International Journal of Circuit, Computing and Networking 2024; 5(2): 56-59

International Journal of Circuit, Computing and Networking

E-ISSN: 2707-5931
P-ISSN: 2707-5923
www.computersciencejournals.com/ijccn
IJCCN 2024; 5(2): 56-59
Received: 22-11-2024
Accepted: 24-12-2024

Devendra Sood
Department of Computer Applications, Tula's Institute, Dehradun, Uttarakhand, India

Corresponding Author:
Devendra Sood
Department of Computer Applications, Tula's Institute, Dehradun, Uttarakhand, India

Significance of social media appreciation in cyber crime

Devendra Sood

DOI: https://www.doi.org/10.33545/27075923.2024.v5.i2a.91

Abstract
More than 60 percent of World population will use Internet and among these users' 90 percent users will have their detailed profiles in any one of the social media, 321 million new users came in last 6 months. Social media are interactive computer-mediated technologies that facilitate the creation and sharing of information and expression via virtual networks. Cyber-crime is computer-oriented crime which involves computer and network. In this paper I am focusing about how crime rate will expand by social media in other words how social media users will become victims of cyber-crime and measures to be taken by the users along with avoidance of crime.

Aim

- To recognize about the temperament of social media in Cyber Crime
- Steps to be taken to evade crime rate by social media

Keywords: Social media, cyber-crime, security, algorithm, population, networks, computer-oriented

Introduction

Now a day the internet is a needed part for everyone. The Internet contains everything we need to lead life, so, people are using and depending on it more and more. As internet usage is increasing day by day, it makes the world small; people are coming closer. Speedy technological growth and developments have provided vast areas of new opportunity and efficient sources for organizations. It has become now a national asset; the whole national security is also depending on it. But these new technologies have also brought unparalleled threats with them. Today our lives are public through social media, while many are colourful and satisfactory with sharing, everything about their profiles with whom they connect with, most of the cyber-crimes are either done by fraudsters or by someone you know in the close circle. It could be your friend, relative, employee, colleague, or ex-boyfriend/girlfriend. It is essential to have your privacy settings have to be set in such a way that individuals you are not connected should not see a lot about your personal information. Secondly, everything doesn‘t necessarily has to go on social media. Now a day ‘s social media sites were used mostly such that they seem to be out of control of enterprise security teams, they provide a perfect gateway into your networks through social engineering, malware and phishing attempts. As company operations continue to undergo a digital transformation, new risks related to social media usage by your employees and customers emerge. In fact, 15% of large organizations had experienced a break relating to social media sites in 2019, and this number is likely to grow going forward.

- Social media are interactive web 2.0 Internet-based applications.
- Text, photos, videos, and data generated through all online interactions, is the lifeblood of social media.
- Users create service-specific profiles for the website or app that are designed and maintained by the social media organization.
- Social media facilitate the development of online social networks by connecting a user's profile with those of other individuals or groups.

Now will see how social media usage will be in one minute

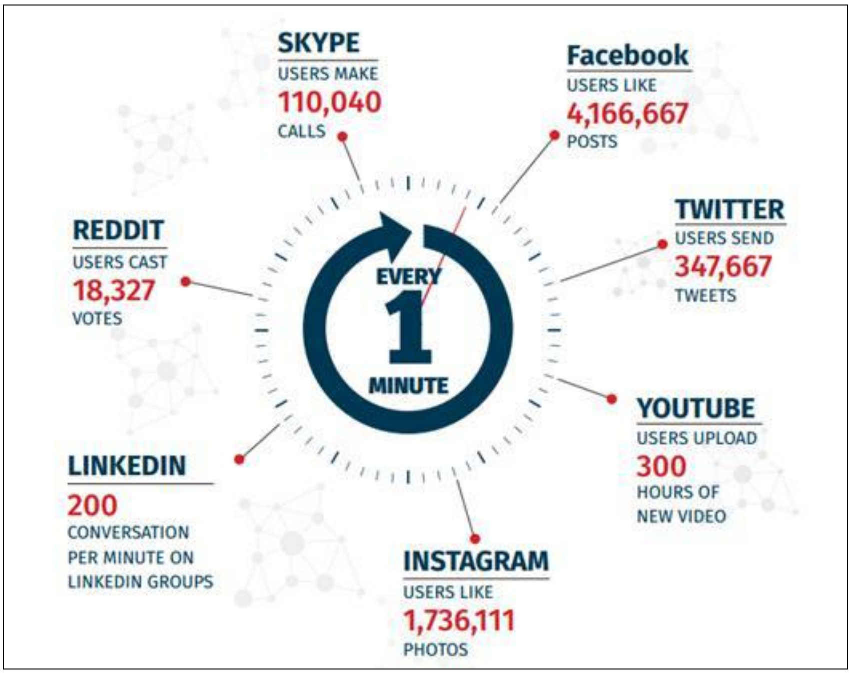

Fig 1: Social Media Usage

Network Name	Number of Users	Network Name	Number of Users
Facebook	2.32 billion	WeChat	1.04 billion
YouTube	1.9 billion	Instagram	1.0 billion
WhatsApp	1.5 billion	QQ	0.80 billion

Mobile social media are a useful application of mobile marketing because the creation, exchange, and circulation of user-generated content can assist companies with marketing research, communication, and relationship development. Mobile social media differ from others because they incorporate the current location of the user (location-sensitivity) or the time delay between sending and receiving messages (time-sensitivity). Most of the social media users will update their profile which is consisting of their information which gives easy access to cyber criminals via e mail or mobile phones. Social media is increasingly being exploited to contact, recruit and sell children for sex, the study, which was requested by the Ohio Attorney General's Human Trafficking Commission, reveals how traffickers quickly target and connect with vulnerable children on the Internet through social media.

We could list the following reasons for the vulnerability of computers

Easy to access

The problem behind safeguarding a computer system from unauthorized access is that there are many possibilities of breach due to the complex technology. Hackers can steal access codes, retina images, advanced voice recorders etc. that can fool biometric systems easily and bypass firewalls can be utilized to get past many security systems.

Capacity to store data in comparatively small space

The computer has the unique characteristic of storing data in a very small space. This makes it a lot easier for the people to steal data from any other storage and use it for own profit.

Complex

The computers run on operating systems and these operating systems are programmed of millions of codes. The human mind is imperfect, so they can do mistakes at any stage. The cybercriminals take advantage of these gaps.

Negligence

Negligence is one of the characteristics of human conduct. So, there may be a possibility that protecting the computer system we may make any negligence which provides a cyber-criminal the access and control over the computer system.

Loss of evidence

The data related to the crime can be easily destroyed. So, Loss of evidence has become a very common & obvious problem which paralyzes the system behind the investigation of cyber-crime.

Types of Crimes

Reconnaissance

Criminals will create a fake social media profile by reading continuously the posts and updated information by the user to impersonating someone from your organization or a known public figure to distribute malicious links. The information gathered from social media can also be used by cyber criminals to craft phishing emails that look more authentic and thus more likely for included links to be clicked or attachments downloaded, both of which can install malware on the endpoints used by your employees.

Brand Hijacking

Digital brand hijacking can make or break your business. In the age of digitalization, intangible assets such as the brand name and your brand‘s reputation comprise as much as 88% percent of enterprise market value. Cybercriminals can easily hijack your online brand by creating fake company pages and online communities, abusing your brand and its reputation for personal gain

Weaponization of social media profiles

Complete and convincing fake accounts are created and then linked to many other phony profiles in order to boost their credibility. Often, these accounts adopt the personality of talent recruiter (head-hunter), to attract users to connect with them.

Malicious bots

Social media bots are often used to mass distribute malicious content. Bots can generate fake likes, re tweets and views to fake user profiles to boost credibility and reach. Tens of millions of malicious bots infest social media platforms, many of them used deceptively for political purposes or malicious gain.

Distributed denial of service (DDoS)

Attacks against company pages. Attackers can launch a DDoS-like attacks against a brand‗s official Facebook page, for example, and flood it with bot-generated comments, which are too numerous for the brand to respond to, and come in faster than the company can delete. This makes the site useless for the intended customer engagement or brand promotion.

Social engineering

As we explained above, attackers can gather information from public-facing social media accounts which can then be used to construct convincing phishing emails and BEC attacks. With BEC attacks totalling over $5 billion in damages worldwide, enterprises should pay close attention to the role of social media in planning and executing sophisticated social engineering attacks. The emergence of a complex and multi-layered cybercrime economy has also begun to suggest a fundamental shift in the very nature of crime itself. In this context, overt acts of crime become less central features of the criminal ecosystem when compared to the services and platforms that feed off and support crime – which become increasingly low-investment, high-yield and low-risk operations.

Major Problems We Can See in Social Media Addicts Are

- **Disparity:** A lack of equality in society
- **Polarization:** The act of dividing something, especially something that contains different people or opinions, into two completely separate groups
- **Stereotyping:** a stereotype is an over-generalized belief about a particular category of people
- Recent research has demonstrated that social media and media in general, have the power to increase the scope of stereotypes not only in children but people all ages

Cognition and Memory

According to writer Christine Rosen in "Virtual Friendship, and the New Narcissism," many social media sites encourage status-seeking. According to Rosen, the practice and definition of "friendship" changes in virtuality. Friendship "in these virtual spaces is thoroughly different from real-world friendship

Physical and Mental Health

There are several negative effects to social media which receive criticism, for example regarding privacy issues, information overload and Internet fraud. Social media can also have negative social effects on users. Angry or emotional conversations can lead to real-world interactions outside of the Internet, which can get users into dangerous situations. Some users have experienced threats of violence online and have feared these threats manifesting themselves offline. At the same time, concerns have been raised about possible links between heavy social media use and depression, and even the issues of cyber bullying, online harassment and "trolling". According to cyber bullying statistics from the i-Safe Foundation, over half of adolescents and teens have been bullied online, and about the same number have engaged in cyber bullying. Both the bully and the victim are negatively affected, and the intensity, duration, and frequency of bullying are the three aspects that increase the negative effects on both of them. Studies also show that social media have negative effects on peoples' self-esteem and self-worth.

Adolescents

Excessive use of digital technology, like social media, by adolescents can cause disruptions in their physical and mental health, in sleeping patterns, their weight and levels of exercise and notably in their academic performance

How We Should Be in Social Media to Reduce Crime Rates

Cyber criminals rely on our laziness and depend on our bad habits to make us vulnerable. Replacing bad habits with good habits isn‗t difficult; it's just a matter of re-training yourself. Here are a few thoughts to adopt that can help you protect against cybercrime:

Use secured wireless System

Stay on the cellular network whenever possible. If you must use Wi-Fi, make sure it requires a password and check on the security. (WPA-2 is ideal.) Avoid public networks (airports, coffee shops, restaurants) that create many attack avenues.

Be Closed

Use encryption on your laptop to protect data in the event of theft or loss. The Ponemon Institute estimates that every week, 12,000 laptops are lost or stolen in U.S. airports alone! Use an encrypted virtual private network (VPN) to remotely access your office network. Only log into websites that are encrypted. (Look for the ―s‖ in https ://.)

Use your own

Now internet is cheaper than mineral water, so use your own devices and hotspot for internet works, don‗t depends on public for anything confidential (checking email, ordering online, accessing client documents, logging into extranet portals, etc.). Bring your own laptop and Internet hot spot. Be in control of your own security.

Awareness while clicking

We should be care enough before clicking a photo and share it, selfie photo with back ground details we can search location, some time we will click selfie in front of company, which gives criminals an information about the location and about company too, the dangers of travel don‘t need to include the many new ways we are accessible due to technology. Be aware of potential dangers, and put your natural scepticism and good habits to work whether at home or on the road. Don‘t let those malicious magicians play a trick on you! "It is vitally important to educate parents, professionals and youth— especially our middle school or teenage daughters who may be insecure—about the dangers of online predatory practices used by master manipulators," said Dr. Celia Williamson, UT professor of social work and director of the UT Human Trafficking and Social Justice Institute. "Through this outreach and education, we can help save children from becoming victims of modern-day slavery."

Artificial Intelligence

A cyber security skills shortage is one reason why many are pinning their hopes on AI to help manage risk in concert with human intelligence. For example, MIT ‘s Computer Science and Artificial Intelligence Lab has developed an ―adaptive cyber security platform‖ called AI2 that adapts and improves performance over time by combining machine learning tools with human security analysts. AI2 sifts through tens of millions of log lines each day, flagging anything deemed suspicious. Analysts confirm or adjust the results and tag legitimate threats. Over time, AI2‘s algorithms fine tune their monitoring, learn from mistakes, and get better at detecting breaches and reducing false positives. In early trials at MIT, AI2 has correctly predicted 85% of cyber-attacks.

Algorithms used

Triple DES

Triple DES was designed to replace the original Data Encryption Standard (DES) algorithm, which hackers eventually learned to defeat with relative ease. At one time, Triple DES was the recommended standard and the most widely used symmetric algorithm in the industry.

RSA

RSA is a public-key encryption algorithm and the standard for encrypting data sent over the internet. It also happens to be one of the methods used in our PGP and GPG programs. Unlike Triple DES, RSA is considered an asymmetric algorithm due to its use of a pair of keys. You ‘ve got your public key, which is what we use to encrypt our message, and a private key to decrypt it. The result of RSA encryption is a huge batch of mumbo jumbo that takes attackers quite a bit of time and processing power to break. Expert observers are hopeful that a new method called Honey Encryption will deter hackers by serving up fake data for every incorrect guess of the key code. This unique approach not only slows attackers down, but potentially buries the correct key in a haystack of false hopes. Then there are emerging methods like quantum key distribution, which shares keys embedded in photons over fibre optic, that might have viability now and many years into the future as well.

Conclusion

In this paper I mentioned different types of crimes and property of Crimes which can be happen with excess and unsecured use of social media, to protect our self and society from cyber criminals we have to adopt some superior qualities which is explained above. Implementation of new algorithms will also reduce percentage of crime, more over we should not get addicted to social media through which we are exposing our self completely to the world which will give the direction to criminals to attack very easily, we should educate parents regarding usage of social media by their child and we our self should determine which information should be there on social media and which should not be.

References

1. Kietzmann JH, Hermkens K. Social media? Get serious! Understanding the functional building blocks of social media. Bus Horiz. 2011;54(3):241–251. DOI: 10.1016/j.bushor.2011.01.005.
2. Obar JA, Wildman S. Social media definition and the governance challenge: An introduction to the special issue. Telecommun Policy. 2015;39(9):745–750. DOI: 10.1016/j.telpol.2015.07.014.
3. Liddell HG, Scott R, Jones HS, McKenzie R, editors. A Greek-English Lexicon. Oxford: Oxford University Press; 1984.
4. Rivest RL. Cryptography. In: Van Leeuwen J, editor. Handbook of Theoretical Computer Science. Vol. 1. Amsterdam: Elsevier; 1990. p.
5. Bellare M, Rogaway P. Introduction. In: Introduction to Modern Cryptography. 2005 Sep 21. p.10.
6. Cyber-crime. http://krazytech.com/technical-papers/cyber-crime.
7. Pahuja R. Impact of social networking on cybercrimes: a study.