INTERNET SAFETY

DIGITAL EMPOWERMENT *foundation*

digitally empowering grassroots organisations

Why is it important?

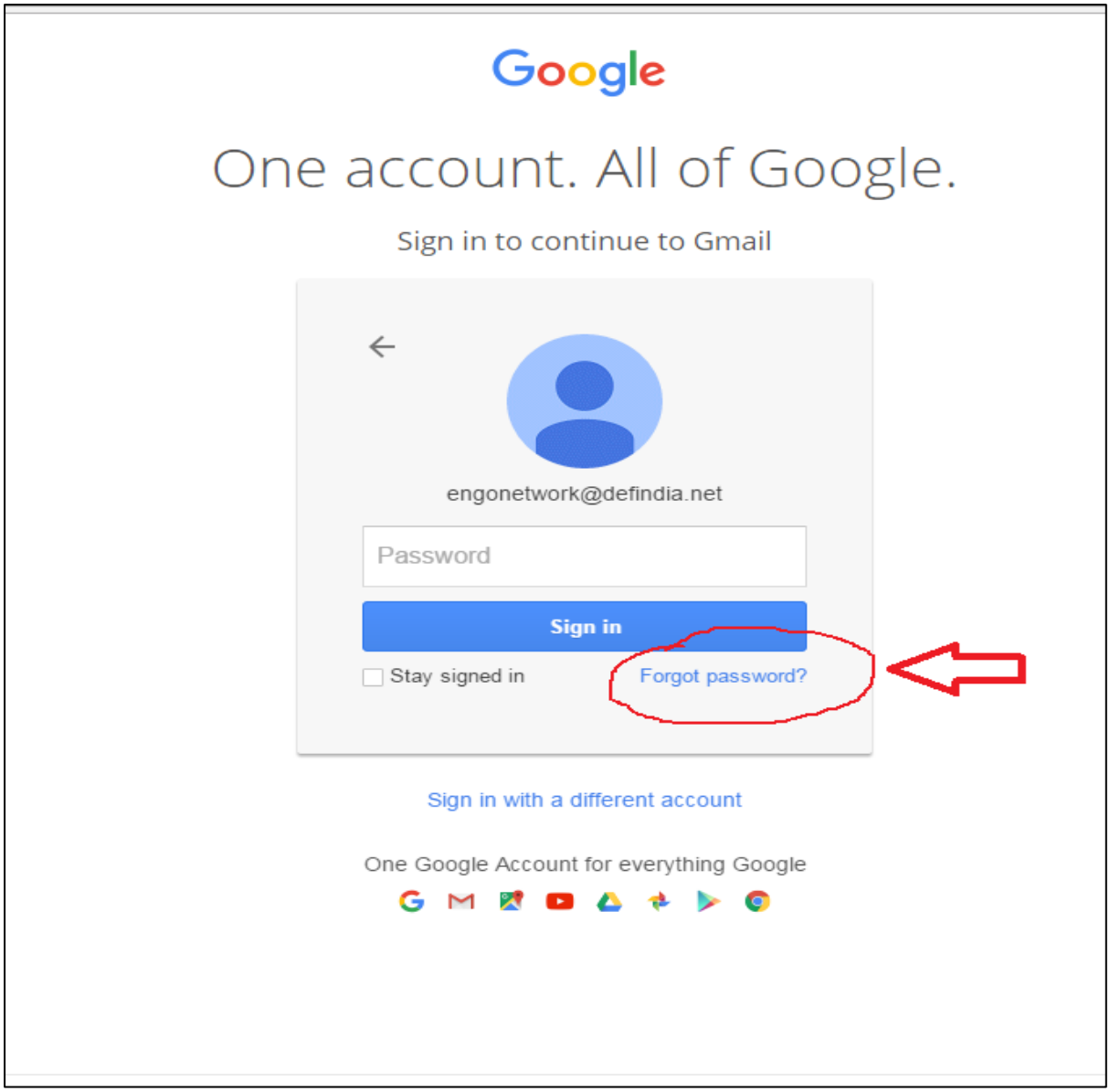
The potential of Internet to be valuable and resourceful is commendable. But the use of internet can also be a source of illegal activity and online abuse. It also places your personal information on public domains making it accessible to everyone and anyone. Our personal information on public domain is not difficult to be hacked by hackers making one more vulnerable to online crime and abuse. Preventing cybercrime is possible through little awareness and knowledge. This guide will help you prevent your information being misused on the internet.

How can you be safe on Internet?

1. Passwords

Passwords are the most important to remain safe online. They ensure your personal information is safe & secure on internet/online. One must keep in mind the points below, when it comes to safe & strong passwords:

- Passwords must be strong.
- Generic numbers can be easily hacked therefore should be avoided
- Always keep a special character in your password like @,#,%,*
- A good password is a mix of alphabets, numbers, special characters
- Keep your password long. Minimum 8 characters
- Never share your passwords with anyone, not even with your family members
- Changing passwords to passphrases, which are longer and more secure is suggested
- Never share your password or other sensitive details in a text file on your desktop or in any other way
- You can install a standalone password/ passphrase manager application. This allows you to easily copy and paste passphrases into online forms (Although confirm the reputation of the passphrase manager before use)
- To change your gmail password refer to www.passwords.google.com

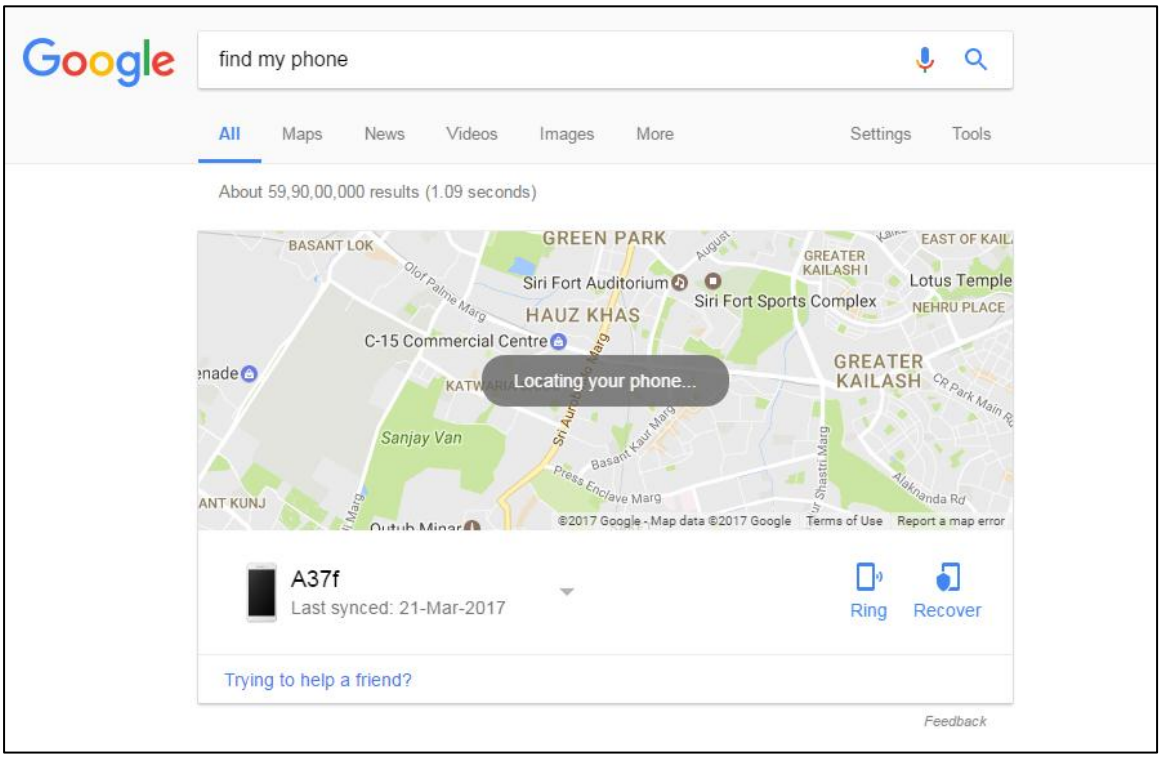


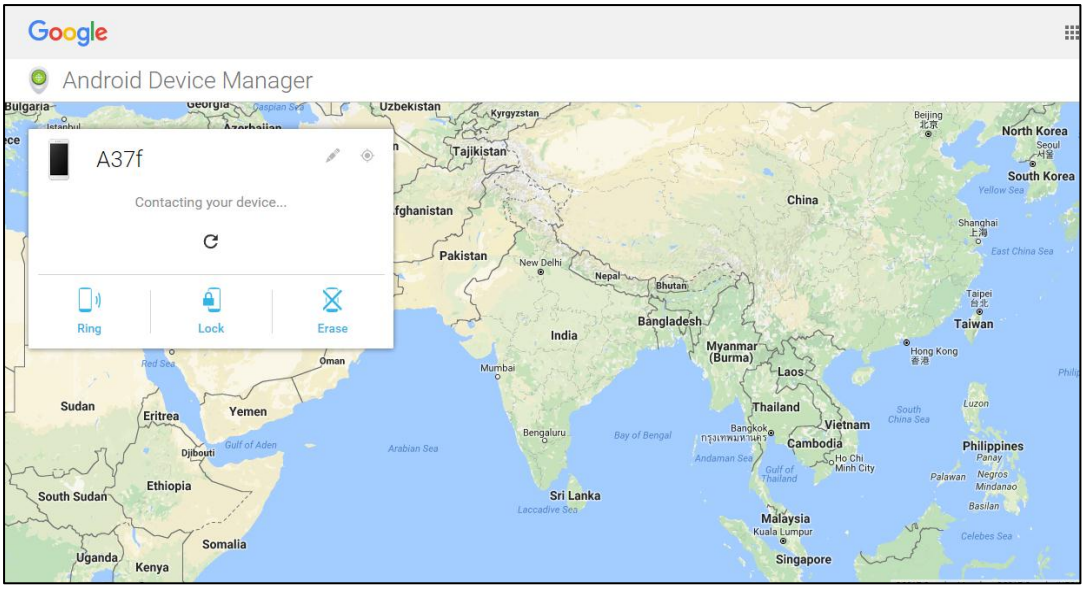
2. 2 step verification

- While making any transactions or sharing your important information online, 2 step verification ensures your information is secured
- 2 step verification takes place through two ways:
  - OTP (One Time Password)
  - A Security key
- OTP ensures your online safety as it gets invalid after few minutes of its generation
- Never share your OTP or Security key with anyone

3. Device Protection

- Secure your desktop and phone with a password
- Keep your device safe. Do not hand it to just anyone
- Do not save passwords or any important information in your phones
- If your phone is lost or stolen, go to Google home page and type “Find my phone”
- You must be signed in to your gmail account before you do this
- You can lock your phone from their or can delete the important information or can call on your phone
- *It is Android phone specific only





- For iPhones, there's an inbuilt app **'Find My iPhone'**
- It can also be downloaded from App store in ios
- 'Find My iPhone' uses your Apple id
- You can check location, can ring your phone through this app

4. Timely Software updates

- There are flaws with any software system — and it's just a matter of time before someone discovers them
- Software updates notification that appears on your device are important
- Regularly install software updates
- Software updates are useful to avoid your device being hacked

5. Download apps from a trusted source

- While downloading any app, keep in mind to download it form a trusted source
- Download only from Google Play Store in Android and App store in ios
- Look for the permissions they ask, very carefully. Look specifically for the privacy access asked for
- Review app reviews, star ratings & download counts
- Report bad apps to Google
- Do not download apps from any random internet site

- Your phone and personal data are vulnerable to attack by apps from unknown sources. If you download apps from unknown sources, be aware that your phone may be damaged or may lose data
- If you download apps from sources outside Google Play or App store, Verify Apps, scans those apps for malware before and after you install them
- When you try to install a potentially harmful app from outside of Google Play, Verify Apps will either:

- Recommend that you don't install the app.
- Block the installation of the app completely (if there's a security threat to your device).

- Keep app verification on

  Verify Apps regularly checks activity on your device and prevents or warns you about potential harm. Verify Apps is on by default, but you can turn Verify Apps off. For security, we recommend that you keep Verify Apps on.

  To turn Verify Apps off or back on:

  1. Open your device's Settings app .
  2. Under "Personal," tap **Google** > **Security**.
  3. Under "Verify apps," tap **Scan device for security threats**.

  Tip: On some devices, you'll find your Google Settings in a separate Google Settings app .

- Get warnings about potentially harmful apps

  Verify Apps checks apps when you install them from sources other than Google Play. Verify Apps also periodically scans for potentially harmful apps.

6. Lock your screen

- Always keep your phone locked with a password
- One can go to settings and can set a strong password
- Configure your computer device and mobile phones with a password or passphrase, necessary for access
- Activate a passphrase-protected screen saver or lock screen that automatically activates after few minutes of computer or device inactivity

7. Spam mails

- Be aware of Spam mails that land in to your email
- Incase you receive an email with a link, instead of clicking on it, open a new webpage, type the website name yourself and then log in. Alternatively, you can also click on the website name from your bookmarks list.
- Never respond to mails asking your important information like bank account password or bank account number
- Research before you believe or share any such important information with anyone over email
- Be aware of online scams
- Malware warning- When it detects a problem, the browser shows a warning, alerting user that content from a site we have identified as being malicious is being loaded.
- Be aware of 'Phishing'
- Phishing is the fraudulent practice of sending emails puporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers.

8. Secured Communication

- Certain mobile apps are not privacy-friendly. To install them, you must give them permission to access and in some cases control over many other services on your device. Make sure you use them wisely
- Be careful on what you share online (images, important and personal information)

9. Prevent your website getting hacked

- Secure traffic to the site. It is extremely important to enable HTTPS access to your site
- Transport Layer Security (**TLS**) and its predecessor, Secure Sockets Layer (SSL), both frequently referred to as "SSL", are cryptographic protocols that provide communications security over a computer network.
- The secure channel requires you to validate the site's trustworthiness with a TSL certificate that you purchase from a certificate authority

- Several certificate authorities issue free certificates to nonprofits, choose wisely

10. Online Abuse

- Wi-Fi hotspots and Bluetooth connections can reveal your location and make it easier for people to hack your phone. Secure your Wi-Fi and turn off Bluetooth when not using it
- Disable GPS when not using
- Disable GPS on your mobile camera
- Install trusted anti-malware
- Maintain privacy on social media. Leave optional fields blank while registering online
- Be careful with your profile photo on social media and other personal information
- Check your privacy settings regularly. Social media services change their privacy policy all the time, so check in regularly so that you are ensured you are sharing the information that you want to share

- As much as you must be careful about your safety online, you must educate your children on how to be safe on internet.
- Always have an Anti-Virus installed on your computer and on your phone too.
- Do not give access to your photographs in your phone to various apps that demand the access.
- You only need to be careful and aware!