

IMPORTANCE OF DATA PROTECTION & ONLINE SECURITY

Ms. Kajal Kashyap
CDAC NOIDA

प्रगत संगणन विकास केन्द्र

Centre for Development of Advanced Computing

अनुसंधान भवन, सी-56/1, संस्थागत क्षेत्र, सैक्टर- 62, नोएडा- 201307 (उ.प्र.) भारत

Anusandhan Bhawan, C-56/1, Institutional Area, Sector- 62, Noida- 201307 (U.P.) India

THE INTERNET IN INDIA BY 2021

730

Million
Internet
Users

70
%

E-commerce
transactions are via
mobile

50
%

Travel
transactions are
in online

175

Million
Online
shoppers

1.10

Billion mobile
connections

448.
0

Million Social
Media Users

WHAT IS CYBER CRIME

•Cybercrime is criminal activity that either targets or uses a computer, a computer network or a networked device.

‘A major attack vector of Cyber Crime is to exploit broken software’



THREATS IN COMMON APPS USED

- Online Taxi Applications
- Education Applications
- Banking Applications
- Shopping Applications
- Job Portals
- Chatting/ Instant Messaging Applications
- Travel and Hotel Booking Applications
- Online Gaming



WHAT IS CYBER SECURITY

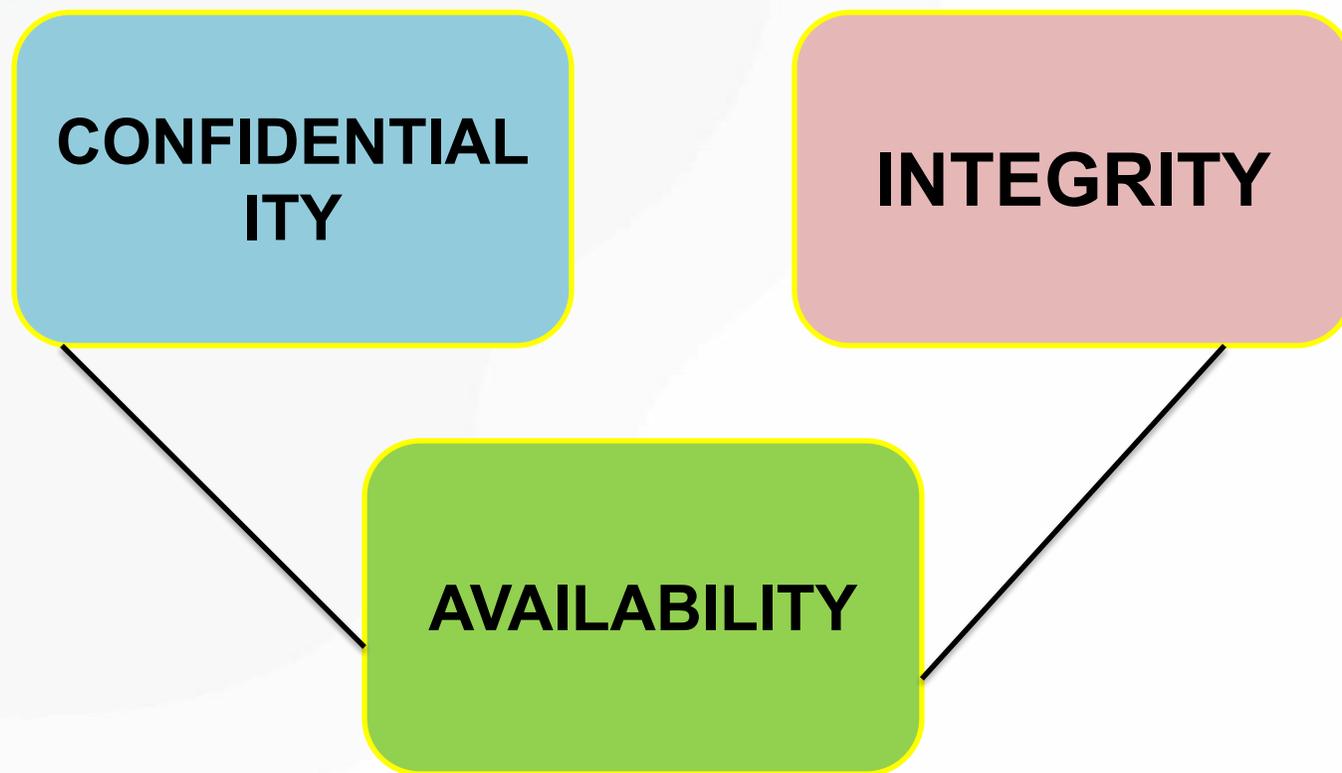
‘Cyber Security is the body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access.’



INTERNET USERS () SECURITY THREATS ()

‘A major part of Cyber Security is to fix broken software’

GOALS OF CYBER SECURITY



2021 This Is What Happens In An Internet Minute



Created By:
@LoriLewis
@OfficiallyChadd

HOW DOES **GOOGLE** TRACK YOU ?



CHROME

Browser history,
website visited



YOUTUBE

Videos watched,
uploaded



MAPS

Locations visited,
place searched



HANGOUTS

Contacts,
conversations



PHOTOS

People and
places tagged



CALENDER

Upcoming plans,
appointments



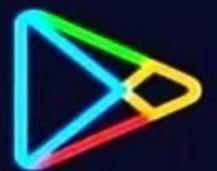
SEARCH

Queries searched



GMAIL

Contacts, emails
sent, email content



SHOPPING

Products searched,
clicked on



ADS

Ads clicked,
topic intrested in



NEWS

News sites viewed,
stories read

DIGITAL FOOTPRINTS

It is the information that exists online about you and your activity.

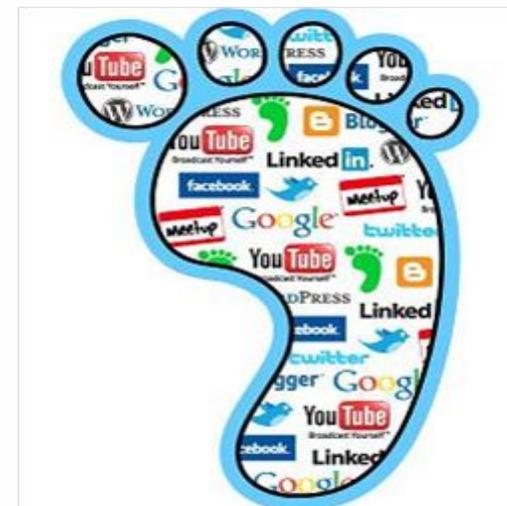
What are examples of digital footprints?

- Your search history.
- Text messages, including deleted messages.
- Photos and videos, including deleted ones.
- Tagged photos, even those you never wanted online.
- Likes/loves on sites like Facebook and Instagram.



DIGITAL FOOTPRINTS

- Be Careful About –
- - **What you share**
- - **Where you share**
- - **With whom you share**
- There are two kinds of Digital Footprints -
 - **Passive Digital Footprint**
 - **Active Digital Footprint**
- Be Smart About –
 - **Sites you visit**
 - **Emails you open**
 - **Links you click**



HOW TO PRESERVE YOUR DIGITAL FOOTPRINT?

- Always think long term before posting.
- Avoid Making Virtual or Online Friends.
- Keep your personal information private.
- Verify the profile on different platforms like LinkedIn, Twitter, Instagram and Facebook.
- Use privacy settings on social networking pages
- Protect your privacy and privacy of your friends
- Have a time limit on the time spend on social media.

PASSWORD SECURITY



VARIOUS TECHNIQUES USED BY HACKERS/CRACKERS TO RETRIEVE YOUR PASSWORDS

**SHOULDER
SURFING**

**WRITING YOUR
PASSWORDS ON
PAPERS OR
STORING IT ON
HARD DISK**

**BRUTE FORCE
ATTACKS**

**DICTIONARY
ATTACK**



BEST PRACTICES TO KEEP PASSWORD SAFE

- Use a different Password for each Service
- Use a long and complex Password
- Change Password regularly
- Do not use your passwords on a shared computer
- Use Passphrase

SWITCH TO PASSPHRASE

MY PASSPHRASE



Never judge a book by its cover

MY PASSWORD



nj@66!C



Never judge @ 6ook 6y !ts c cover

PREVENTIONS

The Indian national flag is visible in the top left corner of the slide, showing the saffron, white, and green horizontal stripes and the Ashoka Chakra in the center.

Refresh the browser after returning back from other tabs.

Avoid Financial Transactions on tabbed browsing

Avoid Phishing Emails and questionable websites.

Always use updated Antivirus Software.

Don't fall for ads that tempt you into downloading free software.

Use Private Browsing.

Increase your browser security settings.

Always clear Cookies and Cache, history daily.

PREVENTIONS

- Disable auto-connect when joining networks
- Never re-use passwords for Wi-Fi
- Change the Name of Your Default Wi-Fi Network
- Disable Your Wireless Home Network While You're Not at Home
- Do use two-factor authentication on everything possible.
- Don't install apps from a third party
- **Record IMEI number:** Record the unique 15 digit IMEI number. In case Mobile phone is stolen/lost, this IMEI number is required for registering complaint at Police station and may help in tracking your mobile phone through service provider.

PREVENTION TIPS



Never Open E-Mail attachments With the file extensions Such as VBS,SHS,PIF etc



Never open Web-links in your e-mail.
Always type links in Web browser

Always use e-mail transaction through secured mail sites

Never download anything from e-mail when the sender is unknown or the attachment has a doubtful name

New viruses creep upon a daily basis. It is important that we do back up our valuable data files regularly



Check for spelling mistakes.
Fake job offer mails generally have spelling mistakes and grammatical errors



Never trust the icons in the e-mail attachment. The virus file may be shown as PDF file.

Never send your photograph through e-mail to unknown persons.



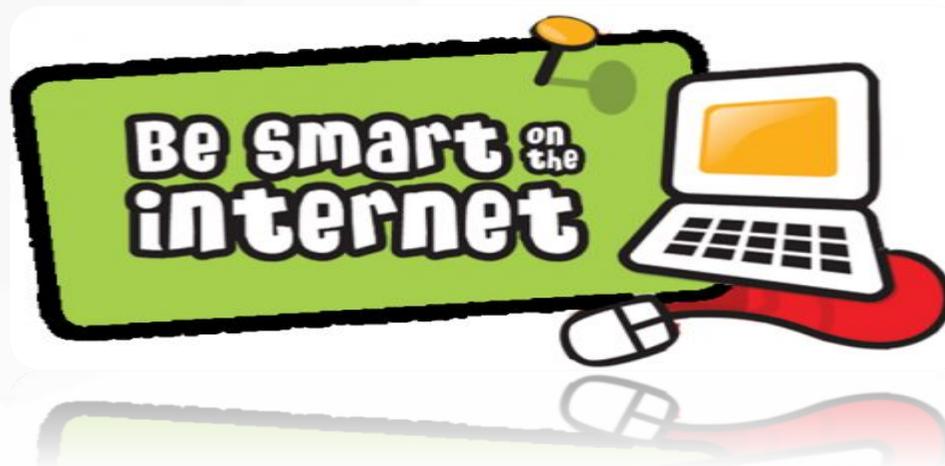
Don't respond to spam mails without verification of the e-mail origin

CONCLUSION

The only system which is truly secure is one which is switched off and unplugged.

So , only way to be safe is Pay attention and Act smart.

- **The Mantra of Online Safety**
- **‘Pause & Think before you Connect’**
- **‘Secure Yourself and Secure the Nation’**



THANK YOU!

STAY SAFE STAY SECURE

Do Your Part

#Becybersmart