Newsletter 2023 Issue II

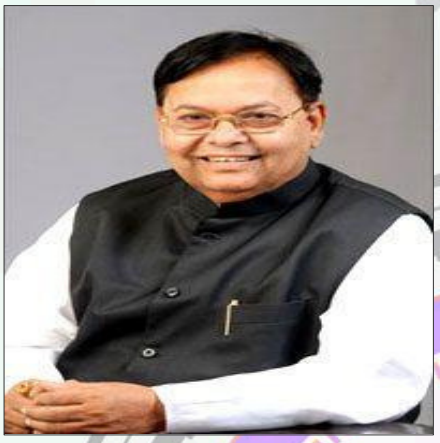
CYBER SECURITY

प्रभात

Exploring Tech Rising Star

Bharati Vidyapeeth's
Institute of Management and Information Technology
Navi Mumbai

BHARATI VIDYAPEETH'S
INSTITUTE OF MANAGEMENT AND INFORMATION TECHNOLOGY
NAVI MUMBAI



Dr. PATANGRAO KADAM

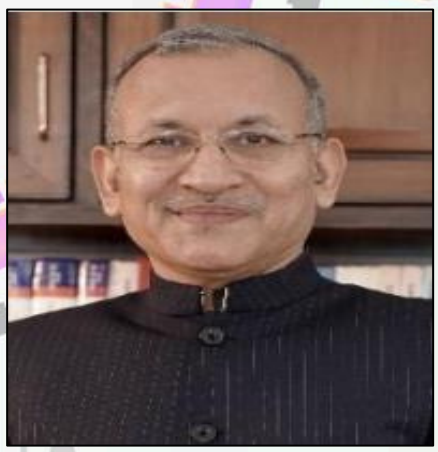
Founder
Bharati Vidyapeeth
(Deemed to be University), Pune

Prof. Dr. SHIVAJIRAO KADAM

Chancellor
Bharati Vidyapeeth
(Deemed to be University), Pune

Dr. VISHWAJEET KADAM

Pro-Vice Chancellor & Secretary
(Deemed to be University), Pune



Prof. Dr. VIVEK A. SAOJI

Vice-Chancellor
(Deemed to be University), Pune

ADVISORY BOARD

Dr.V.J.Kadam
Regional Director
Navi Mumbai Campus

Dr. Jyoti Kharade
Vice Principal

Dr. Suhasini Vijaykumar
Principal

CHIEF EDITOR

Dr. Pratibha M. Deshmukh

STUDENT EDITORS

Nupur Desai

Chanchal Dwivedi

Principal Desk

Dr. Suhasini Vijaykumar
Principal

BVIMIT fortifies student's intellectual awaking and social transformation in different spheres that makes them to contribute to the organization and world as well. We strengthen student's hard work and commitments towards knowledge.

BVIMIT provides MCA, VI semester course enables overall development of students and give a different perspective towards corporate life.

Current newsletter entitled "***PRABHAT-exploring tech rising star"*** is a combined effort of students and staff members that commences articles on emerging technologies with theme as **"Cyber Security"** provides articles for the same.

I hope "**PRABHAT"** will take you to the world of prominent technologies.

Editorial Desk

Dr. Pratibha Deshmukh
Editor-in-chief

It is indeed a great honor to be the Newsletter Editor for me and also an immense pleasure to launch the first edition of BVIMIT Newsletter "PRABHAT- exploring tech rising star".

As we are living in the technological era, we have selected the topic for the article as "**Cyber Security**" to make students aware about this emerging technology. It aims to be a truly interdisciplinary platform seeking to bring together a range of diverse voices on the topic in order to stimulate discussion.

A huge thank you to all the students who contributed writing the articles, without which there wouldn't have been this newsletter.
I appreciate PRABHAT student members for their everlasting support throughout the creation of this edition.

I hope "**PRABHAT**" will convey some technical knowledge to you.

Chanchal Dwivedi
MCA student

SOCIAL MEDIA AND CYBER SECURITY

Social media, in today's digital society, is an increasingly important tool for both personal and professional engagement in communication. This same pervasiveness brings huge challenges to cybersecurity. To protect your personal information and ensure safety over the airways, there are various security measures that should be implemented. The paper gives an in depth discussion of ways to enhance your social media security by deriving lessons from some recent research into emerging threats.

1. Strengthen Your Passwords

Social media security 101 starts with strong passwords. Your password must be a mix of uppercase and lowercase letters, numbers, and special characters. None of the common words or easy to guess sequences like "123456" have to be included, just as personal information such as birthdays. In case you would like to remember several, you should use a password manager. As a rule, these applications create unique passwords for each of your accounts and manage them so that you wouldn't have to burden yourself with them while keeping good security.

Why It Matters: Weak passwords are one of the biggest vulnerabilities. Very often, these cybercriminals make use of brute force attacks or stuffing techniques to gain unauthorized access. Unique and strong passwords on every platform drastically reduce the risk that if one gets compromised, it won't lead to a multitude of breaches.

Why It Matters: Weak passwords are one of the biggest vulnerabilities. Very often, these cybercriminals make use of brute force attacks or stuffing techniques to gain unauthorized access. Unique and strong passwords on every platform drastically reduce the risk that if one gets compromised, it won't lead to a multitude of breaches.

2. Enable Two Factor Authentication (2FA)

2FA does not rely only on your password. It allows only with another kind of verification; this could be done through a code that will be sent to your mobile device or generated by an authentication app. This second factor gives much stronger protection because it becomes much harder for an attacker to break into your account, even with your password.

Why It Matters: It prevents a huge number of attacks, especially those that pertain to phishing and credential theft. 2FA makes unauthorized access a lot more difficult in the case of such requirements being present for two forms of identification.

3. Review and Manage Privacy Settings

Most social media sites have privacy setting options for their users to decide better on who can view their posts, personal information, and contact details. Check it often to ensure it is at your present comfort level of privacy. Setting private profiles wherever possible limits the number of people who have access to your information and thus protects you from unwanted exposure.

Why It Matters: Excessive exposure of personal information might lead to identity theft, phishing attacks, or other forms of cybercrime. These privacy settings will help a user to be more in control about who has access to their data and so be better positioned to avoid risks.

4. Beware of Links and Messages

These sometimes also take the forms of phishing attacks and malware distribution. Avoid clicking links or opening attachments from unknown sources, unsolicited messages, those asking for personal information, or prompting immediate action. Check first if the source is credible before engaging with such suspicious content.

Why It Matters: Phishing schemes are some targeted scams that these cybercriminals use to make users reveal sensitive information or download malware. Be extra careful while evaluating the links and messages so that you don't end up being a potential victim of the scheme.

5. Keep Tab on Your Accounts Regularly

Regular monitoring of your accounts can help you notice any kind of unusual activity or unauthorized access. Look out for any strange locations from which your account has been accessed, changes within the settings that you never did, or posts you never made. To any suspicious activity, reach out to the platform support team right away and take as many actions as you need to secure an account.

Why It Matters: Very often, it is early detection that may just help prevent further damage. With regular monitoring, you'll detect any possible breaches or attempts at account compromise earlier so you can act really fast in mitigating risks.

6. Keep Yourself Informed and Inform Others

Keeping yourself updated on threats and various practices concerning cybersecurity is a necessary measure for an assurance of security. Attend cyber security training, know new features and updates from all your social media platforms, and spread the word whenever you grab something. It contributes to a safe space whenever you can educate someone about the security of social media.

Why It Matters: Cyber threats keep evolving very quickly. The more knowledgeable you are about cyber security, the more you can let yourself and your network be one step ahead in risks and measures of protection, enhancing general security.

7. Manage Third Party Apps Wisely

its image as an innovative and forward-thinking brand,
further enhancing its appeal to tech-savvy consumers.

It's also worth mentioning that most social networking sites enable third party applications. In most instances, this can be dangerous. Check the permissions granted to these apps and delete any of them that are no longer needed or you just don't trust. Make sure the apps you're using come from a reputable source and have good security practices in place.

Why It Matters: If third party applications can access your social media data, the insecure or untrustworthy ones may abuse this privilege. Management of application permissions aids in protecting your information from probable exploitation.

8. Keep Your Software Upto Date

By keeping your OS, browsers, and social media applications up to date, you add great security. Most of the time, software updates include patches for known vulnerabilities, and sometimes, they can even be security enhancements. This leads you to save yourself from newly discovered threats and obviously boosts your general security posture.

Why It Matters: Very often, cybercriminals tend to exploit security vulnerabilities in out of date software. By updating your applications on time, the chances of an attack are lessened since the latest security fixes are already installed on your machine.

9. Keep to secure networks:

Try to avoid unsecured or public WiFi when accessing social media because it is easy for cybercriminals to intercept. Always, if possible, connect through a secure, trusted network or use a virtual private network; this way, the internet traffic will get encrypted, and your online activities will be totally safeguarded.

Why It Matters: Public WiFi is typically a hotspot for cyberthreats. Secure connections prevent the theft or compromise of your data in any way possible.

10. Stay up to Date with New Social Media Threats

Staying updated about new emerging threats of social media will help you protect your measure in better and efficient ways. A recent series of studies have pointed out some of the emerging threats, including:

Social Engineering Attacks: Cybercriminals use manipulation techniques to get people to divulge confidential information.

Credential Stuffing: Username password combinations stolen through earlier breaches are used to gain access to accounts on other platforms.

Impersonation Scams: Scammers set up fake profiles to dupe other users into disclosing personal information or processing financial transactions.

Why It Matters: Being aware of emerging threats allows you to tweak your security practices to stay abreast with them and be better at repelling the innovative attacking techniques.

Conclusion

By implementing these integrated ways and remaining vigilant regarding fast evolving threats, you can significantly increase your level of security on social media. Protecting your online presence is actually more of a proactive exercise—be it using strong passwords or enabling two factor authentication, and being aware of threats. Safeguarding strong security measures remains important in this digital engagement for protection against personal information in order to ensure safe activity online.