

# PROTECTING YOURSELF FROM HACKERS ON FACEBOOK

Facebook, as much as we would like it to be, is not a foolproof website. Accounts get hacked and tampered with frequently and unless it happens to us, we never take adequate measures towards implementing more secure safety measures. We leave our accounts and most importantly our senses uncon-

2. Click on Settings.  
3. From there find the bar on the left and click on Apps and Websites.  
This is where you'll find a list of Active Apps which currently have access to your Facebook. Make sure to remove any app or website from that list that looks fishy to you.

want to add and follow the on-screen instructions. There are a couple of methods to choose from such as text messages sent to your mobile phone or login codes via third-party apps like Google Authenticator or LastPass.

It is important to have two-factor authen-



control is another. This is why knowing whether or not you've been hacked and the ways of getting your account back under your control are imperative to ensuring your safety on the website.

#### Finding Out Whether Your Account's Been Hacked

If you have the slightest hint of anyone trespassing on your account, go to the Settings option on your profile, click on Security and go to Where You're Logged In. You'll reach a page with a list of devices from where your account had been logged into. If you find any device or location that's unrecognizable, you can easily remove it and change your password to make sure that the suspect is unable to login from that location again.

Facebook can also notify you when your account has been logged into from a new device. To set this up, go to Settings -> Security & Login -> Setting up Extra Security -> Get Alerts about Unrecognized Logins. You then click on Edit to see your options. Here you can choose to be notified via your e-mail ID or your phone number.

But if your password has been changed without your knowledge, you'll be unable to login into your account. For this, you have to go to <https://www.facebook.com/hacked> and click on "My Account Has Been Compromised". From there, Facebook will redirect you to a search option where you put in your email address, phone number or any other unique information tied to the account. Eventually, Facebook will find your account.

This is where you have to play things smart. Enter the last password you used and a new page will come up where you click on Reset My Password. Facebook will ask you for your recovery email ID but hackers have surely changed that as well by now in which case, click on the "No longer have access to these" link. Write down your new email address where Facebook will send the password change link to and then set that as your new email ID. Follow all these steps and you will have your account back in less than 24 hours.

Bottom line is that Facebook contains all our personal messages, pictures, and valuable

cerned with the consequences of being hacked ourselves.

People generally fall for traps like, phishing emails, auto-like generator websites and quiz apps which leave their Facebook accounts vulnerable. This and the added negligence towards proper safety measures are why hacking is rampant and there's a widespread fear of hackers. Setting up a tight seal can be ensured through a number of ways however.

#### Filtering App Permissions

Every time you grant an application the permission to view your information on Facebook, you are letting it gain access to a plethora of your personal details. We do it unknowingly for utility apps but in the case of other more suspicious apps, it is best to keep your guards up regarding what information you are giving it access to. Thankfully, there is a way to filter out app permissions directly from Facebook.

#### ON PC

1. Go to the top right corner of your page and click on the downward facing arrow beside the question mark.

The process is still simple on mobile devices but has a few extra steps.

#### ON MOBILE

1. On the Facebook App, press the icon with three lines below your messenger icon.
2. Go all the way down to Settings and Privacy, click on it, and then click on the first submenu which says Settings.
3. From there, click on the Apps and Websites page under the Security submenu.
4. Click on the Logged in with Facebook and you will find a list of apps logged into your account. From there remove the ones you do not trust with your information.
5. Choose the authentication method you

cation set up because whenever you are logging in from an unknown location, you would have to complete the second phase in order for Facebook in order to verify whether it is actually you. This can save you from most garden-variety hackers who are looking to get past your password.

#### Some other security measures include:

1. Strong Password.
2. Not using your Facebook password on any other site.
3. Enable Login Notification. Go to Home -> Account Settings -> Security -> Login Notification
4. Making sure that the email account associated with your Facebook account is secure.
5. Updating your phone number.
6. Running an Anti-virus on your devices.
7. Most importantly, being careful about liking pages, downloading content from the website and while talking to unknown people.

#### PREPARING FOR THE STORM

Ensuring better security is one thing but being prepared for an attack and damage

#### Retrieving Your Hacked Account

Once you are certain that your account has been hacked, it's the time to take the necessary measures to retrieve your account. If someone only logged into your account but did not change the existing password, it means it's not too late. You can easily change your password and set up the above security measures.

#### Security Settings

information and despite all this, it's usually most people's least protected asset. But just by following the steps stated above, we can set up our accounts more securely against traps and hackers.

ASIF AYON

## MommyDaddyMe

### A SOCIAL MEDIA PLATFORM JUST FOR KIDS

Connecting children, parents and educators in a safe and friendly space.

MommyDaddyMe.com is a global social networking and knowledge-sharing platform that helps children connect with friends, learn from

guests of the event was Notre Dame University Bangladesh's VC Patrick D. Gaffney.

Javed Rahman, CEO of MommyDaddyMe.com said, "We are very keen to take down the borders and enable children to communicate, with other children or with educators around the world, under the supervision of their parents. We want to help parents raise children to be responsible users of the digital world."

The entire website is designed to encourage quality family projects and fun interactions between parents and children. It also offers parental education service as well as professional online video workshops and offline activities designed to help parents better understand their children's behaviour.

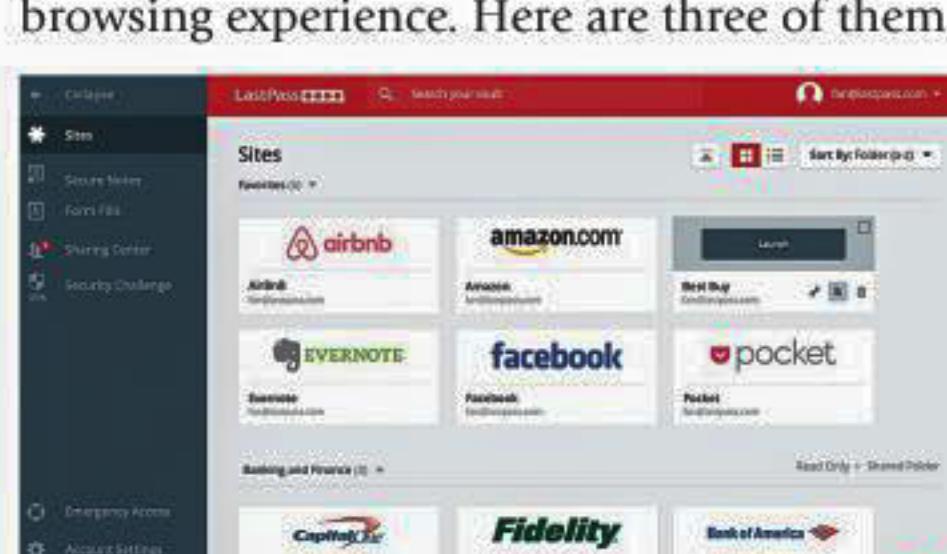


The website was introduced to the local media in a cozy press conference last week. The event was hosted by Bangladeshi national Javed N. Rahman, Co-founder and CEO; Leslie Wang, Co-founder and COO; and Mir Hasan, Managing Director of MommyDaddyMe BD Limited. Special

## APPS ON THE FLOOR

### Three essential apps for better online security

Whether it be browsing the web or having a personal conversation on the internet, nothing is truly safe from hackers and the prying eye anymore. But there are apps out there which offer better security for your existing social media accounts and your internet browsing experience. Here are three of them.



**LASTPASS** Free  
Platform: Microsoft Windows, Android and iOS  
LastPass is a great tool for storing and remembering passwords for all your different accounts. The app even allows you to enable auto login to various websites. Lastpass also has a built-in password generator so you don't have to keep using "Th1s1smyp@ssw0rd" and

other variants anymore because the app will remember the passwords for you. LastPass is a must have for remembering and organizing passwords and login IDs.

#### TELEGRAM

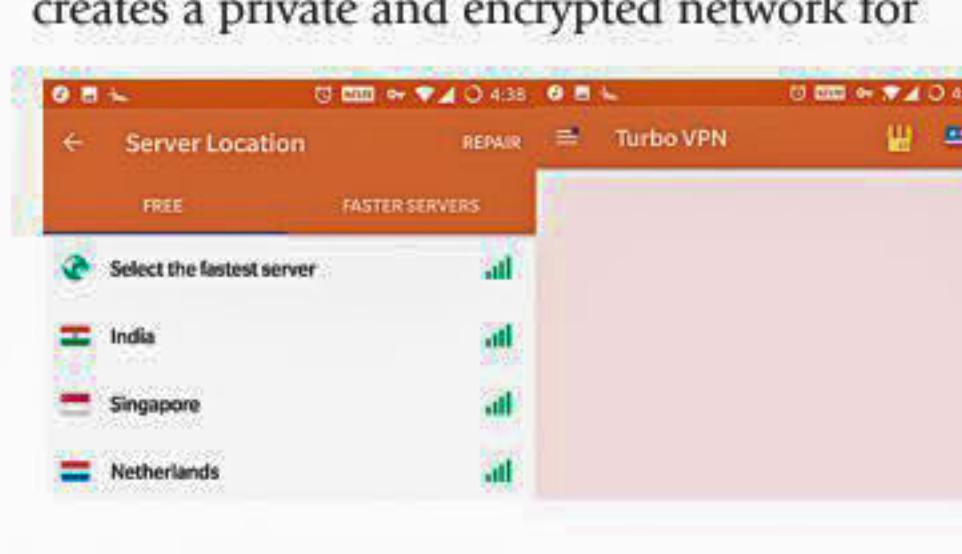
Platform: Android and iOS  
Telegram is the best WhatsApp alternative out on the market right now. Its key feature is its secret chat option which is an end-to-end encrypted communication log, accessible and viewable only through the devices the chat was initiated from. The secret chat also comes with a self-destruction function which allows the app to natively delete the conversation based on a timer you set for it. Telegram's other features are well rounded but it's the air tight secret chat function which makes it the



go-to app for having sensitive conversations over a secure space.

#### Turbo VPN

Free  
Premium Version Available  
Platform: Android and iOS  
A Virtual Private Network or VPN for short creates a private and encrypted network for



you to access over a public one that is, the internet. Turbo VPN is just one of the many free VPN apps that are available but its specialty is that, unlike most free VPN applications, it comes with a handful of servers for you to pick and choose from. It is also surprisingly quick and isn't bombarded with ads. Turbo VPN is a must have for anyone looking for better security on the internet.

ASIF AYON

