Social Media

Usage and Challenges

A SOCIAL NETWORK...

Is a social structure where users establish relationships based on their   common interests
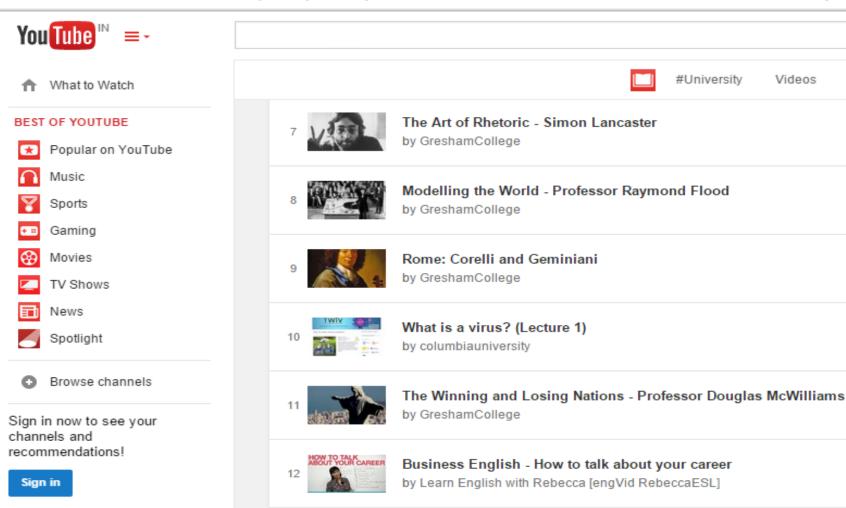
What is Social Media?

Social media depend on computer-mediated tools, mobile and web-based technologies to create highly interactive platforms through which individuals and communities share pictures/videos, co-create, discuss, exchange information and modify user-generated content.

We are now collaborators and producers of information

Every person has the ability to contribute ideas and experiences through various electronic

Youtube is the most popular video based social media on the planet (Any registered user can upload videos)

facebook

Instagram

Tumbler

Flicker

Linkedin

Twitter

Google Plus

Pinterest

The Naga Blog: A group on facebook with 71,400 members

Zhoku Rhakho
April 6 at 2:21pm · Edited

LOST & FOUND
A BLACK BAG containing the following items has been found dropped in a car at Dimapur town probably by mistake!! the rightful owner is therefore requested to reclaimed it by identifying the same.
ITEMS
1. Signed cheque of Rs. 1 lakh for Govt. Middle School teachers, Kehuto (Niuland)
2. Five passbooks and cheques... See More

Unlike · Comment

👍 You, Thejakhrietuo Kire, Atsung Imchen, Nokchem Angth and 198 others like this.

💬 View 29 more comments

Toka Assumi God bless u!!!!
Yesterday at 2:38pm · Like

Akum Meren Longchar U will be the next MLA...thumbs up.
14 hrs · Like

Khrievotuo Sekhose So proud of you brother Zhoku Rhakho! You set an good example for our society ..keep it up and may GOD bless you
10 hrs · Edited · Like

Hetoka Awomi God bless u.
13 mins · Like

✓ **Open discussions**
✓ **Online Blood Bank**
✓ **Lost and Found**
✓ **Offline campaigns**
✓ **Debates, Discussions**
✓ **Research, Surveys**

- **Students**
- **Politicians**
- **Bureaucrats**
- **Scientists**
- **Engineers**
- **Scholars**
- **Journalists**
- **Musicians**
- **Activists**
- **Academicians etc**

E-Commerce
Nagaland Open Online Barter and Sell(Noobs on facebook)

I-Yanger Lemtur
10 mins

WagonR LXI, 2005. 51,000km done
₹180,000
📍 Dimapur

Well maintained and negotiable.
Contact- 8575658503

Effective use of social media by Government-I

Effective use of social media by Government-II

Nagaland Public Service Commission
July 29, 2015 · 🌐

Advertisement No. NPSC-3/2015 dt. 29.07.2015 (NCS, NPS, NSS & Allied Services Examination 2015)

Link to NPSC Website:
http://www.npsc.co.in/advertisements/3313.html...

Continue Reading

👍 Like   💬 Comment   ➤ Share

⊕ Nyukshing Lam, Akani Kiho and 79 others   Chronological ▾

17 shares

Alem Jamir Can i reapply a new form altogether? I made a silly error while applying the other day! Does the Instruction No. 3b allow me to do so? That is to apply a fresh new application? Kindly clarify Sir/ Madam. Thank you.
Like · Reply · August 4, 2015 at 3:54pm · Edited

Nagaland Public Service Commission Joseph Naga
Upper age limit for ST candidates is 35 years. If you have selected "ST" under Sl. No. 7 Category then you need not apply again.
Like · Reply · August 5, 2015 at 10:20am

✓ **Engaging citizens**

✓ **Bridging the trust and confidence of the public**

✓ **Detection and control of crime**

✓ **Disaster Management**

✓**Traffic Regulation**

✓ **Dissemination of information**

✓ **Collection of feedback**

✓ **Conducting surveys and polls**

Challenges/Misuse of Social Media

Types of Cyber Crimes :

• Cyber Bullying, cheating by Personation, Identity Theft

• Obscene Material, Offensive/Harassing Messages,Cyber Extortion

• Virus Attacks, Hacking,

• Publishing/Circulation of Rumours especially hurting religious,

  tribal and communal sentiments

• IPR violations, Financial Frauds, Skimming, Cyberstalking

• Cyber Terrorism

To register a Cyber Crime related complaint, the same should be

lodged with a local police station or Cyber Crime Cell (if available)

Cyber Crimes - 1

- **Hacking**

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

- **Child Pornography**

  The Internet is being highly used by its abusers to reach and abuse children sexually, worldwide.

- **Cyber Stalking**

  Cyber Stalking can be defined as the repeated acts harassment or threatening behavior of the cyber criminal towards the victim by using internet services.

- **Denial of service Attack**

  This is an act by the criminal, who floods the bandwidth of the victim's network or fills his e-mail box with spam mail depriving him of the services he is entitled to access or provide

Cyber Crimes - 2

- **Virus Dissemination**
  Malicious software that attaches itself to other software (virus, worms, Trojan Horse etc).

- **Software Piracy**
  Theft of software through the illegal copying of genuine programs or the counterfeiting and 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.

Cyber Crime - 3

Phishing

The act of sending an e-mail to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft. The e-mail directs the user to visit a Web site where they are asked to update personal information, such as passwords and credit card, social security, and bank account numbers, that the legitimate organization already has.

Credit/ Debit Card Fraud

The unauthorized and illegal use of a credit card to purchase property.

Legal Provisions(IT Act 2000)

66A: Sending offensive messages through communication service, causing annoyance etc through an electronic communication or sending an email to mislead or deceive the recipient about the origin of such messages (commonly known as IP or email spoofing) are all covered here. **Punishment for these acts is imprisonment upto three years or fine.**

66B: Dishonestly receiving stolen computer resource or communication device with **punishment upto three years or one lakh rupees as fine or both.**

66C: Electronic signature or other identity theft like using others' password or electronic signature etc. **Punishment is three years imprisonment or fine of one lakh rupees or both.**

66D: Cheating by personation using computer resource or a communication device shall be punished with **imprisonment of either description for a term which extend to three years and shall also be liable to fine which may extend to one lakh rupee.**

LEGAL PROVISIONS (INDIAN TELEGRAPH ACT 1885)

Section 5. Power for Government to take possession of licensed telegraphs and to order interception of messages

(1) On the occurrence of any public emergency, or in the interest of the public safety, the Central Government or a State Government or any officer specially authorized in this behalf by the Central Government or a State Government may, if satisfied that it is necessary or expedient so to do, take temporary possession (for so long as the public emergency exists or the interest of the public safety requires the taking of such action) of any telegraph established, maintained or worked by any person licensed under this Act.

(2) On the occurrence of any public emergency, or in the interest of the public safety, the Central Government or a State Government or any officer specially authorized in this behalf by the Central Government or a State Government may, if satisfied that it is necessary or expedient so to do in the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of an offence, for reasons to be recorded in writing, by order, direct that any message or class of messages to or from any person or class of persons, or relating to any particular subject, brought for transmission by or transmitted or received by any telegraph, shall not be transmitted, or shall be intercepted or detained, or shall be disclosed to the Government making the order or an officer thereof mentioned in the order:

Provided that press messages intended to be published in India of correspondents accredited to the Central Government or a State Government shall not be intercepted or detained, unless their transmission has been prohibited under this sub-section
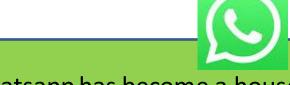
Legal Provisions
IT ACT 2008 - Section 66 A

However, The Supreme Court declared Section 66A of Information Technology Act as unconstitutional on March 24, 2015 as making it further difficult for the police to harass innocent for their comments on social network sites.

TWO OF THE MOST POPULAR SOCIAL MEDIA IN NAGALAND

facebook

- FB is one of the most popular social media
- Subscriptions of Nagaland based facebook groups and pages have surpassed newspaper subscriptions
- Facebook introduced CONTENT REGULATION wherein sensitive content can be reported to facebook and taken down

- Whatsapp has become a household application
- Almost every person with a smart phone from the village to the city uses whatsapp extensively
- Whatsapp has no Content Regulation unlike facebook
- videos and pictures which go viral and defaming cannot be reported on whatsapp

CERT-In

Indian Computer Emergency Response Team

- CERT-In is the national nodal agency functioning since January 2004 for responding to computer security incidents as and when they occur.

- In the recent Information Technology Amendment Act 2008,CERT-In has been designated to serve as the national agency to perform the following functions in the area of cyber security:

  a) Collection,analysis and dissemination of information on cyber incidents.

  b) Forecast and alerts of cyber security incidents Emergency measures for handling cyber security incidents Coordination of cyber incident response activities.

  c) Issue guidelines,advisories,vulnerability notes and whitepapers relating to information security practices,procedures, prevention,response and reporting of cyber incidents.

Telecom Enforcement, Resource and Monitoring (TERM) Cells

- With the increasing number of telecom operators in the country, TERM Cell has been set up in all the Licence Service Areas and Large Telecom Districts of the country. It is meant to ensure that telecom service providers adhere to the licence conditions and also take telecom network security issues. Following are main functions:

- Inspection of premises of Telecom and Internet Service Providers

- Curbing illegal activities in telecom services

- Control over clandestine / illegal operation of telecom networks by vested interests having no license

- To file FIR against culprits, pursue the cases, issue notices indicating violation of conditions of various Acts in force from time to time.

- Analysis of call/subscription/traffic data of various licensees.

- Technical arrangement for the lawful interception / monitoring of all communications passing through the licensee s network.

- To ascertain that the licensee is providing the services within permitted area.

- Co-ordination with all service providers.

- Matters related to national security.

- Disaster Management: Taking over of network in the events of natural calamities or the other emergency situations.

- Grievance redresses of subscribers in respect of deficiency by various operators.

- Technical interface between Security Agencies and Telecom Service Providers

Framework &Guidelines for Use of Social Media for Government Organisations

In order to encourage and enable government agencies to make use of this dynamic medium of interaction, a Framework and Guidelines for use of Social Media by government agencies in India has been formulated.

Example of use of Social Media
Prime Minister Narendra Modi's Facebook page

What is Cyber Security?

- Cyber security is the prevention of damage to, the protection of, and the restoration of computers, electronics communications systems, electronic communication services, wire communication and electronics communication, including information contained therein, to ensure its confidentiality, availability, integrity and authentication.

- Security as a process typically includes three key elements :
  1. Prevention: It deals with the implementation of security controls and   countermeasures.
  2. Detection: Deals with monitoring the IT infrastructures and assets.
  3. Response: is a reaction that an organisation takes in response to a   security breach.

Way forward - 1

✓ Awareness and sensitisation on responsible use of social media should be conducted.

✓ Every service providing Departments like Power, PHED, Education etc may be advised to use social media to provide better services. E.g. Dimapur Police and NPSC.

✓ Social Media monitoring cell may be set up to address social media and cyber crime related issues

✓ Police modernisation is required to address cyber crime as most of the current crimes are now cyber related.

Way forward - 2

✓ Robust cyber forensic lab should be established in Police Head Quarter

✓ A separate police cyber wing headed by IGP may be established

✓ Cyber Legal cell should be established to handle critical cyber crime cases

✓ All district Head Quarters should have a **Cyber Crime Police Station**(Eg. Bangalore Police). (As per the amendments to the IT Act 2000 , the minimum rank of investigation of cyber crimes is Police Inspector and any jurisdictional police station can register and investigate).

Mumbai Police

The Invisible Criminal is Dangerous than the visible one.

He uses technology as his weapon; we use the same to nab him.

Cyber crime training facilities

	States	Purpose
1	Kerala	Cyber forensic training and investigation laboratories for training law enforcement agencies and judiciary.
2	Assam	
3	Mizoram	
4	Nagaland	
5	Arunachal Pradesh	
6	Tripura	
7	Meghalaya	
8	Manipur	
9	Jammu & Kashmir.	

Cyber laboratory

Sl.No	City	Purpose
1	Mumbai	In collaboration with Data Security Council of India (DSCI), NASSCOM(National Association of Software and Services Companies), Cyber Forensic Labs have been set up at Mumbai, Bengaluru, Pune and Kolkata.

Since their inception, these laboratories with the support Department of Electronics and Information Technology, (DeitY), GoI has trained over 45,000 personnel through these cyber labs. Apart from that regular training program like special trainings for CBI Academy, North Eastern Police Academy, National Police Academy, National Institute of Criminology and Forensics Sciences were also conducted by the DSCI team. |
2	Kolkata	
3	Pune	
4	Bengaluru	
5	Hyderabad	

THANK YOU