Open access Journal International Journal of Emerging Trends in Science and Technology

Hacking in Social Media and Some Guidelines to Avoid It

Author
Mamta Gupta
Shyam lal College, Computer Science Department, University of Delhi.
Email: *Mamta07_gupta07@yahoo.com*

Abstract
Hacking in social media means to get private information of user without his permission. In this work, an attempt has been made to show you that what mistakes are generally done by users. So that hacker takes advantages of that. Also we are showing you hacking signs, and some guidelines to avoid this hacking.
Keywords: *Data Breach, Hacking, Phishing, Authentication.*

1. INTRODUCTION

Social media sites allow you to create, to share information, to communicate. Because social media provide largest platform to do all these things. That's why people spend more time with social media sites than any other type of site. Due to that so many Internet users have been registering for new accounts on Face book, Twitter, whatsapp etc. opening just another window for online interaction with friends, relatives or strangers. people share their thoughts ,personal information with their friends or strangers without any caution. Due to significant increase in user accounts on social media there can be a incidents of hacking. This means that many social media accounts get hacked, and this is not a rare thing. So that to taking advantages of social media in safe mode internet user has to deal this negative thing.

2. MISTAKES DONE BY USER

Following are some mistakes that are done by internet user and by taking the advantages of these mistakes; hacker get easily what he wants.

- Creating password without caution.
- Clicking on anything.
- Login from anywhere.
- Don't have antivirus software.
- Use same user id and password in multiple sites.

3. SIGN OF HACKING

Now let's know about the sign of hacking in social media.

- Ad flood on your site.
- You have problem during login.
- Messages posted on your behalf.
- Malicious content on your page.
- Suspicious mails.

4. SOME GUIDELINES

4.1 Password

To secure your account use strong password. Generally user create password using date of birth, their name, 1234567 like that .And also user use same password for all accounts like for emails, online bank account, social sites etc this is very harmful for internet user. So do not do that. Periodically change your password and use combination of lowercase and uppercase letters, numbers and symbols. When you hacked immediately reset your password. Do not share it with anyone.

4.2 Phishing

Many hackers use this technique. They ask sensitive information like card details, account no, pin no etc. And they requests for immediate action through emails. Instead respond to this, contact organization and alert them to the issue.

4.3 Two step verification

Most people only have one layer – their password to protect their account. With 2-Step Verification, if a bad guy hacks through your password layer, he'll still need your phone or Security Key to get into your account. It provides another security layer for your online accounts. For example yahoo and Google provide two step verification securities. To achieve this type of security user has to register their mobile no.

4.4 Antivirus software

Install antivirus on your device. And update antivirus software from time to time. Scan your devices periodically.

4.5 Do not click anywhere

Be careful when downloading software/free files/Programs from internet because malicious code like spyware and keystroke loggers (that secretly track what you are typing) can be downloaded on your system and they can steal your sensitive data so before clicking anywhere think about it. So that install only trusted software. If you have any doubt about a function of software, do not install it. If you receive e-mails from unknown peoples, resist your curiosity and do not open it, just delete it .Under no conditions download or open attachments from anyone that you do not know and even then be cautious. Banks and most companies that create online personal accounts will not send you attachments. If they are doing, it is the best to go to the company site or bank site and request the download or at least see if it is genuine. Whether in your e-mail or online, do not click on ads. If the ad is of interest, find the site.

4.6 Data breach by third party

Cyber criminals hack into e-commerce websites and social networks to extract the user database, including user id and password. Since users often reuse same user id and password, it is highly likely that the same id and password can be used for logging into other systems as well. Using this information, the attacker can access other sites and services. So do not use same user id and password in multiple accounts, specially using the same id and password for job-related accounts and personal accounts. Try to avoid using same id and password across multiple sites.

5. CONCLUSION

Although it's really difficult to achieve safe social media. But, if you follow these guidelines that we have provided. You will see that you can recover from a potential hacking of your social account .As you know that Prevention is better than cure. So follow these guidelines. Last but not least platform of social media is very help full provided when we know what to do or what not to do.

6. REFERENCES

1. "Preventing Phishing Attacks" https://www.centralbankofindia.co.in/site/mainsite.aspx?status=l1&menu_id=55
2. "Two step verification" http://en.wikipedia.org/wiki/Twostep_verification
3. "Two-step verification for extra account security" https://help.yahoo.com/kb/SLN5013.html
4. "Google 2-Step Verification" https://www.google.com/landing/2step/#tab=how-it-protects
5. "a Third-Party Data Breach Leads Hackers to Your Data" http://securityintelligence.com/how-a-third-party-data-breach-leads-hackers-to-your-data/#.VXAty8-qqkp
6. "Fraud prevention tip" http://www.cba.ca/tips/en/content/consumer/tips/October_EN09.html