Callidus News

ADVOCATES,CONSULTANTS & NOTARY

DUBAI | SINGAPORE | DELHI | MUMBAI | KOLKATA | CHENNAI | COCHIN info@calliduscmc.com

Branches

Dubai
Business Avenue Building
Office # 713
Port Saeed Road, P.O. Box # 90992
Dubai, UAE, Tel : +97142956664
Fax : +97142956099

Singapore
20 Maxwell Road
#04-02 D, Maxwell House
Singapore - 069113
Tel: +65 6221 4090

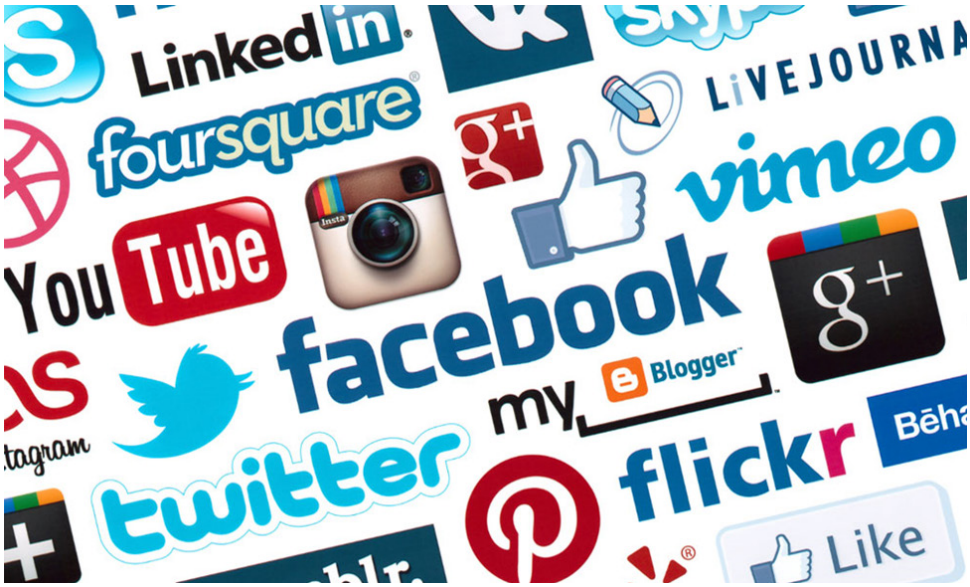
Delhi
D 1st 145 Basement (Rear)
Lajpat Nagar R 1
New Delhi - 110 024
Tel: +91 11 4132 1037

Mumbai
8-B, Dariya Building
2nd Floor, In between
American Dry Fruits & Zara
Dr. D.N.Road, Fort, Mumbai 400 001
Tel: 022-22853371

Chennai
Old No. 123, New No.255,
3rd Floor, Hussiana Manzil,
Ankapanaiken Street,
Parrys, Chennai - 600 001
Tel: +91 98 40 844463

Cochin
Near St.Joseph's High School
Chittoor Road, Cochin - 12,
India
Tel : +91 484 2391895
office@callidusindia.com

SOCIAL NETWORKING – AN INVASION OF YOUR PRIVACY



"When anything is free, your freedom is the price!!" Desmond Tutu once said, "When the Missionaries came to Africa, they had the Bible and we had the land. They said, "let us pray". We closed our eyes. When we opened them, we had the Bible and they had the land". Likewise, when social networking came, they had the WhatsApp and Facebook, and we had the freedom. They said it's free. We closed our eyes. When we opened them, we had WhatsApp and Facebook, and they had our freedom.

With the recent stir created by WhatsApp's new Terms and Conditions, individuals are becoming more aware on the risk in breach of their privacy. This is more of a concern for us in India due to our lack of robust Data Protection Laws. During WhatsApp's launch in 2009, it made a commitment to its users that it will not sell user data to any third party. This changed after Facebook's acquisition of WhatsApp in 2014; in 2017, there was data sharing with the parent company, however users were still given a choice not to opt for the same; with the recent update on the Terms and Conditions of Use, its basically a 'take it or leave it' option.

In effect if you agree to the new terms WhatsApp can share one's metadata, with Facebook and other apps, which encompasses anything other than the actual text conversation. This includes your private and personal activities online, devoid of any government or regulatory supervision, which is the scary bit. Now on the other hand if you are in Europe, WhatsApp would not even dare to make this move, on account of the Data Protection laws as well as agreements with Facebook, on the limit of WhatsApp data collection and use, in place.

All said and done, we have to come to terms with our reality, that online social networks (OSN's) like Facebook, LinkedIn, WhatsApp, Instagram, Twitter and the like, have turned out to be a fundamental part of our online lives. Users download OSN's to connect with family, friends, colleagues, associates or people with shared interests for professional networking, to promote their brand or business,

THOUGHT for the MONTH

You should bring something into the world that wasn't in the world before. It doesn't matter what that is. It doesn't matter if it's a table or a film or gardening - everyone should create. You should do something, then sit back and say, "I did that."

- RICKY GERVAIS

Callidus

job searches, entertainment etc.

The core purpose of this Article is to provide the reader with knowledge on the main categories of security and privacy attacks to OSN's and the counter measures and guidelines that can be deployed to protect ones privacy.

Most OSN's allow users to create their profile and user accounts and to post pictures, videos, blogs, to create links etc. It is the sheer amount of this personal information that is circulating on the web that provokes malicious users to gain access and obtain such personal information of genuine users for criminal purposes and fraudulent activities like spamming, virus attacks, phishing etc resulting in information and identity theft.

Some of the common attacks on OSN's are -

Social Engineering – Social engineering attacks mainly occur because individuals/users are not aware of the importance of keeping their private information safe, in such instance's attackers can manipulate users to part with confidential information with their scheming techniques. Reverse social engineering attacks on the other hand deceive the user into them and establish a degree of trust whereby the user parts with information which is then malicious used for phishing and spamming; for instance by luring the user to fake websites by impersonating reputed institutions like financial and educational institutions etc, influencing the user to part with private and valuable personal information. In August 2019, a massive phishing campaign targeted Instagram users, by posing as a two-factor authentication system, whereby users were prompted to log in to a false Instagram page.

Pretexting is another form wherein attackers get users to disclose confidential information, in order to carry out their ulterior motives using pretentious methods like lies which is known as pretext.

Though malware and related deceptive attacks can be minimised by the use of signature based anti-spam filers for emails enabling to block and reported the same; along with the use of anti-phishing tools bars like spoofstick to warn on phishing sites. Users should be vigilant to check if the webpage has deceptive links and if there is any suspicion then clicking or opening such URL's must be avoided. It is further the duty and liability of financial institutes to ensure that their customers are protected by taking appropriate measures to secure and authenticate their online websites periodically and to educate and warn their customers and users on fraudulent and illegitimate sites.

Spamming – The spammers device a method of sending out large amounts of emails to promote their products posing as trusted bankers or online payment service providers and thereby gain access to personal information of the users like username and password; this information is then used by the attacker to create friend requests to a targeted group of individuals or users and wait for them to accept the request and make them victims, then the 3 clique attack method is used to find the vulnerable members of the group to carry out further spamming and phishing attacks.

We can protect ourselves by using keyword spam filtering thereby identifying if the message is spam.

Identity Theft – Here the identity of the user is stolen and used to impersonate the user to the victim, to obtain some information or benefit from the victim or to harm them. Some of the ways in which this is carried out are through phishing, accepting friends request from unknown persons, sharing sensitive and personal information with strangers, accessing external links that lead to third party websites, free application downloads, no strict privacy settings etc.

Malware – This is a type of software designed to cause damage to your computer system by taking control of the operating system to obtain sensitive and privileged information. For instance, the Koobface malware was URL based which tricked Facebook users to instal the malware to steal log-in and other personal information of the user and send spam messages to their Facebook contacts.

Clickjack attacks – In this type of bout, the user is usually deceived into clicking a link that is not the official link but by overplaying multiple frames the user is taken to the desired page from where the malicious activity is launched. Cursorjacking and likejacking are carried out on similar lines wherein either the cursor automatically moves to a malicious link on the page while like jacking takes you to pretentious survey links and obtains your information.

Data Mining – it is a method of using research to segregate valuable and useful data from voluminous and cluttered data; attackers mine this data to obtain users private and personal data, an inference attack is an example of data mining here the personal data is accessed through authorised channels and then a breach is performed.

Botnet Attacks – Social media bots are automatic accounts which create posts or follow individuals, whenever a certain catch phrase or term occurs. A large group of bots can form a network known as a botnet. Bots and botnets on social media are used to steal data, send spam, and launch distributed denial-of-service (DDoS) etc.

Sybil attacks – The invader creates multiple profiles of the victim and dues the victim's friends into sharing their personal information which is then used by the attacker to steal the personal information of the victim's friend. This is also

known as identity clone attack.

We can be cautious, by only communicating with members or users who are trusted and authenticated or certified. Identify and avoid accepting requests from members with fewer connections.

Cross-site scripting – Here the attackers infuses malicious codes into the webpage and provokes the user to run the codes thereby stealing personal data and information. The operator makes use of XSS scripting to create XSS worms / viruses via HTTP using AJAX technology. An example of this XSS attack was Mikeyy, which was used to deploy almost 10,000 tweets exposing the susceptibility of Twitter users.

Cyberbullying – This is matter that is posted anonymously which in not easily traceable to the attacker, who sends out offensive material with intent to harm the targeted victim, this is mainly carried out on teens/youth.

Internet fraud – Threats here come in the form of non-delivery of online orders, identity theft, credit card fraud etc. The Rogue Antivirus was used as a download program to allegedly remove malware but instead installed malware on the system infecting it and then got the victim to pay for removal of malware or offers to solve performance issues.

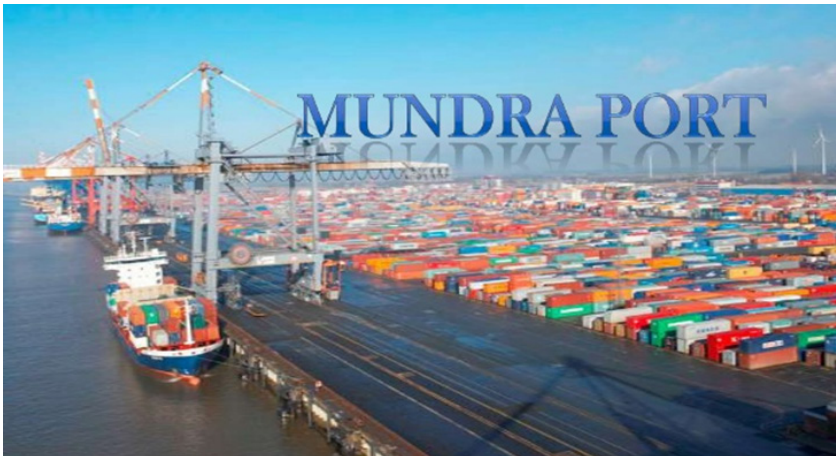
Some of the other guideline and ground rules that one can establish while using OSN's are –

1. Read and understand the Terms and Conditions for use of any app
2. Change the privacy setting to suit your needs.
3. Do not share any personal information, bank account details, login or passwords with persons or apps you don't trust.
4. Limit the extent of personal information that is shared online.
5. Refrain from friending unknown persons.
6. Have internet security installed and delete all third-party apps that gather personal information.
7. Turn off location setting.
8. Report all instances of cyber-attack to the nearest cybercrime authority, initiate investigation; protect others vulnerable users from such attacks.

The 3 main issues to be looked into while using OSN's are their privacy policy, integrity of the service provider in ensuring that the communications exchanged by its members is kept confidential and the app itself is secure from internal and external breaches and the availability or access to private data and information is permission based, with measures in place to ensure that those in possession of such data, do not misuse or abuse the same.

In the end, the rampant increase of technology usage, has its consequences on our privacy; companies rely on our information to conduct their daily business, to improvise and expand operations; hence social media and networking platforms will find ways to obtain and use our information with or without our knowledge and consent; it is upto us to know where to draw the line else our freedom and privacy will be at stake.

MUNDRA PORT BAGS A BIG SHARE IN SHIPPING OPERATION



Port located at the Gulf of Kutch, known to be Mundra port becomes a major player in shipping operation bagging 52 percent of operation for the month of December 2020 compared to JNPT Port which constituted to only 10 to 11 percent. The largest private port in India had handled 586,952 TEU compared to 459,920 TEU at JNPT port as per the latest port figures, the same comes as a both shock as well as a welcome one since the entire shipping operations were under standstill last year because of the covid 19 pandemic.

As per the latest Data India's total container operation was around 1.72 Million TEU for the month of December 2020 which was sightly higher after the covid 19 pandemic, out of 1.72 Million TEU Adani port's contribution alone was having staggering figure of 45% which is quite high for a private port operations in India. The Mundra Port also saw an increase in Transhipment due to heavy congestion in colombo, this also made Mundra Port as an Transhipment port for colombo due to heavy congestion in Colombo. It also understood that

the port offers various offers with respect to freight, draft and inland pricing. The said port is the nearest port for the North and Northwest India grabbing a major work operations from Majority population of India.

What makes Mundra Port so Special ?

The Natural Gateway to Cargo and Logistics operations, grabbing the attention of North and North west Traders in India who form Majority of Population in India. The port is also the first of its type as it is port based Special Economic zone Attracting larger traders compared to other ports. Though the said port was conceptualised only in 1998, within a span of 10 years it had already attracted 35% of the Compound annual growth rate across India. The opening of the Mundra port made the logistics and shipping easy for the entire north and north west India.

Though this pandemic had redefined the entire shipping and logistics operations, the same didn't affect Mundra Port anyway, on the contrary the Mundra port gained its significance relatively high on this pandemic over shadowing JNPT, Mumbai.

HOT TIPS

20 TIPS TO BECOME A SUCCESSFUL ENTREPNEUR

1. Understand the industry completely before you foray.
2. Set your goals and vision.
3. Challenge and Believe in Yourself.
4. Make a great plan to raise capital for your company.
5. Position yourself as a leader.
6. Communicate confidently with strategies.
7. Mange your energy and not your time.
8. Build a good and strong team.
9. Don't be afraid to take risks.
10. Deliver value and not just quick profit.
11. Seek new ideas especially beyond your industry.
12. Build long-term relationships.
13. Inspire your team and carry them along through your success.
14. Know what your clients really want.
15. Accept your mistakes and learn from it.
16. Research your competition and know them fully well.
17. Customer Feedback is important.
18. Never stop networking as that's the key for more business.
19. Look for results, not reasons.
20. Innovate, innovate and always innovate!

Address: Near St.Joseph's High School, Chittoor Road, Cochin- 12, India, T:+91 484 2391895, office@callidusindia.com