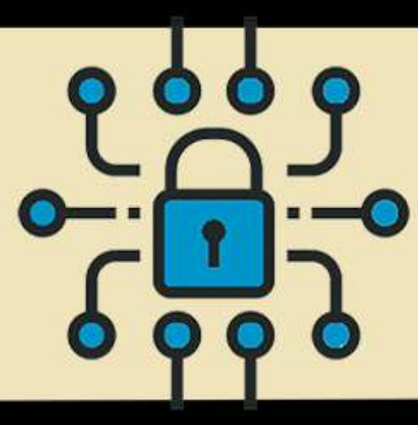
Student Press:

IT Kaleidoscope

jims
Sector-5, Rohini, Delhi

THEME: CYBER SECURITY



Cyber bullying- A Virtual Nuisance!

PROGRAM INCHARGE:
Dr. Praveen Arora

FACULTY INCHARGE:
Mrs. Priyanka Gandhi

CONTENT EDITOR:
Kirti Bhardwaj

CONTENT WRITERS:
Falguni Saini
Kirti Bhardwaj

DESIGNER:
Deepanshu Jain

"A safer online space is the need of the hour."

With more and more people joining the online community, the threat landscape on social platforms is also evolving, which proves that you don't need arsenal to cause widespread panic. One such threat is Cyberbullying!

Cyberbullying or cyber harassment is a form of bullying via electronic means, wherein the offender uses technology as a weapon to harass, threaten, embarrass or target another person in the digital space. The most worrisome trend is that it has become increasingly common among teenagers who prove to be easy prey on the World Wide Web.

Today, it has become a worldwide problem that has manifested itself into many forms.

There is 'frapping' that involves invoking fights on social platforms and using degrading language in doing so. Also, 'denigration' that involves sending or posting gossip or rumors about the target for defamation purposes, 'trickery' that involves making the victim reveal sensitive information with the intention of misusing it, 'exclusion' that involves deliberate segregation of the intended so as to affect the emotional well being of the victim or 'trolling' which involves posting insults or using bad language in order to provoke a particular person on online forums and social sites like Instagram, Facebook, Twitter, etc.

Some forms of Cyberbullying like Cyberstalking and Catfishing are more dangerous than the others since many reported cases saw the victims coming to physical harm as well.Cyber bullying is a heinous practice that may leave the bullied with various short and long term psychological disorders like depression, anxiety, panic attacks, etc as often the bullied victims fold into themselves, withdrawing from family members, relatives, and friends. The emotional stress, in many cases, also leads to physiological changes like weight loss and it may happen that over time, the person may develop self-harming tendencies.

In regard to this growing issue, the government has enforced the "Anti-Bullying Laws" to eliminate bullying in any form, from its roots. From schools and workplaces to virtual cyberspace, these laws protect not only teenagers who are most vulnerable to cyberbullies online but everyone who is active on the internet, henceforth making it extremely important for us to educate ourselves and those around us about the same.

Apart from the government, various steps can be taken on an individual level including having a strong and unique password for different accounts, keeping your personal information hidden, redefining security settings and privacy controls and eventually, educating yourself of the cause and effects of this problem and spreading awareness about it among peers.

So, it's about time that people living the digital life realize how to protect their own interests in this technological driven-era which is both a boon and a bane for us.

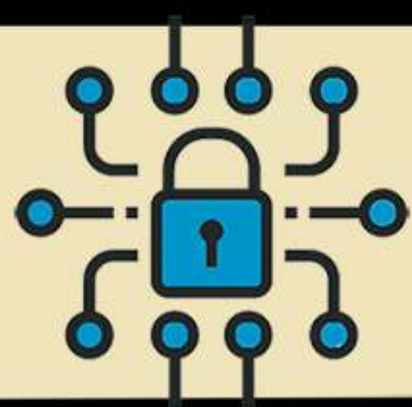
-Falguni saini
BCA I year I shift

Student Press:

IT Kaleidoscope

jims
Sector-5, Rohini, Delhi

THEME: CYBER SECURITY



FUN FACTS

- 92% of malware is delivered by email.
- It takes organizations an average of 191 days to identify data breaches.
- There is a hacker attack every 39 seconds.
- As of May 2016, 6 lakh Facebook accounts were compromised every day.
- China is the country with the highest number of malware-infected computers in the world.
- Android is the second most targeted platform by hackers after Windows.
- 90 % of hackers cover their tracks by using encryption.
- Bitcoin or cryptocurrency mining, a peer-to-peer computer process used to secure and verify Bitcoin transactions, is an area with big growth in cybercrime field.
- Elk Cloner is the first microcomputer virus with its creator being Richard Skrenta, who was only 15 years old at that time!

KIRTI BHARDWAJ
BCA II YEAR I SHIFT

THE DARK SIDE OF CRYPTOCURRENCY

"Is cryptocurrency the perfect gateway to crime ?"

In the past year, we saw the rise of digital money that promoted transparency in transactions.
But in contrary to what the layman thinks, the money kept in Paytm and Amazon wallets is not the only digital currency you can use. There is also cryptocurrency, a digital asset that is backed by cryptography to secure and verify transactions.
Examples of such digital currencies include the infamous Bitcoin, the explosion of which on the investing market has lead to a dozen other cryptocurrencies called Altcoins like Litecoin, Hypercash, Ripple etc and is also believed to give a substantial surge to blockchain technology, but, apart from serious investors, cybercriminals too are thrilled at the idea of untraceable money.
Even though digital currencies offer the ease of having no middleman between transactions, they are not without risks and this vulnerability is often taken advantage of by criminals using the dark web.
The dark web, that is only accessible through specialised browsers and promotes anonymous user activity, is one such space where cybercriminals sell and purchase all things illegal, from compromised credit card credentials to ammunition and all these transactions are made via cryptocurrency as it lacks a central governing body, making the storage wallets for the same difficult to trace.
Speaking of currency, the most profitable form of malware - ransomware that keeps your files and personal information hostage in exchange for money, is also thriving as in most cases of ransomware attacks the hackers demand the payment be made in cryptocurrency while also displaying pop-up messages with instructions to buy and use cryptocurrency on the compromised system's screen.
It is quite similar to attackers providing customer service, but with a twisted sense of humour.
Some cybercriminals, though, target the underlying mining process (crypto mining) involved in cryptocurrency exchange transactions, which when executed legally leads to high equipment costs and inflated electricity bills since it involves solving of complex puzzles to create new cryptocurrency that in turn consumes a massive amount of energy. However, to decrease these costs, criminals use 'crypto jacking' by deploying malware that compromises public websites and steals the processing power of visitors without compromising their personal information, unlike ransomware.
Moreover, a new application of crypto jacking has tried to make it more mainstream and legally justified, disguising it as a legitimate revenue stream.
Salon.com launched a "Suppress Ads" feature which enables site visitors to block ads by allowing Salon to use their unused computing power and giving them an ad-free experience if they crypto mine for Salon in return, making web traffic a means to profit.
Among the ever-present and the ever-evolving threats on the internet, the only way that guarantees a safe online haven is awareness.
Even if you never plan to invest in cryptocurrency, being conscious of its working can go a long way so that when an unlikely situation does arise you won't be blindsided.because, in the end, prevention is always better than the cure.

-KIRTI BHARDWAJ
BCA II YEAR I SHIFT