Internet Security

- How to use privacy dashboard for your account security?
- What to do if you are hacked?

How to use privacy dashboard for your account security?

Microsoft provides a privacy dashboard common for an account regardless of a number of devices.

To access privacy dashboard go to : https://account.microsoft.com/account/privacy

Sign-in to access your account.

In this page, you can manage things from your browsing data to location privacy settings. Moreover, scrolling down shows you options to manage privacy settings for various Microsoft applications.

image-1594977314366.png

Image not found or type unknown

Within the Windows app, you can control many privacy options. To see these options go to, Setting-> Privacy.

Here for each option, you maintain your privacy by enabling or disabling app permissions (location, camera, microphone etc.) which can be accessed through the options shown in the left pane.

image-1594977328610.png

Image not found or type unknown

Another important thing to note that you can choose which all apps can run in the background. This option can be visible by scrolling down the left pane.

image-1594977353585.png

Image not found or type unknown

Choose the apps you don't want to run in the background. You can turn off the apps permission by switching off the corresponding sliding switches.

What to do if you are hacked?

There are millions of hacking cases reported each year. The following steps help you to get back in track even though you are tracked.

Usual incidents following an account hacking:

- Call from your credit card company regarding any unusual activity or you notice any unusual account usage
- Strange requests to friends or family requesting money.

You can check whether your email address has been hacked by entering the website:

https://haveibeenpwned.com/

Scan your computer for any virus in your computer, as it might be the primary reasons for your account breach. Do anti-virus scan to outroot any source of breaches within the system.

Step 1: change your passwords for all your accounts: email, bank, Paypal etc. if available set-up two-factor authentication to prevent unauthorised access.

Step 2: check for any usual activity in your account, check inbox or sent items to know any contacts or password reset request happened. In such cases, inform your company or any official persons that your account is breached.

Step 3: Check your bank transactions for any transactions, it is always preferred to inform the bank to block bank cards to prevent any loss.