JOURNAL PUNJAB ACADEMY OF SCIENCES (Peer Reviewed Open Access Journal)
JPAS, 21: 24-27 (January-December, 2021)
Available online at www.jpas.in
ISSN 2229-7014 (P)

SOCIAL NETWORKING THREATS AND THEIR PREVENTIONS: A REVIEW

Ashwani Kumar
Department of computer Science & IT,
Baring Union Christian College, Batala, Punjab, India.
E-mail: ashwani_apjim@yahoo.co.in

ABSTRACT

Social networking is the need of the hour. It has become the necessary part of every one's life. There are so many benefits of social networking like social gathering, online advertisement, real time idea and matter sharing etc. but also have so many draw backs of using social networking major one is security and privacy. In spite of many disadvantages there is nothing bad to using these tools as these are the best method to interact with millions of online users including yours friends and family, even you can find out your old friends and any person that you want to search. But the concern is the security and privacy of your information. This paper contains social networking threats and their preventions.

Keywords: Social networking, Threats, Security, Information.

INTRODUCTION

Social networking now a day's become a popular tool among the people. People of any age; teenager, young or old age, all are using some kind of social networking tool. In this era of 4G technology 50% of time is consumed on social networking by the user of mobiles especially students. Most commonly used social networking tools are Facebook, WhatsApp, Twitter, Google+, Hike, Instagram and YouTube. Most of the users in India are using Android phones and all these social networking organizations have given application of these social networking based upon Android and IOS or iPhone etc so that user can easily access these networking site through there apps. People are using these very applications, even most of them have made a habit of using this tools like Facebook and WhatsApp etc. Some people became addicted to these. There is nothing bad to using these tools even these are the best method to interact with millions of online users including yours friends and family, even you can find out your old friends and any person that you want to search. But the concern is the security and privacy of your information. This paper contains security threats and their resolution.

1. **Top security threats in using social networking tools:**

Stolen of your identity: Most of the time users enter their exact identity on social networking site or application that can be easily accessible by anyone just from your public profile. e.g if anyone has tagged his or her mother on his birthday, it is easy to know your mother's median name and this is the most commonly filled security question.

1.1 Access to your social profile: Hackers generally inject virus and small program through some links, while clicking on these links your computers or your social

profile can easily be hacked and that can be further misused.

1.2 Steal your location information: Most of these applications access your location from your devices using GPS (Global positioning system). From these locations any one can easily trap you any time.

1.3 Stealing of your schedule: Most of the people share their schedule like traveling from this to that place, eating pizza at this location etc. From these types of posts or events any one can easily find your location and plan. This type of information can be used to harm the user.

1.4 Becoming the overconfident. Some time due to his or her overconfidence he or she has to pay. Most of the users of above said networking tools they are not aware of the technicalities behind these application or sites and they are posting with overconfidence that nothing is important in my device, but your device is associated with others.

1.5 Getting your contacts: Stealing your contacts is the most common hacking on social networking. After stealing your contacts they generally sell to marketing companies that is the reason users are getting bulk mails and phones.

1.6 Accessing your private photographs: Most of the social networking tools are popular among users due the sharing of photographs and videos. Generally all the users are posting their snaps on these sites that can be further misused.

1.7 Accessing all your online activities: any one can easily trap your activities like when you are using a particular application or your device.

1.8 Access to your private messages: Most of the applications required OTP (One time password) to complete your registration process and for that you have to give the access to particular application to access your contacts and messages. It means further these applications can read your private messages like PIN(Personal Identification Numbers) and OPTs. Misuse of these OTPs and PINs can harm the user financially.

1.9 Social Networking used for spreading spam and malware: Most of the Cyber criminals generally mask their links with a short URL, for the user it is very difficult to identify whether the link is legitimate or malicious site further are used to spread links and news in a very short span of time.

1.10 To make the financial loss to you: These tools are used for accessing your banking transactions, debit or credit card details these details are then further use for cloning of your cards etc.

1.11 Blackmailing: From these tools hackers access your family details and then using personal photographs or details that can be used to blackmail the user.

1.12 Profit from the empathy: Fraud people can get the empathy from user by posting some fake photographs of patients from different medical histories and collect money.

1.13 OTP(One time Password) scam is very popular on social media.

1.14 QR Code Scam is the newest scam these days

2. Measures to Prevention of threats of social networking:

2.1 Post as minimum as possible on social networking public profile.

2.2 Set a strong password to maximum length i.e combination of small, capital, numeric and some special symbols.

2.3 Carefully post your status as in this paper the example of mothers birthday has already been taken to explain the threat.

2.4 Never click on the small URLs or short hand links visible on website or application.

2.5 Always hover over the link that you want to open.

2.6 There are different link scanners are available online you can use to check the legitimacy of link.

2.7 Nothing is private after posting on social networking so be careful while posting and think many times before posting. Sometimes user has to pay for their overconfidence.

2.8 Most of the applications or sites keep the track of your activities. You can enable the link don't tack my activities.

2.9 Always check the privacy conditions of particular app before using or installing the same.

2.10 Always visit the privacy setting and set the different option according to your need. Try to keep the maximum privacy.

2.11 Never share or post your Travel plans, Bank account information, your daily schedule, your full address and birthdays.

2.12 Never fill your spouse and children's names, school, and birthdates, Location information, such as the name of your work place while registering the particular website or application.

2.13 Make your phone number and email hidden. You can turn on the option that any one request your phone and email and get it after your approval.

2.14 Restrict the users to access your profile by making the appropriate setting in privacy and security setting of particular application or website.

2.15 Restrict the visibility of your personal posts.

2.16 Never blindly trust on any posts that demand money on medical ground.

2.17 Never think empathically, always verify the facts before reacting on these social media tools.

2.18 Never scan QR code shared by strangers on social media this may lead to financial or informational loss.

2.19 Never share OTP or code received on your phone number to anyone.

2.20 Always log out when you are not using the media sites to make sure that other people won't use your social media profile and account.

2.21 At last the most important point is understand security settings for each social media and seek consultation. This will assure that privacy and settings are in place.

CONCLUSION

Social networking is a tool that can both help and harm. Whether it is used for business, school, research, or for relationship building, social networking offer many new and exciting opportunities. However due to unsuspecting users there is always potential danger if we do not take the above preventions.

Although popularity of social media has brought many benefits to society, it has also resulted in privacy and security threats. After assessing the security and vulnerability of different social media sites the findings indicate that most sites posted privacy and security policies but only a minority stated clearly their execution of the key security measures. The network information that was publicly available through Internet search, which was vulnerable to cyber intrusion.

So it is advised to all the social media user to use these tools with greater care.

REFERENCES

http://www.adweek.com/digital/

http://www.debate.org/opinions/are-social-networking-sites-generally-beneficial-to-our-way-of-life

Cisco, Social Media: Cultivate Collaboration and Innovation, white paper, Cisco Inc.,

M. Ahlgren,. (2020, January 4). 40+ Twitter Statistics 2020: Must-Know User Demographics & Facts. Website Hosting Rating. https://www.websitehostingrating.com/twitterstatistics/

Zebari, R. R., Zeebaree, S. R., & Jacksi, K. 2018. Impact Analysis of HTTP and SYN Flood DDoS Attacks on Apache 2 and IIS 10.0 Web Servers. 2018 International Conference on Advanced Science and Engineering (ICOASE), 156–161.

Oxley, A. 2011. A best practices guide for mitigating risk in the use of social media. IBM Center for the Business of Government Washington, DC.

Chaffey, D. (n.d.). Global social media research summary 2019 | Smart Insights. M. Retrieved February 1, 2020, from https://www.smartinsights.com/social media-marketing/social-media-strategy/new-global-social-media-research/