauds:

- Job frauds
- Matrimonial frauds
- Financial Frauds



Hacking in simple terms means an illegal intrusion into a computer system and/or network.



YOU HAVE BEEN
HACKED !

Denial of Service (DoS)

Service Unavailable

HTTP Error 503. The service is unavailable.

Denial of Service (DoS)



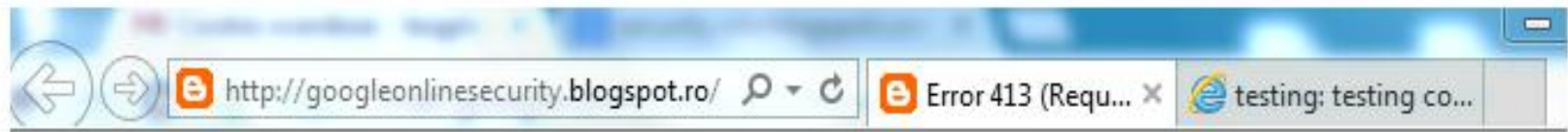
The connection has timed out

The server at www.cia.gov is taking too long to respond.

- The site could be temporarily unavailable or too busy. Try again in a few moments.
- If you are unable to load any pages, check your computer's network connection.
- If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the Web.

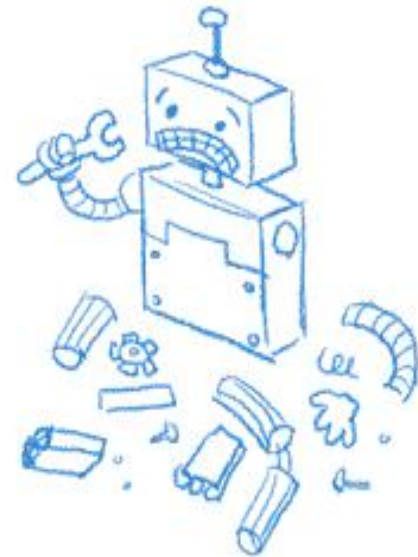
Try Again

Denial of Service (DoS)



413. That's an error.

Your client issued a request that was too large. That's all we know.



Signs of a DoS attack



DEGRADATION IN NETWORK PERFORMANCE

Especially when attempting to open files stored on the network or when accessing websites.



SPECIFIC WEBSITE UNAVAILABLE

A particular site does not open or cannot be found.



INABILITY TO ACCESS ANY WEBSITE

All websites are inaccessible on the network.

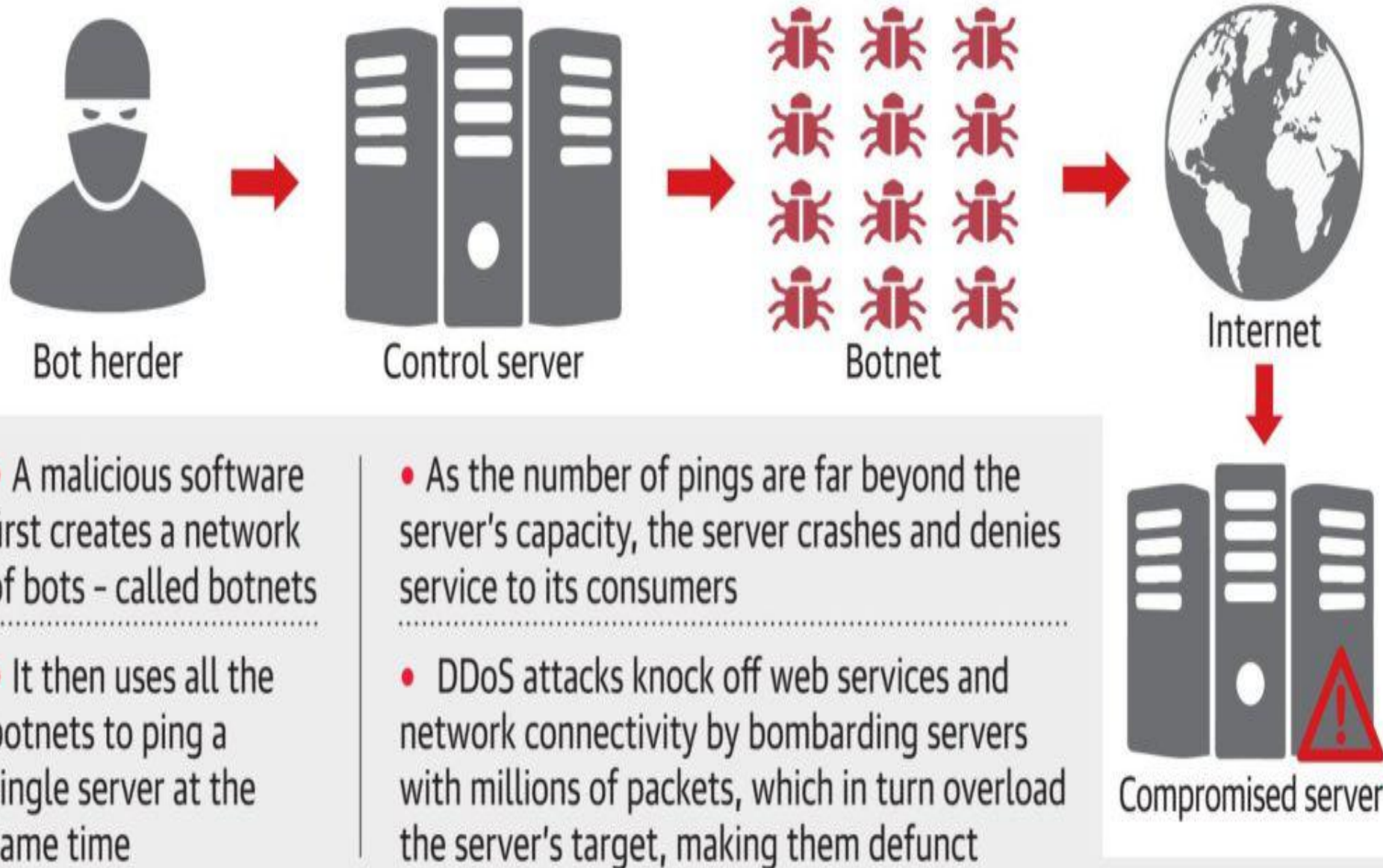


HIGH VOLUME OF EMAIL SPAM

A higher than usual volume of spam email.

What is a DDoS attack

DDoS, or distributed denial of service attack, is a malware (malicious software) attack



DENIAL OF SERVICE ATTACK

- Act by the criminal, who floods the bandwidth of the victims network.
- Is his e-mail box with spam mail depriving him of the services.

CYBERWAR

Cyber warfare involves the actions by a nation-state or international organization to attack and attempt to damage another nation's computers or information networks through, for example, computer viruses or denial-of-service attacks.

40,300 cyber attacks in the last 4-5 days from China, more coming: Maharashtra cyber department

The threat of cyber attacks from China has re-emerged after the violent clash at the LAC in Ladakh between the armies of the two countries.

INDIA

Updated: Jun 23, 2020 19:47 IST



[hindustantimes.com](https://www.hindustantimes.com) | Edited by Abhinav Sahay

Hindustan Times, New Delhi



Basic Reasons of Attacks on Email Accounts

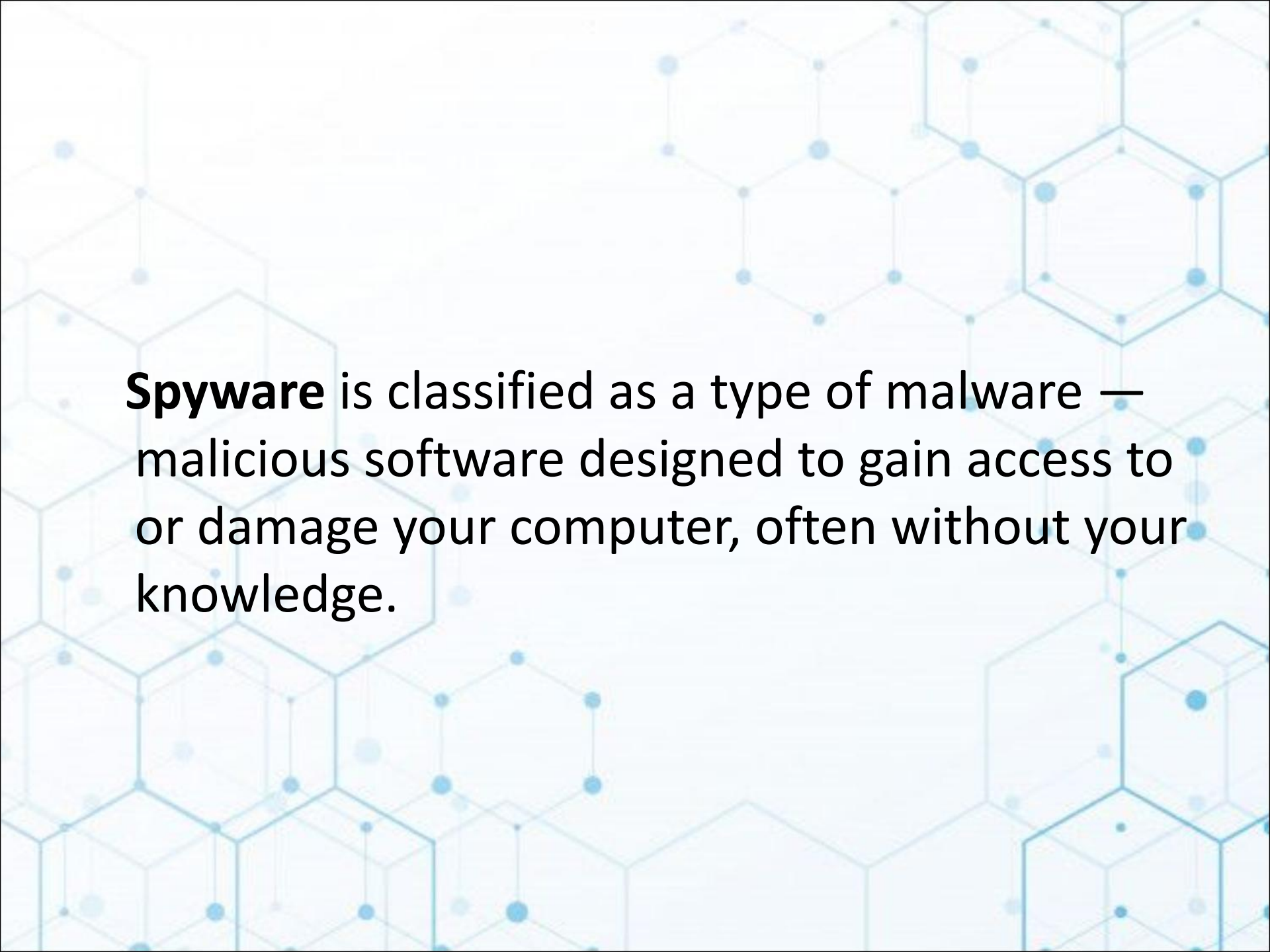
- When one discloses his or her password to another person
- Forgetting to log out from public computers
- Technologically based processes of hacking are that of Phishing, Cookie Hijacking and Key logging.
- Lack of awareness about legal remedies to sue a bad man.

Challenges of email security

- Ongoing threats that spread through email
- Hoaxes – fake news sent by email
- Spam – massive, anonymous and unwanted messages
- Phishing messages
- Malware propagation

Spyware is unwanted software that infiltrates your computing device, stealing your internet usage data and sensitive information.



The background of the slide features a light blue and white geometric pattern. It consists of a grid of hexagons, some of which are outlined in a slightly darker blue. Scattered throughout this grid are small, semi-transparent blue dots of varying sizes. The overall effect is a clean, modern, and tech-oriented aesthetic.

Spyware is classified as a type of malware — malicious software designed to gain access to or damage your computer, often without your knowledge.

Salami Attack

- In such crime criminal makes insignificant changes in such a manner that such changes would go unnoticed.
- Criminal makes such program that deducts small amount like Rs. 2.50 per month from the account of all the customer of the Bank and deposit the same in his account. In this case no account holder will approach the bank for such small amount but criminal gains huge amount.

VIRUS DISSEMINATION

- Malicious software that attaches itself to other software. (virus, worms, Trojan Horse, web jacking, e-mail bombing etc.)

COMPUTER VANDALISM

- Damaging or destroying data rather than stealing.
- Transmitting virus

CYBER TERRORISM

- Use of Internet based attacks in terrorist activities.
- Technology savvy terrorists are using 512-bit encryption, which is impossible to decrypt.

SOFTWARE PIRACY

- Theft of software through the illegal copying of genuine programs.
- Distribution of products intended to pass for the original.

IRC CRIME...

Internet Relay Chat (IRC) servers have chat rooms in which people from anywhere the world can come together and chat with each other. Criminals use it for meeting coconspirators. Hackers use it for discussing their exploits / sharing the techniques.

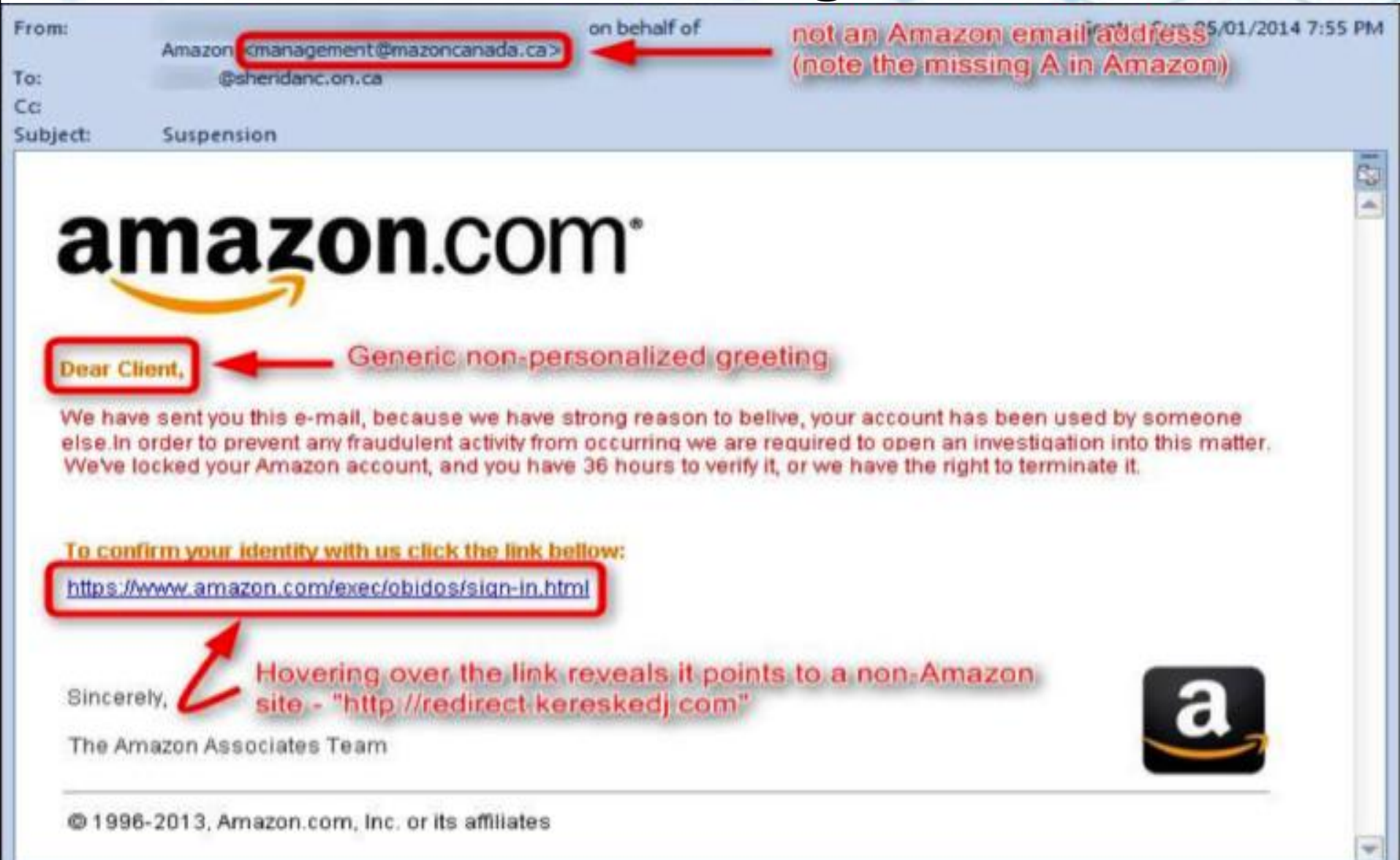
Pedophiles use chat rooms to allure small children.



Phishing

- Phishing is a method of sending a user (or many users) digital correspondence that appears **legitimate** but is actually meant to **lure a potential victim** into providing some level of personal information for nefarious purposes, including **identity or monetary theft**. The phishing scheme could use email, text, or web page.

Phishing



Phishing

NETFLIX

[Your Account](#) | [Queue](#) | [Help](#)

Your Account Has Been Suspended

Dear Netflix,

We are sending this email to let you know that your credit card has been expired. To update your account information, please visit [Your Account](#).

-Your friends at Netflix



Alice's computer
gets infected by
malware

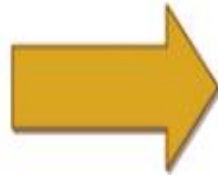
Email Spoofing



Bob



Charlie



Bob



Charlie

The malware
collects email
addresses of Bob
and Charlie

The malware sends email
to Charlie forging email
address of Bob

TYPES OF CYBER ATTACK BY PERCENTAGE

- Financial fraud: 11%
- Sabotage of data/networks: 17%
- Theft of proprietary information: 20%
- System penetration from the outside: 25%
- Denial of service: 27%
- Unauthorized access by insiders: 71%
- Employee abuse of internet privileges 79%
- Viruses 85%

Cyber Cases

Personal Cases

1. Cyber Police has arrested a Husband for misusing his wife's FB account, in a cyber case in India. He hired an ethical hacker to hack into his wife's FB account so that he can find pieces of evidence regarding her bad character.
2. Using the trojan or malware, a woman's webcam was accessed to capture her private videos and posted on an illegal website. The incident came into light when the Mumbai resident appeared for an interview.
3. The **cyber fraud case** of duplication of a SIM card was registered with the police when a businessman from Ahmedabad caught wind of it. He registered a complaint under the cyber and financial crime since the defrauders had submitted fake documents with the mobile company to gain the businessman's personal details.
4. In a social media related cybercrime complaint, a famous Gujarati singer claimed that her photos were being used by an unknown man, saying they were married and had a child together.
5. To gain personal revenge, an ex-boyfriend, working as a software engineer, posted his ex's personal phone number on a 24*7 dating service helpline, was arrested in a leading cybercrime case.



KASPERSKY^{lab}

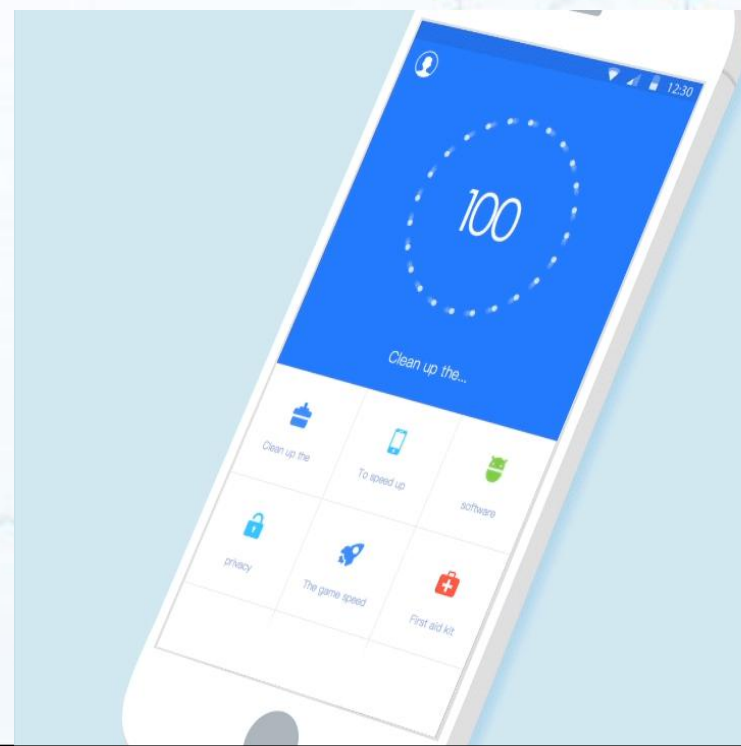
Welcome to
Kaspersky Free

Continue

By clicking the Continue button, you accept the terms of the [End User License Agreement](#).



- Install **latest** licensed version of **antivirus software's**.
- Uninstall unnecessary software
- Check security settings.



SAFETY TIPS FOR CYBER CRIME

Stay anonymous - choose a genderless screen name.

- Never give your full name or address to strangers.
- Keep updating yourself about Internet privacy



PASSWORD

- Passwords are the only keys that prevent unauthorized entry to many systems. (Laptops and Mobiles)
- Bad guys may want to corrupt your files.
- Bad guys may want to send embarrassing or offensive emails to you.
- Bad guys may want to use your system or systems belonging to your school/organization to compromise other systems.
- Bad guys may want to steal resources, like bandwidth, processing power, or storage space.
- Bad guys may want to use your organization to attack others.

Password security Preventions

- Passwords should be separate for 2 different email accounts
- Don't ever reveal your passwords to anyone.
- Write down in a secure location
- Change your passwords if compromised suspected.
- Add complexity to passwords like uppercase, lower case, special char, numbers combination : * _ - +=()!@#%^ (chin_2)
- Application should be updated and all the latest preventions applied.

Note: It can be a Computer Passwords,
Email Passwords, and Credit/Debit
Cards Passwords ...etc.





[SHOP NOW](#)



Order Now On Raho Safe



It Deeply Nourishes The Skin And Prevents The Skin From Drying Up.

Ad Pee Safe

Garlic bread



Domino's Style Cheesy Garlic Bread With



SAFETY TIPS FOR CYBER CRIME

- Put an opaque tape on your computer cam when your not using it. Same for smart TV and Mobile Phones.
- Use VPN number while using hotspot. (It will send encrypted messages and the Bad Guys can not use it)



DOWNLOAD FREE

- Do not give your mobile phone to anyone. If urgent; make sure that no new app is downloaded in the phone.
- While using someone else's phone make sure the screen recorder Is not on.

SAFETY TIPS FOR CYBER CRIME

- Do not click on link sent by unknown number or unknown/spam mails.
- Do not put personal and family photographs on Facebook.
- Set up Privacy settings on You tube & Face book.



0.5KB/s 4G 77%



June,06

09:27

Saturday

Cloudy 31°C



Weather



Gallery



Settings



Themes



Google



Security



Tools



Play Sto...



GetApps



SAFETY TIPS FOR CYBER CRIME

Facebook and Other Social Networking Sites

In Privacy settings:

- Check location history
- Get alerts about unrecognized logins
- Use two-factor authentication
- Secure your Profile picture (If possible do not put your image as profile pic)
- Allow access your profile to your Friends only.
- Upload pics/posts only for friends display. Do not put on public setting.
- Do not accept friend request of Unknown (Even if FB shows 1 or multiple mutual friends)

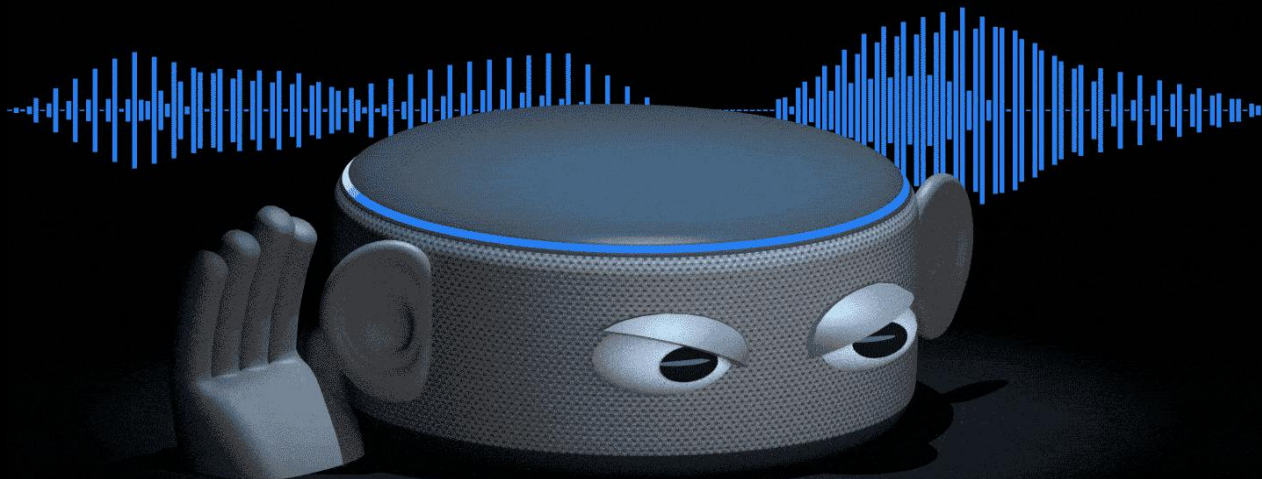
SAFETY TIPS FOR CYBER CRIME

- Never Post Illegal Activities
- Avoid Bullying class mates
- Don't Trash Your Teachers
- Don't Post Objectionable Content from any Computer/Mobile or Networks
- Don't Post Confidential Information
- Don't Overly Specific Location Check-Ins

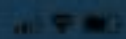
SAFETY TIPS FOR CYBER CRIME

- Don't Lie/Cheat/Plagiarize
- Don't Threaten / Violence
- Unprofessional Public Profiles
- Never Rely on Privacy Settings 100%
- Post Sensibly (Think Twice)

Are you Using Alexa?



9:15



amazon alexa

SAFETY TIPS FOR CYBER CRIME

- Don't respond to texts from people you don't know, "Friend" people you don't know on Facebook,
- Don't post information on Facebook when you're getting ready to change your location—to attend an event, run an errand, or take a trip later that day or in the future.

Concealing your location can help prevent cyber stalking and it keeps would-be robbers from knowing that you're away from home.

SAFETY TIPS FOR CYBER CRIME

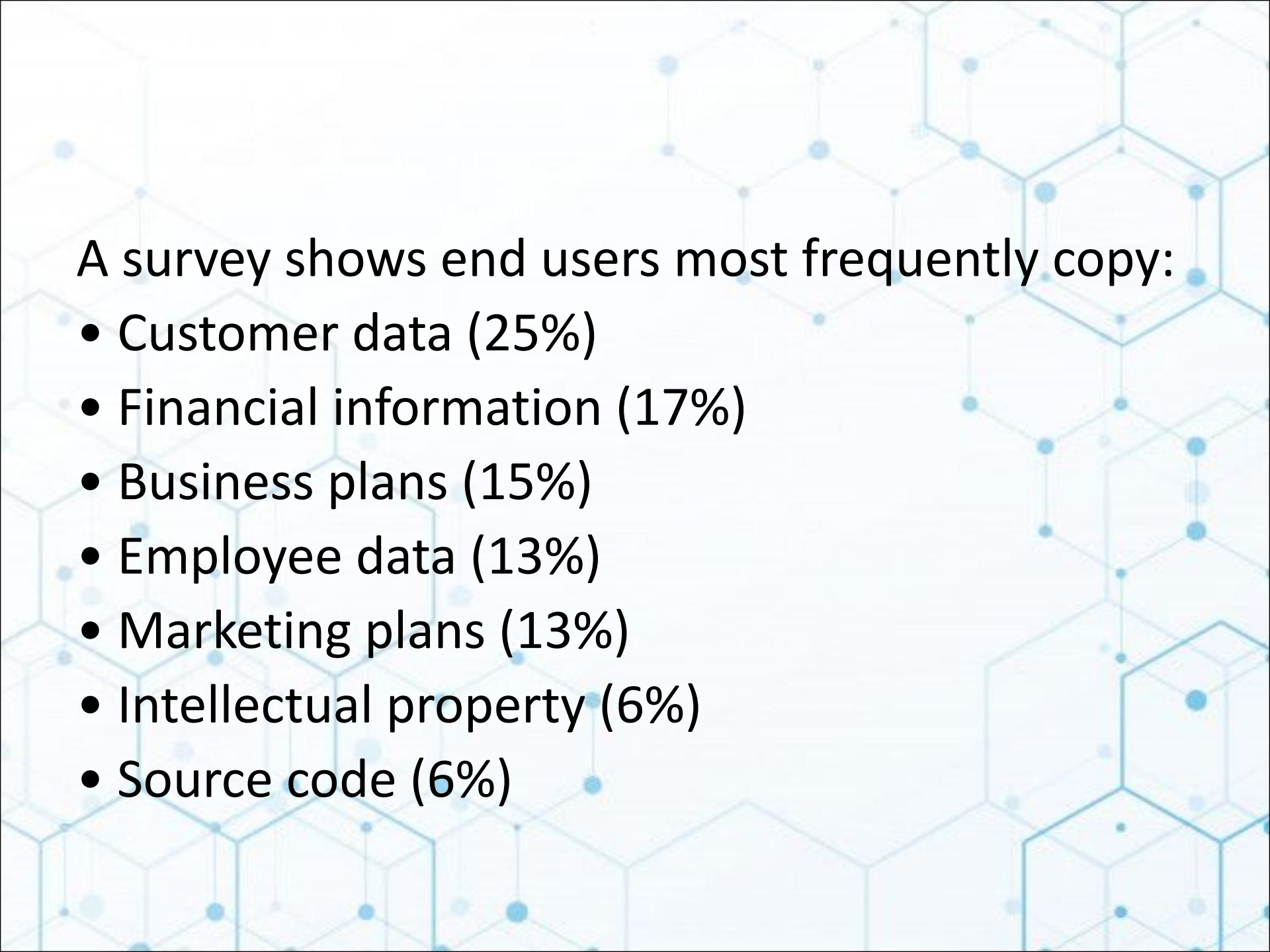
- Watch out for “Google Bombing” and avoid clicking on the links to unknown news sources when searching for a popular topic.

Hackers and others take advantage of big news stories, such as the April 2016 death of the artist, Prince, to get their site high on the Google rankings and increase the chances that their link will be clicked on, allowing them to use malware to steal personal information.

SAFETY TIPS FOR CYBER CRIME

Do not Share USB Drives

- Though USB flash drives are hard to track physically, being stored in bag, pocket, jacket, purse, cupboard but can be dangerous if left at unattended workstations.



A survey shows end users most frequently copy:

- Customer data (25%)
- Financial information (17%)
- Business plans (15%)
- Employee data (13%)
- Marketing plans (13%)
- Intellectual property (6%)
- Source code (6%)

SAFETY TIPS FOR CYBER CRIME

- Install anti-virus software that will scan any device that connects to your PC via a peripheral port. (Such as USB).
- Never connect a found jump drive or media device to a PC. Give any unknown storage device to security or IT personnel near where you found it.
- Disable the Auto Run and AutoPlay features for all removable media devices. These features automatically open removable media when it's plugged into your USB port or inserted into a

SAFETY TIPS FOR CYBER CRIME

Use firewalls with VPN system to stop DDoS and password protected Wi-fi

Insert firewalls



SAFETY TIPS FOR CYBER CRIME

- Keep your personal and business data separate. Don't plug your personal audio player into your work PC or your work jump drive into your home PC.
- Secure all sensitive data stored on jump drives using strong encryption, Also be sure to have a backup copy located in a secure location.
- When you have finished transferring sensitive data from a USB drive, be sure to delete it using a secure delete utility.

SAFETY TIPS FOR CYBER CRIME

Secure USB Drive

- Manually Save Files with a Password
- Control and Limit: In addition to malware scanning, limits can be set on allowed USB devices and file types based on the user's role at the organization.
- Avoid Direct Plug-Ins, the USB security system can securely transfer the allowed files from the USB drive to a corporate portal from where the user can download the files.

SAFETY TIPS FOR CYBER CRIM

Make Web Browsing Secure by Following these Steps

- Don't download free media
- Don't store your payment information online
- Don't overshare personal information on social media accounts
- Change passwords regularly
- Keep your browser software up-to-date
- Run anti-virus software

SAFETY TIPS FOR CYBER CRIME

- Scan downloaded files before executing
- Watch out for phishing
- Don't reuse passwords
- Use HTTPS: The "s" in "https" stands for secure
- Read privacy policies
- Regularly monitor your bank statements
- Disable stored passwords
- Turn on your browser's popup blocker

Ransomware

- A ransomware is a type of malware that locks your files, data or the PC itself and extorts money from you in order to provide access.
- This is a new way for malware writers to 'collect funds' for their dishonest activities on the web.
- The second type of ransomware prevents access to files to potentially critical or valuable files like documents and spreadsheets Ransomware is considered "scare ware" as it forces users to pay a fee (or ransom) by scaring or threatening them.

HOW RANSOMWARE ATTACKS WORK



Spam attachment

Ransomware comes inside an email attachment



Malware execution

Malware gets installed on machine



Files encryption

All files are encrypted rapidly



Computer locked

Access to computer is blocked



Ransom demand

Payment demanded to retrieve access to computer

What can you do to protect against ransomware

- Back up your data
- Disable files running from AppData/LocalAppData folders
- Patch or Update your software
- Disconnect from Wi-Fi or unplug from the network immediately
- Use System Restore to get back to a known-clean state

SAFETY TIPS FOR CYBER CRIME

- Turn off the Bluetooth on any phones or devices. It prevents hackers' ability to steal contact lists and other information.



- Use HTTPS:// websites for online transactions
- Don't use same Pwds for all
- Delete Inactive accounts
- Screen locks on screens of mobile or computers
- Install apps from trusted sources

- Avoid sensitive information on mobile
- Avoid online offers
- Don't save debit cards/credit cards details on email and phones
- Use Cash on Delivery for unfamiliar websites



SELF-CHECK

Are You Ready To Protect Yourself From Cyber Crime?

- **Discipline**
- **Organized and systematic**
- **Honest**
- **Patience**
- **Respect**
- **Maintain Privacy**



HOME

REPORT WOMEN/CHILD RELATED CRIME ▾

REPORT OTHER CYBER CRIME

RESOURCES ▾

CONTACT US

HELPLINE

Filing a Complaint on National Cyber Crime Reporting Portal

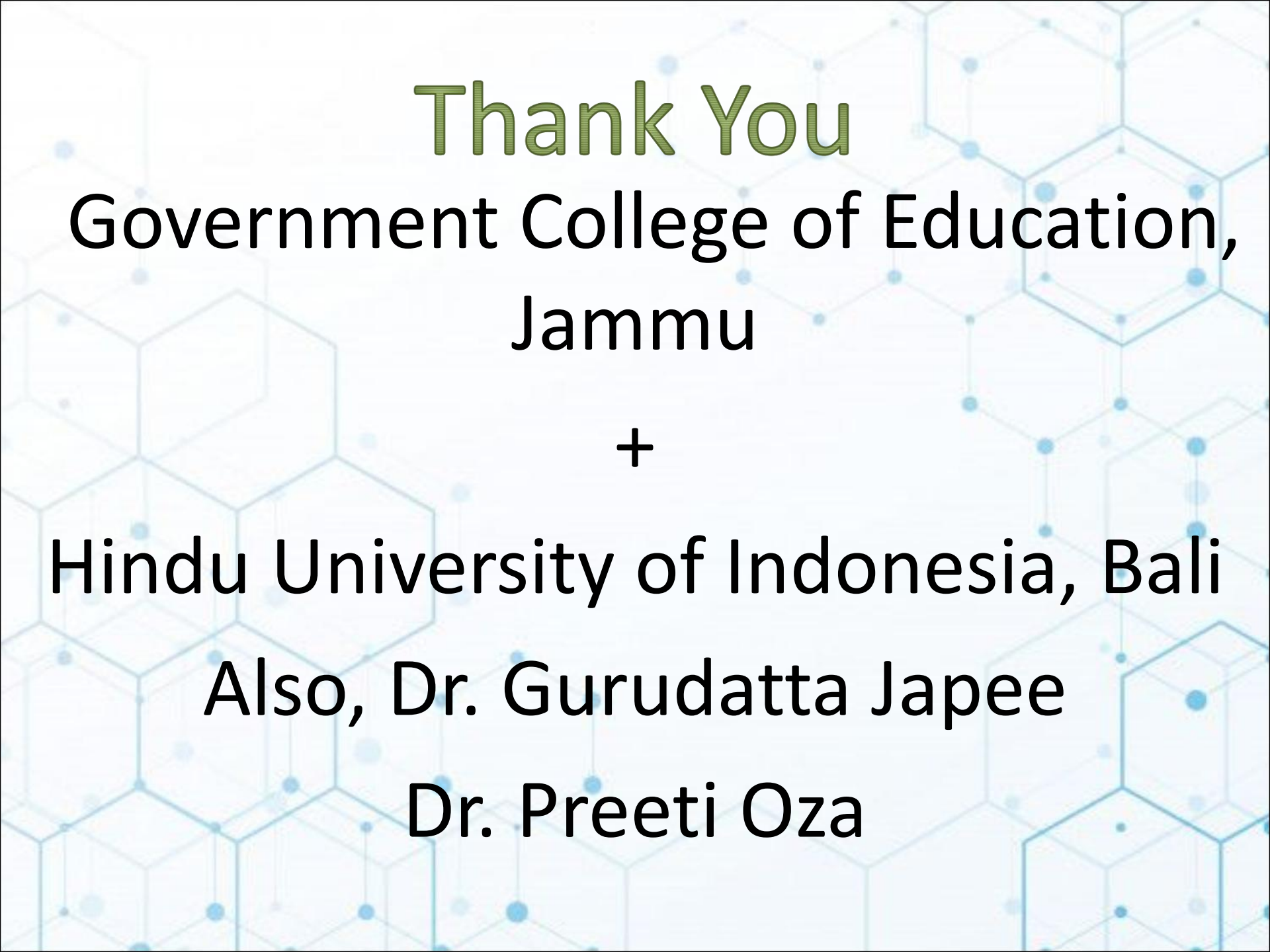
This portal is an initiative of Government of India to facilitate victims/complainants to report cyber crime complaints online. This portal caters to complaints pertaining to cyber crimes only with special focus on cyber crimes against women and children. Complaints reported on this portal are dealt by law enforcement agencies/ police based on the information available in the complaints. It is imperative to provide correct and accurate details while filing complaint for prompt action.

Please contact local police in case of an emergency or for reporting crimes other than cyber crimes. National police helpline number is 100. National women helpline number is 181.

[Learn about cyber crime](#)

[File a complaint](#)





Thank You

Government College of Education,
Jammu

+

Hindu University of Indonesia, Bali

Also, Dr. Gurudatta Japee

Dr. Preeti Oza

drpriyankakacker@gmail.com

Thank You!

