The do’s and don’ts of staying safe online.

bodhini.in/the-dos-and-donts-of-staying-safe-online/

October 13, 2019

The DO’S

1. Be careful about what you post online
Never post your future plans, information that reveals your location, phone, address, school, relations or anything that will help someone learn about you.

2. Check the photographs you share once again
Your photos may have your GPS locations, landmarks, house, vehicle number or other information that should not be made public.

3. Use a strong password
Take three random words (TOYOTA, MONKEY, JUPITER). Join them and replace characters with similar looking numbers (tOyOt4mOnk3yyjupi73r). Now add a secret line and name of the app to make a unique password. (t0y0t4mOnk3yyjupi73rhellogmailb).

4. Use open source software’s that are more secure
Make use of Firefox, Open office, VLC media player, Linux riot etc. instead of the ones by companies. Check the list at prism-break.org

5. Make sure you are connecting to the right website
Check if you can see the https:// in the address bar and read out the spelling for the website.

6. Use a firewall app
Use a firewall app in your phone and make sure incoming connections are dropped.

7. Do not use pirated software
If you want free software search for opensource software eg: “Opensource media player”, Opensource camera app”.

8. Be careful about downloading applications
Spend some time reading the permissions and terms and conditions of apps.

9. Be careful when using games
Games can at times ask for too much information from you. If you need to, give false data. Don’t reveal your real details including number or chat id online.

10. Be careful while making video calls
No matter what people tell you, chats and calls can be recorded.

11. Learn to switch off
Studies have shown links between depression and social media. Watching other people’s seemingly exciting lives and feeling low seem to be connected. If you do feel low, switch off your gadgets and look for other options like arts, reading a book, listening to music, connecting with nature etc. What you see online of people’s lives are what they want to project, not necessarily real. If you feel that your gadgets are taking over your life, stay off the net for14-21 days and use them minimally thereafter.

12. Use encrypted vaults to store personal photos
For example: https://play.google.com/store/apps/details?id=com.netqin.ps

13. Save Evidence
Block out sexually suggestive messages or chats from unwanted people. Do not delete or deactivate accounts or texts. Back up information for proof.

14. Reach out
Reach out to friends, family or the law enforcement agencies like the police if in trouble. If you give in to threats, it only gets worse.

15. Turn off Bluetooth and wi-fi when not in use

16. Use two factor authentication

17. Lock screen for added protection

The DON’TS

1. Trust no one with your phone
Do not leave your phone with friends or at repair shops. Remove the SIM, SD Card and reset before giving for repair. If you can’t do this, stay with the phone while it gets repaired and as much as possible get it done at authorized service shops only.

2. Do not share Children’s photographs Online The internet is not a safe place for a child’s photograph, their photos can be sold online to pedophile’s and sex traffickers. Let us not put their lives at risk.

3. Do not give in to threats or blackmail The person hiding behind a gadget and trying to scare you is a coward. Break the cycle of fear. Warn him that you will report him to the law enforcement if he does not stop harassing you.

4. Avoid posting photos while traveling Photographs and updates you share while traveling can reveal way too much about you and your location. Make sure you keep this to the minimum.

5. You need to be alert and careful about what you share Understand that privacy settings won’t protect you totally.

6. Do not bully anyone online Bullying people online is not only illegal, it could lead to them taking their lives and leave you with a charge of abetting to murder.

7. Do not blindly share information Do not share information without checking if they are genuine, as in a lot of cases, it turns to be wrong or fake.

8. Never store anything that is too personal on cloud drive, email account or in phoneEverything stored online will get deleted or become public in time. Online is not where you should store critical materials.

9. Auto deleting apps do not protect you well Apps that seem to delete messages after some time do not always work and data can be retrieved. So if you don’t want something to be recorded, don’t say or post it.

10. Do not look up Social Media profile of people you have broken away from It could lead to mood swings and depression.

11. Do not spend time online when you are depressed It could leave you feeling more depressed looking at other people’s seemingly exciting lives.

12. Do not Share Hate inducing posts, It not only wrecks beautiful relationships but also adds to hate and negativity in your life.

13. Do not charge your phone in public ports

DOWNLOAD OUR POSTER

STAYING SAFE ONLINE

Use your gadgets wisely, Do not let it use or define your life

DON'TS

- **Trust no one with your phone**
  Do not leave your phone with friends or at repair shops. Remove the SIM, SD Card and reset before giving for repair. If you can't do this, stay with the phone while it gets repaired and as much as possible get it done at authorised service shops only.

- **Do not share Children's photographs Online**
  The internet is not a safe place for a child's photograph, their photos can be sold online to paedophiles and sex traffickers. Let us not put their lives at risk.

- **Do not give in to threats or blackmail**
  The person hiding behind a gadget and trying to scare you is a coward. Break the cycle of fear. Warn him that you will report him to the law enforcement if he does not stop harassing you.

- **Avoid posting photos while traveling**
  Photographs and updates you share while traveling can reveal way too much about you and your location. Make sure you keep this to the minimum.

- **You need to be alert and careful about what you share**
  Understand that privacy settings won't protect you totally.

- **Do not bully anyone online**
  Bullying people online is not only illegal, it could lead to them taking their lives and leave you with a charge of abetting to murder.

- **Do not blindly share information**
  Do not share information without checking if they are genuine, as in a lot of cases, it turns to be wrong or fake.

- **Never store anything that is too personal on cloud drive, email account or in phone**
  Everything stored online will get deleted or become public in time. Online is not where you should store critical materials.

- **Auto deleting apps do not protect you well**
  Apps that seem to delete messages after some time do not always work and data can be retrieved. So if you don't want something to be recorded, don't say or post it.

- **Do not look up Social Media profile of people you have broken away from:** It could lead to mood swings and depression.

- **Do not spend time online when you are depressed**
  It could leave you feeling more depressed looking at other people's seemingly exciting lives.

- **Do not Share**
  Hate inducing posts, It not only wrecks beautiful relationships but also adds to hate and negativity in your life.

- **Do not charge your phone in public ports**

BODHINI
Freedom From Fear

HELPLINE

Bodhini : 8891320005
Crime stopper : 1090
Childline: 1098

Email:office@bodhini.in
Web: www.bodhini.in
Facebook: https://www.fb.com/BodhiniHelp/

DO'S

- **Be careful about what you post online**
  Never post your future plans, information that reveals your location, phone, address, school, relations or anything that will help someone learn about you.

- **Check the photographs you share once again**
  Your photos may have your GPS locations, landmarks, house, vehicle number or other information that should not be made public.

- **Use a strong password**
  Take three random words (TOYOTA, MONKEY, JUPITER). Join them and replace characters with similar looking numbers (t0y0t4m0nk3yyjupi73r). Now add a secret line and name of the app to make a unique password. (t0y0t4m0nk3yyjupi73rhellogmailb).

- **Use open source softwares that are more secure**
  Make use of Firefox, Open office, VLC media player, Linux riot etc instead of the ones by companies. Check the list at prism-break.org

- **Make sure you are connecting to the right website**
  Check if you can see the https:// in the address bar and read out the spelling for the website.

- **Use a firewall app**
  Use a firewall app in your phone and make sure incoming connections are dropped.

- **Do not use pirated software**
  If you want free software search for opensource software eg: "Opensource media player", Opensource camera app".

- **Be careful about downloading applications**
  Spend some time reading the permissions and terms and conditions of apps.

- **Be careful when using games**
  Games can at times ask for too much information from you. If you need to, give false data. Don't reveal your real details including number or chat id online.

- **Be careful while making video calls**
  No matter what people tell you, chats and calls can be recorded.

- **Learn to switch off**
  Studies have shown links between depression and social media. Watching other people's seemingly exciting lives and feeling low seem to be connected. If you do feel low, switch off your gadgets and look for other options like arts, reading a book, listening to music, connecting with nature etc. What you see online of people's lives are what they want to project, not necessarily real. If you feel that your gadgets are taking over your life, stay off the net for14-21 days and use them minimally thereafter.

- **Use encrypted vaults to store personal photos**
  For example: https://play.google.com/store/apps/details?id=com.netqin.ps

- **Save Evidence**
  Block out sexually suggestive messages or chats from unwanted people. Do not delete or deactivate accounts or texts. Back up information for proof.

- **Reach out**
  Reach out to friends, family or the law enforcement agencies like the police if in trouble. If you give in to threats, it only gets worse.

- **Turn off bluetooth and wi-fi when not in use**

- **Use two factor authentication**

- **Lock screen for added protection**

KERALA POLICE
मृदु भावे दृढ़ कृत्ये