IS NOT A GAME... IT'S YOUR LIFE

STAY SAFE ONLINE !

A presentation on Cyber Safety Awareness..... It's better to be Alert than Sorry!

WHY BEING CYBER SAFE IS IMPORTANT ?

Rising at an alarming rate, the number of cyber crimes in the country may double to 3 lakh in 2015 and could pose serious economic and national security challenges, an Assocham-Mahindra SSG study has warned.

India has emerged as a favourite among cybercriminals, mostly hackers and other malicious users who use the Internet to commit crimes such as identity theft, spamming, phishing and other types of fraud.

Teen hackers held for ₹8 lakh cyber fraud

Jaipur: After carrying out a two-and-a-half month-long technical investigation, the cyber crime police arrested two Information Technology (IT) students from Shimla for allegedly hacking into Data Infosys e-processing system and fraudulently recharging BSNL's pre-paid mobile phones worth Rs 8 lakh. The students used a cyber café to hack into the Data Infosys's website. The youths, Kulshrestha Varma and Hardik Sud, both 19-year-olds, are second-year students of APG University's IT department in Shimla.

They suspect involvement of several other people in the crime.

DSP, cyber crime, Rajendra Sharma told TOI that one Yogita, a representative of Data Infosys, lodged an FIR on December 3 in this connection. "Gupta said Data Infosys runs an e-commerce set-up to recharge pre-paid mobile connections of BSNL," said Sharma. In November, the company found during an audit that someone had hacked into

Fake identity may lead to real crisis

Next time you provide fictitious details about yourself on the net or use offensive language, you could risk being sent to jail for it. As a new proposed law brings all this under the ambit of the IT Act, *DT* does a reality check

While making your email ID or opening a new account on a social networking site, did you fudge your details like 90 per cent of the net users do? After all, chatting or

the net, why would any sane person want to reveal all true details? Also, as far as posting offensive messages are concerned, who will decide the definition of offensive?"

Actor Shreyas Talpade found himself

says, "Internet should be used for the right reasons. If this screening process is put through, the number of evil frauds and harassment issues will be addressed."

Whither implementation?

The experts feel so too. Says NASSCOM president Kiran Karnik, "The proposed act will discourage illegal activities on the Net. I expect a substantial reduction in impersonation and harassment cases."

Hacker breaches Rahul cyber-security

Smriti Singh & Neeraj Chauhan | TNN

New Delhi: This is one aam admi outreach Rahul Gandhi will not appreciate. In April, when the Congress general secretary was in the thick of poll campaigns, hackers were busy breaking into two web servers created by him for family constituencies in Uttar Pradesh. Passwords were illegally accessed and the internet address tweaked to redirect web users onto an engineering college website.

The web servers – amethinet and raebareli – are maintained from 12 Tughlak Lane, Rahul Gandhi's bungalow, round the clock by his own team of technical experts. On April 8, some of them noticed suspicious activity on the network. The site was getting redirected and the email accounts blocked. An FIR was lodged, stating, "officials found that amethi.net website is not accessible". A case was registered under 66 Information Technology Act. The Special Cell of Delhi Police is now on the lookout for the hacker.

"Technically, the hacker cracked the whole domain system of the server and used an email to get the passwords," a senior officer who is part of the probe said.turns here

The hacking reportedly took place between April 4 and April 19. Sources said the servers and websites at 12 Tughlak Lane maintained information on the constituencies of Rahul Gandhi and his mother, Congress chief Sonia Gandhi. The young MP's house is also a hub of policymaking for Youth Congress and the systems store huge databases in terms of constituencies, individuals and trends, they said.

Amethinet and raebareli were created specifically to address the constituents, but the former, after hacking, opened onto www.pdmce.ac.in, the website of an engineering college in Bahadurgarh, Haryana. When Rahul's team checked the domain name system (DNS) of the website, it showed an IP address different from that of Rahul Gandhi's network. "Amethinet domain is registered with godaddy.com domain and when officials tried to log in to the domain management console, it was not working," the FIR said.

Email IDs created for password recovery was also hacked. "The login and password for this email was also not working," said the complaint. As experts reset the password for amethi@hotmail.com and accessed the account, they found several suspicious emails. "These emails were sent by domain management console – godaddy.com (of amethinet) – to an unknown person on his request regarding password recovery," says the FIR.

Officials said the recovered emails revealed the times at which IP address password recovery requests were generated by the hacker. "The unknown hacker has cracked all of our domain management console passwords using password recovery email account amethi@hotmail.com and has made changes in DNS zone files so that it got redirected into some other websites," the FIR said.

Student held for cyber crime

Staff Correspondent

HUBLI: In a joint operation, the Hubli police and the Cyber Crime Investigation Cell of Chandigarh solved a case reported from Hubli by arresting a 20-year-old hotel management student from Chandigarh.

The arrested student, Sahil Sharma, is the son of a senior Haryana Government official. He has been arrested on the charge of fraudulent use of credit cards of people residing outside the country.

The police action follows a complaint by Deepali Gotadke, who runs e-commerce site Clickhubli.com using which customers abroad send flowers and gifts to their friends and relatives in India.

Ms. Deepali takes orders through payment gateway provided by a firm called CCNOW based in the U.S. In August and September 2008, she received three orders from Reji Abraham, a resident of the U.S. And as per the orders, three mobile handsets worth Rs. 75,000 were delivered to Komal Goel, a resident of Gurgaon in Haryana.

Although Ms. Deepali received the amount for the order, the firm which takes the order recovered the amount from her after Mr. Abraham claimed that he had not placed any order for the mobile handsets.

Ms. Deepali then started processing her orders carefully and got suspicious when she received orders for two more mobile handsets from the same email ID through which she had earlier received one of the first three fraudulent orders. These orders had been placed on behalf of Shiela Lane from Britain and Kerrie Sheldon from the U.S. and wanted the handsets to be delivered to Sahil Sharma in Chandigarh.

Ms. Deepali was able to trace the IP addresses of the computers from which the emails had been sent and got confirmation that the orders had been placed from India itself. She then filed a complaint with the Hubli police.

Hubli-Dharwad Police Commissioner N. Shivakumar sent a team to Chandigarh, who in a joint operation on January 8 arrested the accused by sending a courier boy as a decoy.

According to the Police, Sahil worked for an international call centre in 2006 where he used to sell mobile phones to international customers and note their credit card numbers for the company's record. Meanwhile, Sahil Sharma was released on bail by a Hubli court on Saturday.

मुख्यमंत्री ने इओयू को 15 दिनों में प्रस्ताव तैयार कर भेजने का दिया आदेश

सभी जिलों में साइबर क्राइम यूनिट

संवाददाता, पटना

सभी यूनिट में साइबर दारोगा, इंस्पेक्टर व आइटी एक्सपर्ट होंगे बहाल

साइबर क्राइम से जुड़े अपराधी अब कानून से बच नहीं पायेंगे. मुख्यमंत्री नीतीश कुमार ने सभी जिलों में आधुनिक साइबर क्राइम यूनिट जल्द खोलने का आदेश दिया है. आर्थिक अपराध इकाई (इओयू) को 15 दिनों के अंदर इसका प्रस्ताव तैयार कर भेजने को कहा है. मुख्यमंत्री ने शुक्रवार को अपने कैंप कार्यालय में दूसरे दिन विधि-व्यवस्था पर खास समीक्षा बैठक के दौरान मुख्य रूप से पुलिस आधुनिकीकरण को लेकर चर्चा की और पुलिस की जरूरतों और समस्याओं को जाना. आधुनिकीकरण के इस दौर में साइबर क्राइम के मामलों में तेजी

शुक्रवार को लगातार दूसरे दिन विधि-व्यवस्था की समीक्षा बैठक करते सीएम.

ऐसा होगा साइबर क्राइम यूनिट

इस आधुनिक साइबर क्राइम यूनिट में एक साइबर इंस्पेक्टर, एक दारोगा समेत दो आइटी एक्सपर्ट की तैनाती की जायेगी. इनका मुख्य काम साइबर अपराध से जुड़े क्राइम यूनिट के तर्ज पर तैयार किया जायेगा. सभी जिलों के एसपी ऑफिस इसका अलग से सेल बनाया जायेगा.

17 को सीएम अपराध की करेंगे जिलावार समीक्षा

पटना. मुख्यमंत्री 17 फरवरी को विधि-व्यवस्था और अपराध नियंत्रण को लेकर जिलावार समीक्षा करेंगे. विधि-व्यवस्था पर दो दिवसीय राज्य स्तरीय समीक्षा बैठक करने के बाद अब माइक्रो स्तर पर क्राइम की समीक्षा करने के लिए जोन, जिला और थानों का गहन अवलोकन किया जायेगा. सीएम वीडियो कॉन्फ्रेंसिंग से सभी आइजी, डीआइजी और एसपी के साथ समीक्षा करेंगे. किसी थाने में किस तरह के अपराध होते हैं, इसकी जांच-पड़ताल होगी.

Cyber crime against women on the rise

Little Yadav

MUMBAI: While social networking and micro-blogging sites are great tools to stay connected, they are also easy to misuse. And mostly, it's women who are the victims, say the cyber crime police.

An increasing number of women are approaching the cyber crime cell with complaints that fake profiles of them with obscene content have been posted on sites such as Facebook, Orkut and Twitter.

In 2009, the police received as 268 applications of fake profiles, obscene content and defamation, but only nine cases were registered.

They have received 160 applications till June 30 this year, but only six cases have been registered so far.

ON GUARD

YEAR	APPLICATIONS RECEIVED	CASES REGISTERED
2008	254	6
2009	268	9
2010 (till June 30)	160	6

- Let your passwords be more than 10-15 characters and something that cannot be easily guessed.
- Don't share you passwords even with close friends or your partner.
- Don't save your passwords on your mobile phones or emails.
- Don't add strangers to your friends' lists.
- Don't post your photos and personal information on networking sites.

ILLUSTRATION: SHRINIVASAN

Though such incidents are on the rise, few victims are willing to register a case.

Explaining this, cyber security consultant Vijay Mukhi, who often works with the police in such cases, said victims are afraid to proceed with complaints as that could lead to exposure and social humiliation.

"Most victims want the obscene profiles deleted after which they are not interested in proceeding with complaints."

"In the few cases we have solved, the accused has turned out to someone known or very close to the victim," Mukhi added. Bhimrao Sonawane, deputy commissioner of police (preventive), agreed: "Most complainants prefer withdrawing their applications once the offender has been traced. Also, it depends on the seriousness of the offence. While some put crude content, others upload morphed photos and in some cases the phone number of the victim."

Often, victims are careless and tend to add strangers, even from other countries, on their sites. "Our police do not have jurisdiction in such cases, so often the case has to be closed after deleting the profile," Mukhi said.

To add to the problem, tracing the accused is tough as they create profiles from places to which they cannot be traced back, such as cyber cafés far from where they live, or unsecured wi-fi connections.

CYBER CRIMES EVERYWHERE

As per the study's findings, total number of cyber crimes registered during 2011, 2012, 2013 and 2014 stood at 13,301, 22,060, 71,780 and 1,49,254 respectively.

And its increasing at an alarming rate!!!

556 million victims
*** 42 million** in India

COST OF CYBERCRIME

Direct costs associated with global consumer cybercrime
$110 billion in 12 months

556 million victims
*** 42 million** in India

1.5 million adults fall victim to cybercrime everyday – i.e., 18 victims every second

HOW ?

WHO IS AFFECTED MOST?

HIGHEST NUMBER OF CYBERCRIME VICTIMS FOUND IN:

Russia **92%**
China **84%**
South Africa **80%**

Source: Norton
GRAPHIC: B. SRINIVASAN

CYBER CRIME BYTES

BANGALORE accounts for 24.4 per cent of cyber crimes booked under the IT Act among 53 'megacities' across India.

CITY TOPS national charts with 342 cyber crime cases booked in 2012, up from 117 in 2011

KARNATAKA RANKS third in the country with 412 cyber crime cases

registered in 2012. Bangalore accounts for approximately 83 per cent cases being booked in the State

OF 412 cyber crime cases, 323 under IT Act or IPC in Bangalore fall under 'loss/ damage to computer resource' and 'hacking'.

Source: National Crime Records Bureau

WEB OFFENCES

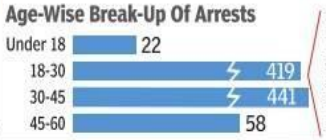
Crime in city	2015	2014	2013	2012	2011
Credit/debit card fraud	320	183	32	8	20
Obscene email/SMS/MMS	152	130	35	12	19
Hacking	26	43	8	2	4
Source code tampering	17	4	2	1	0
Threatening email/SMS	15	13	1	3	5
Phishing	5	4	3	3	9
Other	377	227	88	34	29
Total	912	604	169	62	86

MAHARASHTRA
Cyber crime cases registered under IT Act and IPC

Year	IT Act	IPC	Total
2014	511	1347	1,858
2013	681	226	907

Arrests In Mumbai

Age-Wise Break-Up Of Arrests



Cases under IT Act, IPC and SLL* in state in 2014
*Special and Local Laws

WHO IS BEHIND THESE CRIMES ?

Phishing attacks of online banking accounts or cloning of ATM/debit cards are common occurrences.

Maximum number of offenders belong to the

18-30 age group!!!

WE ARE SMART ! CRIMINALS ARE SMARTER !!

With increasing use of information technology (IT) enabled services such as e-governance, online business and electronic transactions, protection of personal and sensitive data have assumed paramount importance.

Smartphone users rarely check for security certificates while downloading apps (games, music and other software) from third party or unsecured sites, the study said, adding that mobile banking apps store data such as PIN and account number, on the phone.

There is a risk that if the phone is hacked or stolen, then the information is compromised.

THE INDEFINITE CYBERSPACE

Cyberspace is a man made world that is constantly evolving. It differs from the static physical world as it has no boundaries, no geographical mass and no gravity. It is limitless, constantly changing its shape, attributes and characteristics. It exists in a form of bits and bytes; it is an information driven world.

Regulating cyberspace means regulating both man and the machine. There is ethics, safety and security involved.

In Cyberspace, we have

Cyber Ethics exploring appropriate and ethical behaviours related to online environments and digital media. It includes plagiarism, bullying and hacking to name a few.

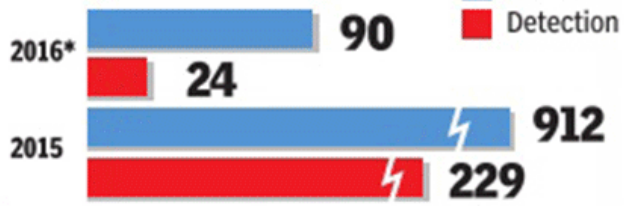
Cyber Safety defining how one operates on-line. It includes rules guiding how to keep personal information safe and limited.

Cybersecurity involving tasks undertaken on the computer to keep it secure from people who wish to harm it or use data stored on it unlawfully. This includes installing virus software and firewalls.

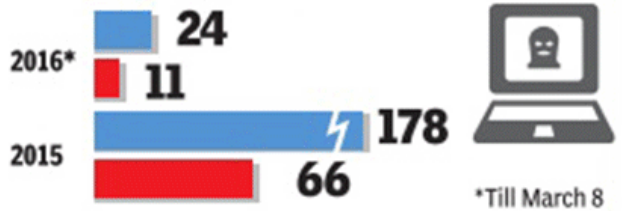
BE SOCIAL BUT BE CAREFUL WHEN U R VIRTUALLY SOCIAL

NO SOCIAL MEDIA ETHICS

Cyber Crimes Registered In Mumbai



Fake Facebook Profile Cases In Mumbai



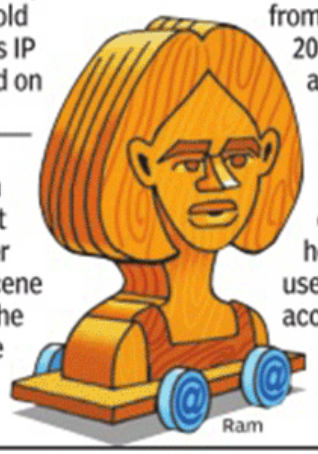
How To Curb Crimes

- Best way to curb such crimes, experts say, is implementing the law strictly. High profile arrests and people being jailed may be a deterrent
- Social media guidelines should be published at the community level and propagated in places of worship, schools and colleges as part of moral science

MAJOR CASES OF FAKE PROFILES REGISTERED IN 2015

August 15 | A 23-year-old woman complained about her fake FB profile and bulk friend requests sent to those known to her. Investigators tracked down a 26-year-old Chembur lawyer from his IP address. He was arrested on February 19, 2016

October 7 | A woman teacher from a suburban school complained about a fake profile made in her name, used to send obscene messages to students. The accused turned out to be a student she had reprimanded in school



October 10 | A 36-year-old woman found her fake profile was used to send friend requests to her brother's friends. The accused, a law graduate from UP, arrested in March 2016, said she dumped him after getting him to elope with her from his marriage years ago

December 17 | A 35-year-old woman complained her fake FB profile was used for obscene chats. The accused proved to be her brother-in-law, upset his mother favoured the victim over his wife

WHAT NOT TO DO ON SOCIAL MEDIA

- Don't give out personal information, like birth date, mother's maiden name
- Don't post personal pictures or your children's photos. These can be morphed for ransom
- Don't accept friend requests from people you don't know on social media accounts. Criminals get easy access to everyone on your friends list through it

- Avoid check-in on Facebook that may be used to track your location. Continuously checking into places makes it easier for criminals to track your lifestyle trends over a period of time
- Do not let children below the age of 13 have social media accounts. When they do get their own accounts, make them aware of the risks

DO NOT FEED THE PHISH

Phishing is the attempt to obtain sensitive information such as usernames, passwords, and credit card details (and, indirectly, money), often for malicious reasons, by disguising as a trustworthy entity in an electronic communication.

Phishing is typically carried out by email spoofing or instant messaging, and it often directs users to enter personal information at a fake website, the look and feel of which are almost identical to the legitimate one.

Don't TRUST strangers....

Fake Pages and Fake People on the internet may try to trap you!

Don't Get Phished

Never trust an unsolicited email, text message, pop-up window, Facebook message, etc. that asks you to: give sensitive information such as your Social Security or bank account numbers; click on a link or open an attachment; or send someone money.
Don't trust the message no matter how convincing or official it looks; no matter if it appears to come from your bank, the government, your ISP, or your best friend.

Use common sense! Always independently verify the authenticity of the message before you respond...

REAL VS FAKE : BE AN ONLINE SLEUTH

Cyber Criminals are now using fake facebook and twitter profiles to lure people (especially teenagers and businessmen) into a vicious honey trap. This may be followed by fixing a meeting, then kidnapping the victim and asking for a ransom. One should be careful while accepting friend requests and conversing with a stranger on such platforms.

It's a FAKE page !

One must know that a person chatting with you as a 16 year old girl may be a 45 year old man!

In August of 2012, CNN reported that there were currently over 83 MILLION fake / impostor Facebook profiles as of that time and that Facebook was working hard to rid their site of these frauds.

CYBER BULLYING : A CRIME THAT ATTACKS THE MIND

Cyberbullies use computers, cellphones, or other devices to harass, threaten, humiliate, or otherwise torment their peers. It may include hurtful text messages to the victim, or rumors spread through cellphones or online.

The psychological and emotional outcomes of cyber bullying are similar to real life bullying outcomes, except for the reality that with cyber bullying there is often no escape. School ends at 3 p.m., while the internet is available all the time.

Bullies create - web pages and videos to make fun of their peers;
- fake, humiliating profiles of the people they wish to intimidate on social networking sites.

Cyber-bullies have used mobile devices to take embarrassing photos or videos, and uploaded them for the world to see and discuss.

Nearly 43% of kids have been bullied online...

70% of students report seeing frequent bullying online...

Over 80% of teens use a cell phone regularly, making it the most common medium for cyber bullying...

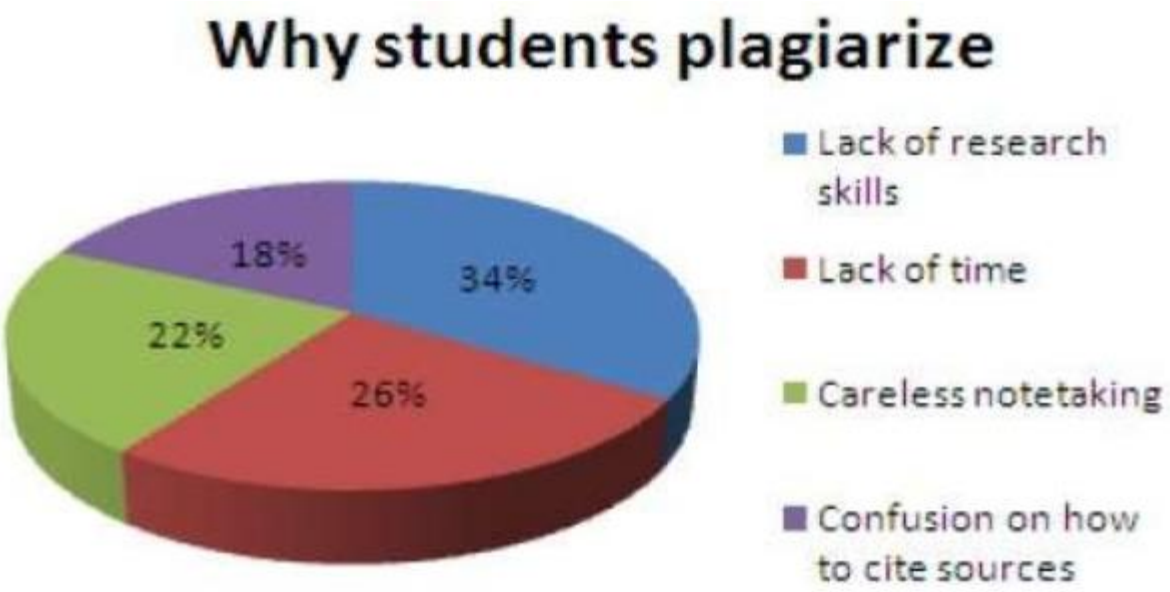
YOU ARE LEAVING UR DIGITAL FOOTPRINTS

A digital footprint is a trail of data you create while using the Internet. In includes the websites you visit, emails you send, and information you submit to online services. A "passive digital footprint" is a data trail you unintentionally leave online.

Monitor your Digital Footprints:

- Use Privacy Settings
- Keep a list of accounts then delete the ones you no longer use.
- Don't overshare, this includes usernames, aliases, passwords, last names, full-names-as-usernames, pictures, addresses, and other important information.
- Use A Password Keeper
- Google Yourself
- Monitor Linking Accounts: When you link your facebook or twitter account to that new site (whatever site that might be), you may not realize-or care at the moment-what you're giving it access to.
- Searches are Social: Google pulls the same trick with search and browsing habits. If a student is logged into their Google account, the service tracks every keyword they search, every Web page they visit and every time they visit Youtube.

SAY NO TO PLAGIARISM



Many people think of plagiarism as copying another's work or borrowing someone else's original ideas. But terms like "copying" and "borrowing" can disguise the seriousness of the offense:

According to the Merriam-Webster online dictionary, to "plagiarize" means:

- to steal and pass off (the ideas or words of another) as one's own
- to use (another's production) without crediting the source
- to commit literary theft
- to present as new and original an idea or product derived from an existing source

In other words, plagiarism is an act of fraud. It involves both stealing someone else's work and lying about it afterwards.

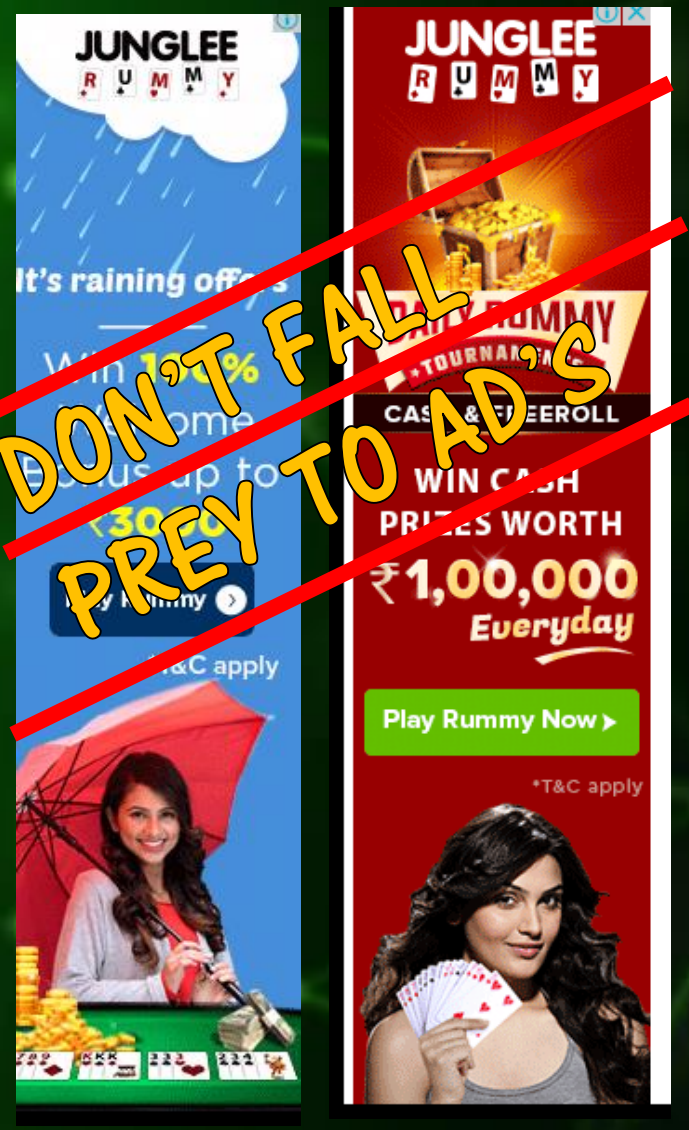
LET'S TOGETHER OUTSMART CYBER CRIMINALS

Protect Yourself with these STOP. THINK. CONNECT.™ Tips:

•**Keep security software current:** Having the latest security software, web browser and operating system is the best defense against viruses, malware and other online threats.

•**When in doubt, throw it out:** Links in email, tweets, posts and online advertising are often how cybercriminals try to steal your personal information. Even if you know the source, if something looks suspicious, delete it.

•**Protect all devices that connect to the internet:** Along with computers, smartphones, gaming systems and other web-enabled devices also need protection from viruses and malware.



•**Plug & scan:** USBs and other external devices can be infected by viruses and malware. Use your security software to scan them.

Think before you act: Be wary of communications that implores you to act immediately, offers something that sounds too good to be true or asks for personal information.

Make your password a sentence: A strong password is a sentence that is at least 12 characters long. Focus on positive sentences or phrases that you like to think about and are easy to remember (for example, "I love country music."). On many sites, you can even use spaces!

Unique account, unique password: Having separate passwords for every account helps to thwart cybercriminals. At a minimum, separate your work and personal accounts and make sure that your critical accounts have the strongest passwords.

Lock down your login: Fortify your online accounts by enabling the strongest authentication tools available, such as biometrics, security keys or a unique one-time code through an app on your mobile device. Your usernames and passwords are not enough to protect key accounts like email, banking and social media.

Protect your Money: Net banking and shopping, check to be sure the sites is security enabled. Look for web addresses with "https://," which means the site takes extra measures to help secure your information. "Http://" is not secure.

Back it up: Protect your valuable work, music, photos and other digital information by making an electronic copy and storing it safely.

IS NOT A GAME ... IT'S YOUR LIFE

STAY SAFE ONLINE !