

## ABCs of Information Security

**A** 

Always properly log out after completion of online transactions

**C** 

Clear cookies and delete browsing history at the end of session and stay safe

**G** 

Giving out your personal information online is not advisable

**K** 

Keep software up to date

**O** 

Only install apps and software from trusted sources

**S** 

Scan any file downloaded from internet before opening/using/installing

**W** 

Watch out for online scams

**D** 

Do not carry your PIN number in wallets better to memorize your PIN

**H** 

Help yourself to maintain a positive online presence

**L** 

Lock your devices when not in use

**P** 

Pay extra attention when using public Wi-Fi

**T** 

Turn on Automatic Updates for your operating system

**X** 

XTRA precaution for your online financial transactions

**E** 

Enlighten yourself on Cyber Security measures

**I** 

Install Anti-Virus Protection

**M** 

Monitor your accounts for any suspicious activity

**Q** 

Quarantine all unused apps

**U** 

Use strong passwords with personal acronym

**Y** 

Your priority on cyber security makes you cyber aware citizen

**B** 

Be careful what you click

**F** 

Following basic rules of social networking can prevent damaging your online relationships

**J** 

Join hands to stop spreading fake news

**N** 

Never believe on forward messages, check source and URL

**R** 

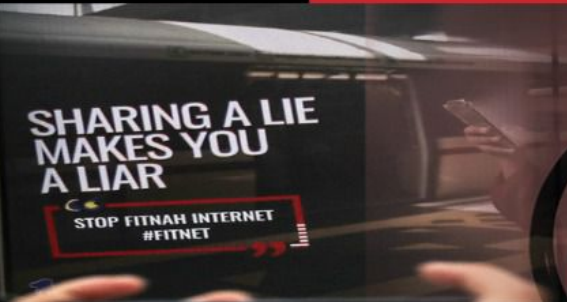
Respect the privacy of others

**V** 

Verify with whom you are interacting online

**Z** 

Zero participation in dark web



SHARING A LIE  
MAKES YOU  
A LIAR

STOP FITNAH INTERNET  
#FITNET



**FAKE  
NEWS**



Misinformation  
Misinformation  
Misinformation  
Misinformation  
Misinformation

## How to spot **FAKE NEWS**



There are a number of things to watch out for when evaluating content online.

### **1** Take a closer look

Check the source of the story, do you recognize the website? Is it a credible/reliable source? If you are unfamiliar with the site, look in the about section or find out more information about the author.

### **2** Look beyond the headline

Check the entire article, many fake news stories use sensational or shocking headlines to grab attention. Often the headlines of fake new stories

are in all caps and use exclamation points.

### **3** Check other sources:

Are other reputable news/media outlets reporting on the story? Are there any sources in the story? If so, check they are reliable or if they even exist!

### **4** Is it a joke?

Mocking sites are popular online and sometimes it is not always clear whether a story is just a joke or parody... Check the website, is it known for creating funny stories?

### **5** Check the facts

check for published date and time. Fake news stories often contain incorrect dates or altered timelines. It is also a good idea to check when the article was published, is it current or an old news story? Have a check on who is the author.

### **6** Check your biases:

Are your own views or beliefs affecting your judgment because of news feature or report?

### **7** Think before you share

## MOBILE PHONE SECURITY

*Mobile phones are becoming ever more popular and are rapidly becoming attractive targets for malicious attacks. Mobile phones face the same security challenges as traditional desktop computers, but their mobility means they are also exposed to a set of risks quite different to those of a computer in a fixed location*



**Mobile phones can be infected with worms, Trojan horses or other virus families, which can compromise your security and privacy or even gain complete control over the device.**

### Do's

- Record the unique 15 digit IMEI number.
- Use auto lock to automatically lock the phone or keypad lock protected by passcode/ security patterns to restrict access to your mobile phone.
- Report lost or stolen devices immediately to the nearest Police Station and concerned service provider.
- Use the feature of Mobile Tracking which automatically sends messages to two preselected phone numbers of your choice which could help if the mobile phone is lost/ stolen.
- Take regular backup of your phone and external memory card.
- Before transferring the data to Mobile from computer, the data should be scanned with latest Antivirus with all updates.
- Use Wi-Fi only when required. It is advisable to switch off the service when not in use.
- Download APPS only from trusted sources to avoid spywares.

### Dont's

- Never leave your mobile device unattended.
- Do not turn on applications [camera, audio/video players] and connections [Bluetooth, infrared, Wi-Fi] when not in use to avoid security issues.
- Never allow unknown devices to connect through Bluetooth.
- Never keep sensitive information like user names/passwords on mobile phones.
- Never connect to unknown networks or untrusted networks.

(<https://cycord.gov.in>)

---

## **NATIONAL CYBER SECURITY AWARENESS MONTH** **OCTOBER, 2020**

### **Conventional Cyber Security Norms and Best Practices**

1. Always use genuine software.
2. Install the latest updates/patches for Operating System, Antivirus and Application software.
3. Enable a firewall. Operating Systems have an inbuilt firewall which can be used to stop unwanted internet connections.
4. Limit user privileges on the computer. Always access Internet as a standard user but not as Administrator.
5. Check and verify email sender IDs and web links before opening file attachments and clicking on links in emails and web pages.
6. Protect against social engineering attacks. Phishing emails and SMS are used to get user credentials like username, passwords, credit card and PIN numbers etc.
7. Regularly check the last logging details of email accounts.
8. Use strong passwords that include a combination of letters, numbers, and symbols.
9. Use only officially supplied USB storage media. USB storage media should be regularly formatted after use to erase any malicious files hidden from normal view.
10. Regularly take backup of document files to avoid loss of files in case of emergencies like malware infections, hard disk crash, corrupted applications and other unforeseen incidents.
11. Users should be periodically briefed about Cyber Security measures.
12. Avoid downloading and installing pirated software.
13. Internet-connected computers should not be used for drafting / storing sensitive official documents / correspondences.
14. Don't open emails from unknown email IDs. Such mails should be deleted from email account inbox.
15. Don't download and open file attachments that originated from unknown sources.

<https://cycord.gov.in>

---

16. Auto storage of user name and password in browser /web page should be disabled in shared computers used for Internet activities.
17. Avoid using personal USB storage devices / Smart Devices on office computers. Don't put unknown USB storage device into your Computer.
18. Don't share passwords with anyone. Don't use the same password on all websites and services.

**A) A few indicators of a Generic Malware infected computer:**

1. Computer runs slowly than normal, stops responding or freezes often. Computer crashes and restarts every few minutes.
2. Unusual error messages pop up constantly.
3. New toolbars, links, or favourites added to your web browser.
4. Home page, mouse pointer, or search program changes unexpectedly.
5. Unusual network traffic and connectivity from the computer even without doing any Internet activity.
6. These are common signs of malware infection, but they may also be indicative of mere hardware or software problems.

**B) Tips to check and protect from malware infections in Windows computer.**

1. Always set automatic updates for Operating System, Anti-Virus and Applications. For Windows OS auto update can be done as follows: -

**Control Panel -> Windows Updates ->Change Settings -> Install updates automatically.**

(For other software follow the steps as given in the respective software.)

2. Checking for unusual network traffic with Windows “netstat -na” command.

**Type “cmd” in “run” and type “netstat -na”. Checkout foreign Established connection and IP addresses. Check the IP address for its ownership**

(<https://cycord.gov.in>)

---

3. Check for any unusual executable running automatically at Windows startup.

**Type “msconfig” in “run” and check for any unusual executable running automatically.**

(Disable, delete or uninstall any unnecessary /unknown executable/program.)

4. Enable hidden files, folders and system files view to find any unusual or hidden files, especially useful while using USB storage devices.

**Control Panel -> Folder Options -> View -> select the “Show hidden files and folders” option and unselect “Hide protected operating system files”**

Make sure there is no hidden file and folders present in the USB Storage device. Format the device if any unusual files (files having extensions exe, com, dat, scr and ini etc) are present besides the data files (doc, ppt, xls and pdf etc).

5. Delete the contents of Windows “Temp” and “Temporary Internet files” regularly.
  - (a) Type %temp% in “run” and delete all the contents of temporary folder.
  - (b) For deleting Temporary Internet Files follow steps as given by different browsers like Windows Internet Explorer, Google Chrome, Mozilla Firefox, Opera and Apple Safari.

**Cyber security awareness and knowledge sharing can be our best defence against emerging cyber threats. Let us work together to maintain high standards of cyber and information security in the country.**

**CyCord Support Team**  
E-mail: [cycordsupport.mha@gov.in](mailto:cycordsupport.mha@gov.in)  
Land Line: 011- 24158307  
WhatsApp: +917292045198  
Website: [www.cycord.gov.in](http://www.cycord.gov.in)