A Handbook on Cyber Hygiene

Cyber Security Centre of Excellence (CS-CoE)
Department of Information Technology & Electronics
Government of West Bengal

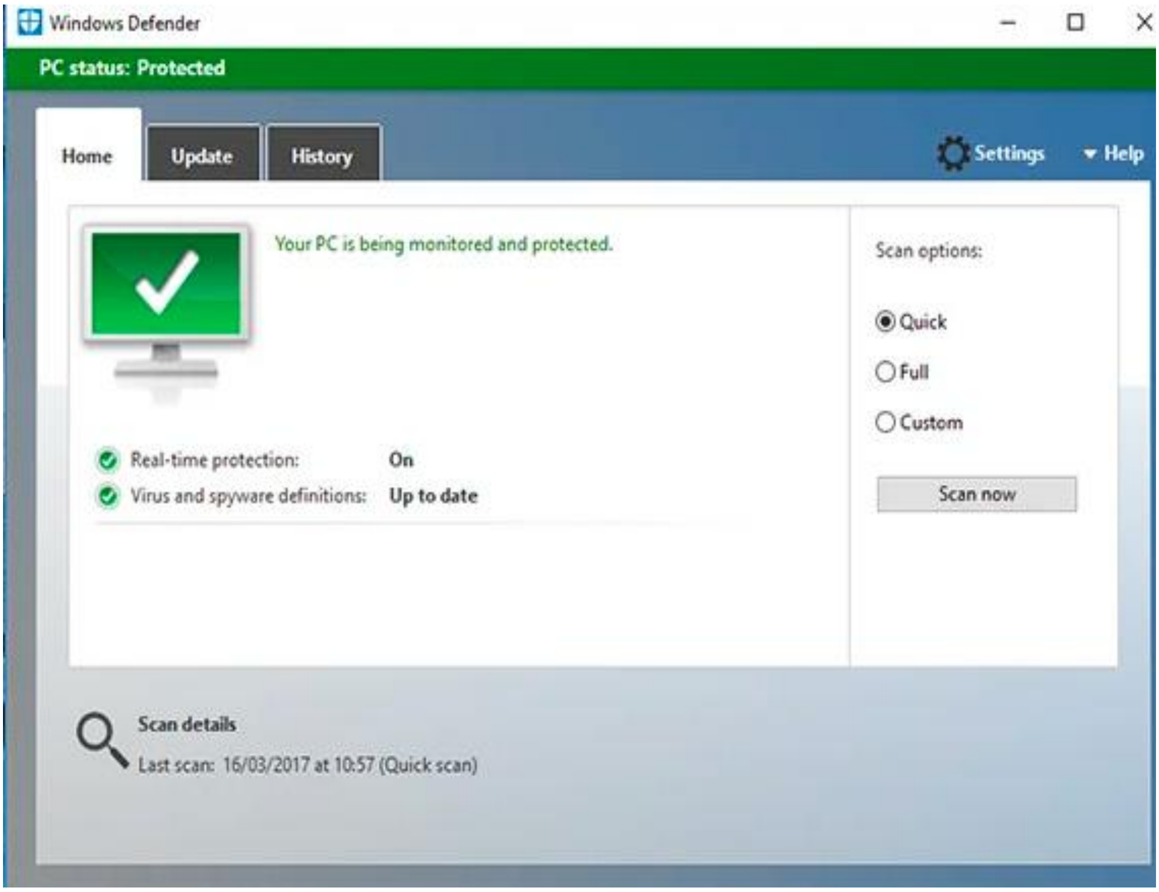
https://cscoe.itewb.gov.in

General Computer Usage

1. Password length should be minimum 10 characters using a combination of letters, numbers and special characters.

PASSWORD
12345678
wH0192014et!V

2. Use of Anti-virus is mandatory. Anti-virus should only be device specific, paid and licensed software application. Anti-virus software available for free download should not be installed.



PC status: Protected

Your PC is being monitored and protected.

Real-time protection: On

Virus and spyware definitions: Up to date

Scan options:

● Quick

○ Full

○ Custom

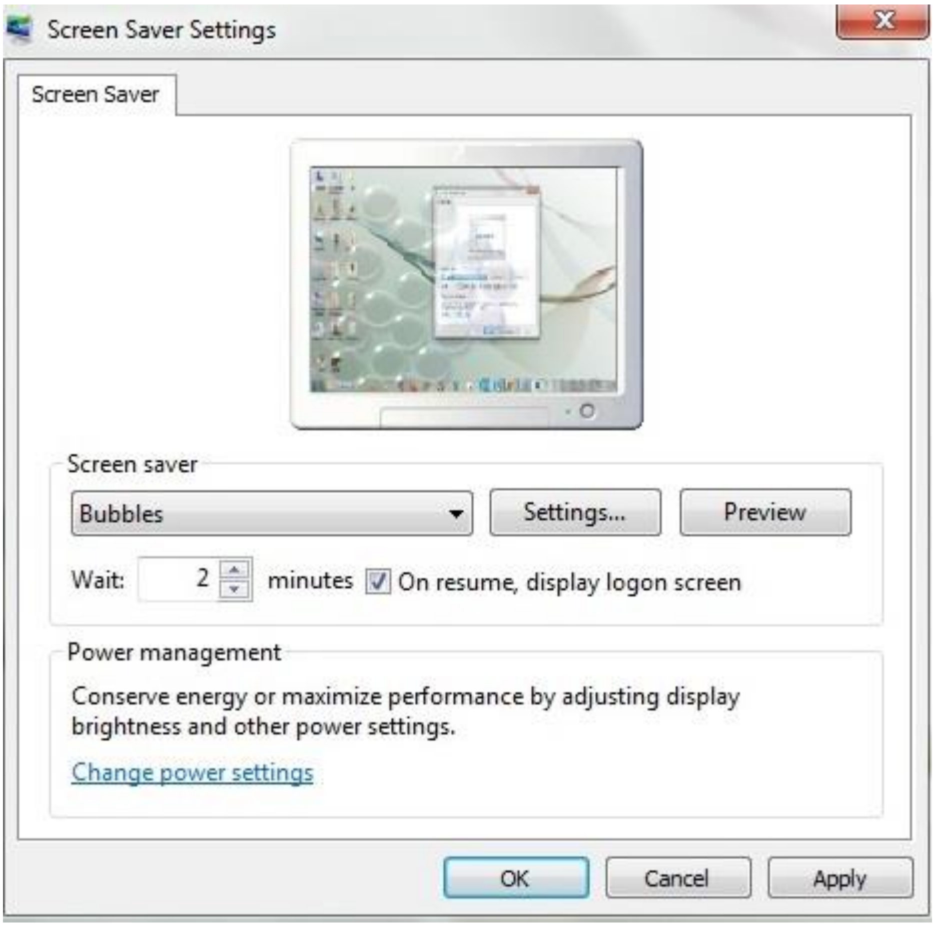
Scan details

Last scan: 16/03/2017 at 10:57 (Quick scan)

3. Always log-off your computer when leaving it unattended with [windows + L] or [Ctrl+Alt+Del]

If all else fails,

4. Screensaver with timeout period of maximum 2 minutes should be enabled.



Screen saver

Bubbles

Wait: 2 minutes ☑ On resume, display logon screen

Power management

Conserve energy or maximize performance by adjusting display brightness and other power settings.

Change power settings

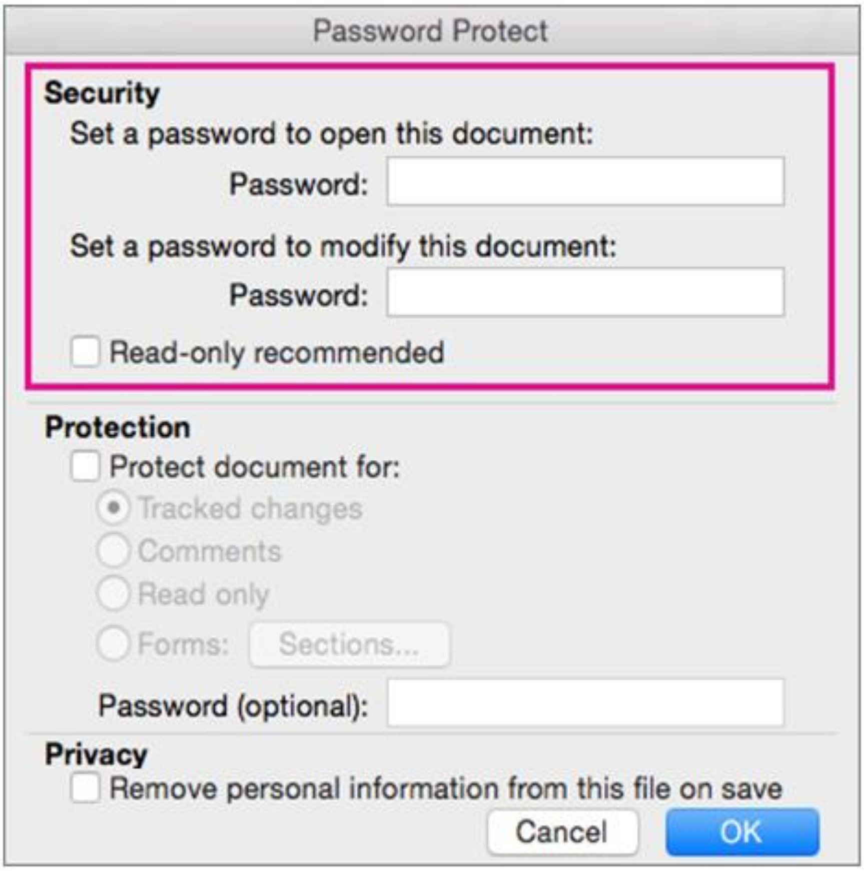
General Computer Usage

5. Do not download unnecessary programs from anywhere, even from legitimate trusted sources.

6. Do not use public computers/ cyber cafes for office work.

General Computer Usage

7. Enable password protection feature for sensitive documents.



Password Protect

Security

Set a password to open this document:

Password:

Set a password to modify this document:

Password:

☐ Read-only recommended

Protection

☐ Protect document for:

● Tracked changes

○ Comments

○ Read only

○ Forms: Sections...

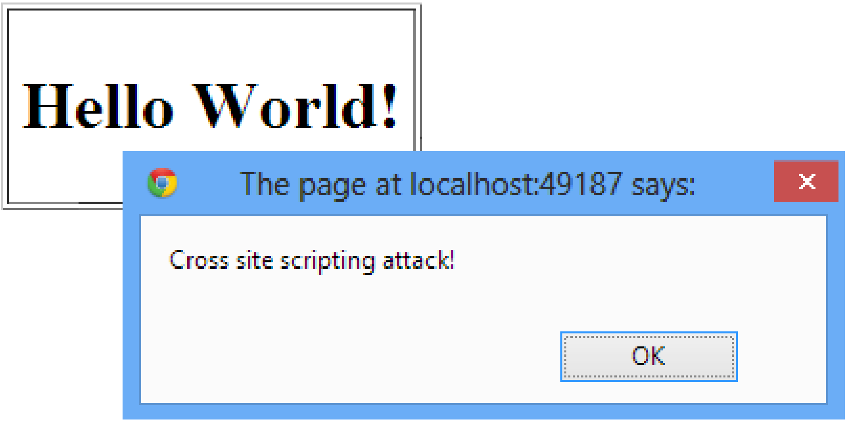
Password (optional):

Privacy

☐ Remove personal information from this file on save

General Internet Browsing

8. Do not click on untrusted links even if they appear to be from a legitimate source. For example, any link to a cricket score website on an airline ticket booking page.



Hello World!

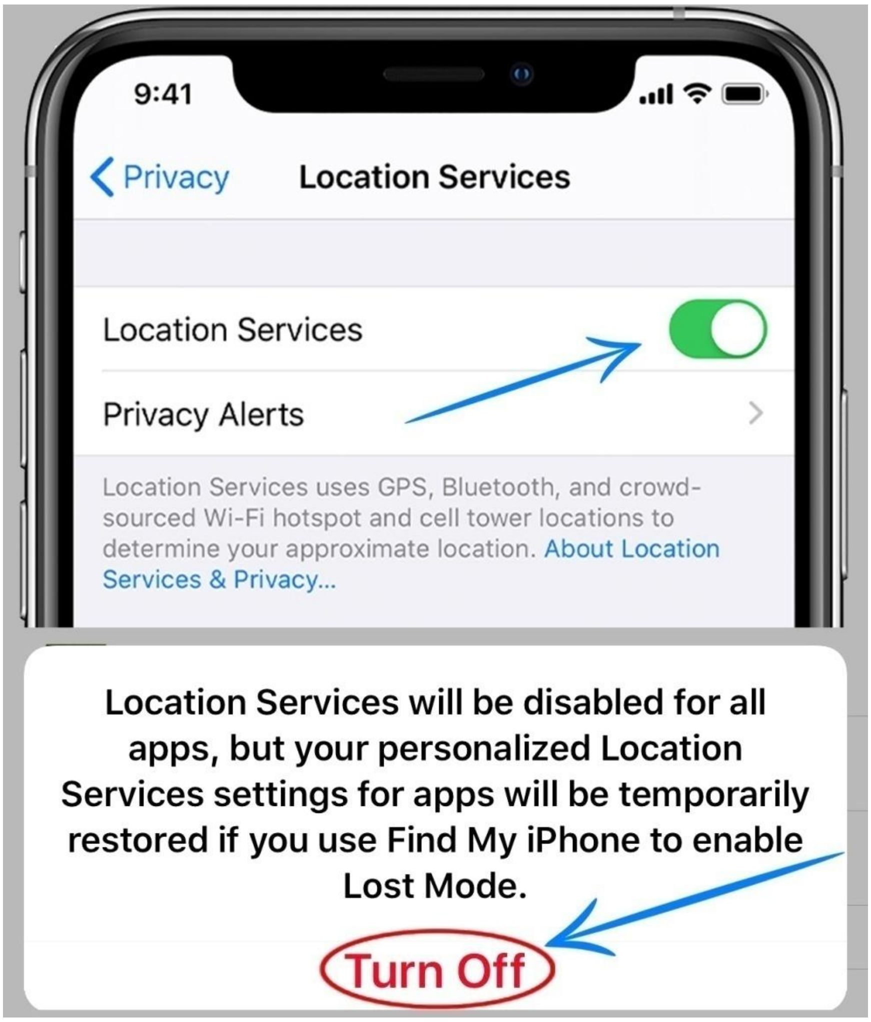
The page at localhost:49187 says:

Cross site scripting attack!

General Internet Browsing

9. Always look for a green/grey padlocked symbol of "https". Yellow or red "https" means that the website is insecure.

10. When on tour, don't avail such services that require location information.



9:41

Privacy | Location Services

Location Services

Privacy Alerts

Location Services uses GPS, Bluetooth, and crowd-sourced Wi-Fi hotspot and cell tower locations to determine your approximate location. About Location Services & Privacy...

Location Services will be disabled for all apps, but your personalized Location Services settings for apps will be temporarily restored if you use Find My iPhone to enable Lost Mode.

Turn Off

General Internet Browsing

11. Don't perform any financial transactions by using public computers or public Wi-Fi connections. There is a risk that your information can be read by unauthorized people.

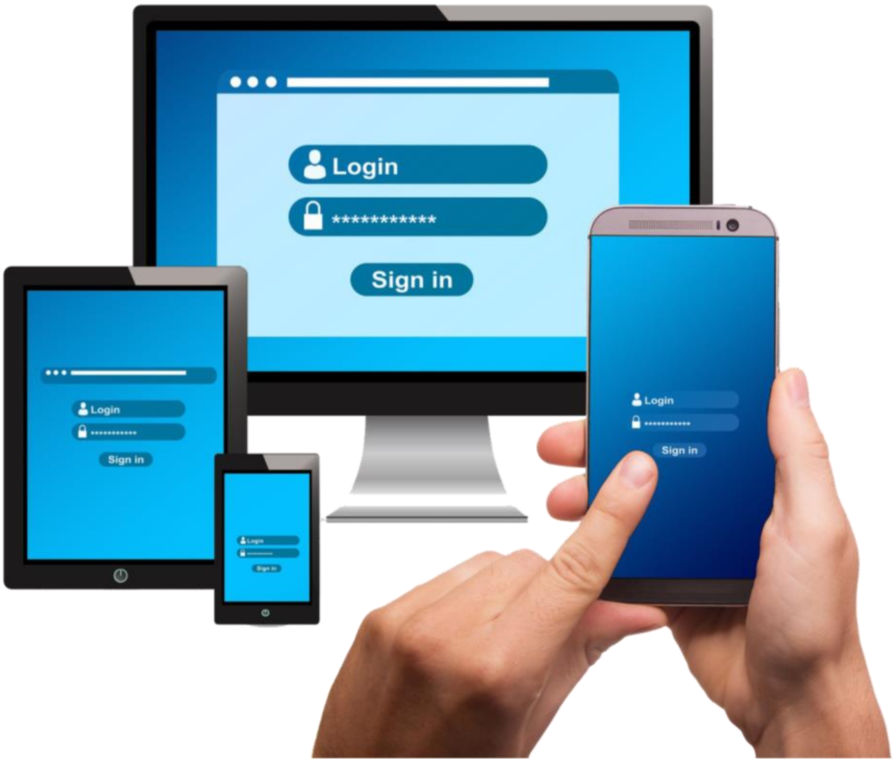
Password Management

12. Be careful while entering passwords in front of others. Change your password immediately if you suspect that it has been compromised.

Password Management

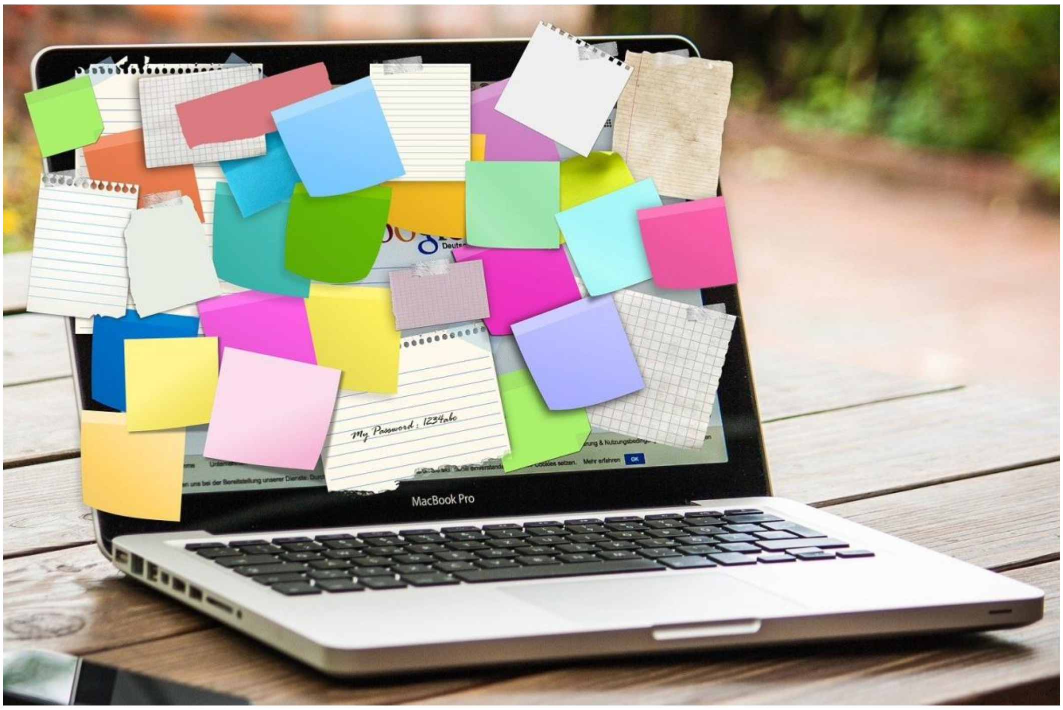
13. Report suspicious activity (such as slow systems/unknown files on desktop/ software applications installed by unknown sources) to the IT team.

14. Don't reuse old passwords. Reused passwords are easier to crackthrough by observing key-log patterns or by social engineering.



Password Management

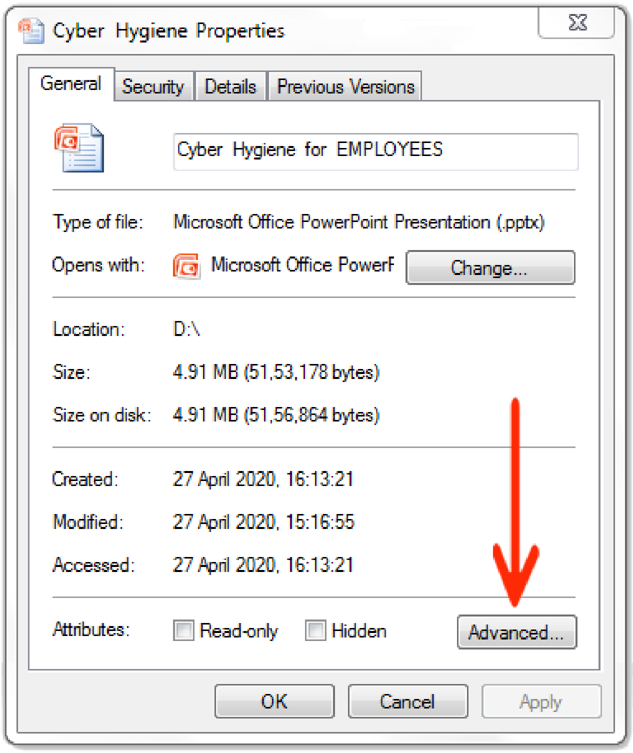
15. Don’t store the passwords in readable form in computers, notebook, notice board, etc.



16. Don’t use the common passwords such as Name of family, pets, friends, birthdays, etc.

Removable Information Storage Media

17. Try to encrypt the data before copying into removable storage media.



Cyber Hygiene Properties

Cyber Hygiene for EMPLOYEES

Type of file: Microsoft Office PowerPoint Presentation (.pptx)

Opens with: Microsoft Office PowerF

Location: D:\

Size: 4.91 MB (51,53,178 bytes)

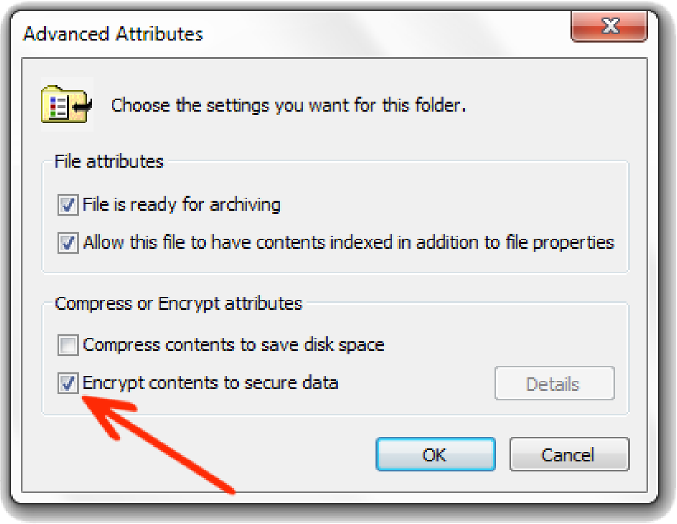
Size on disk: 4.91 MB (51,56,864 bytes)

Created: 27 April 2020, 16:13:21

Modified: 27 April 2020, 15:16:55

Accessed: 27 April 2020, 16:13:21

Attributes: □ Read-only □ Hidden



Advanced Attributes

Choose the settings you want for this folder.

File attributes

☑ File is ready for archiving

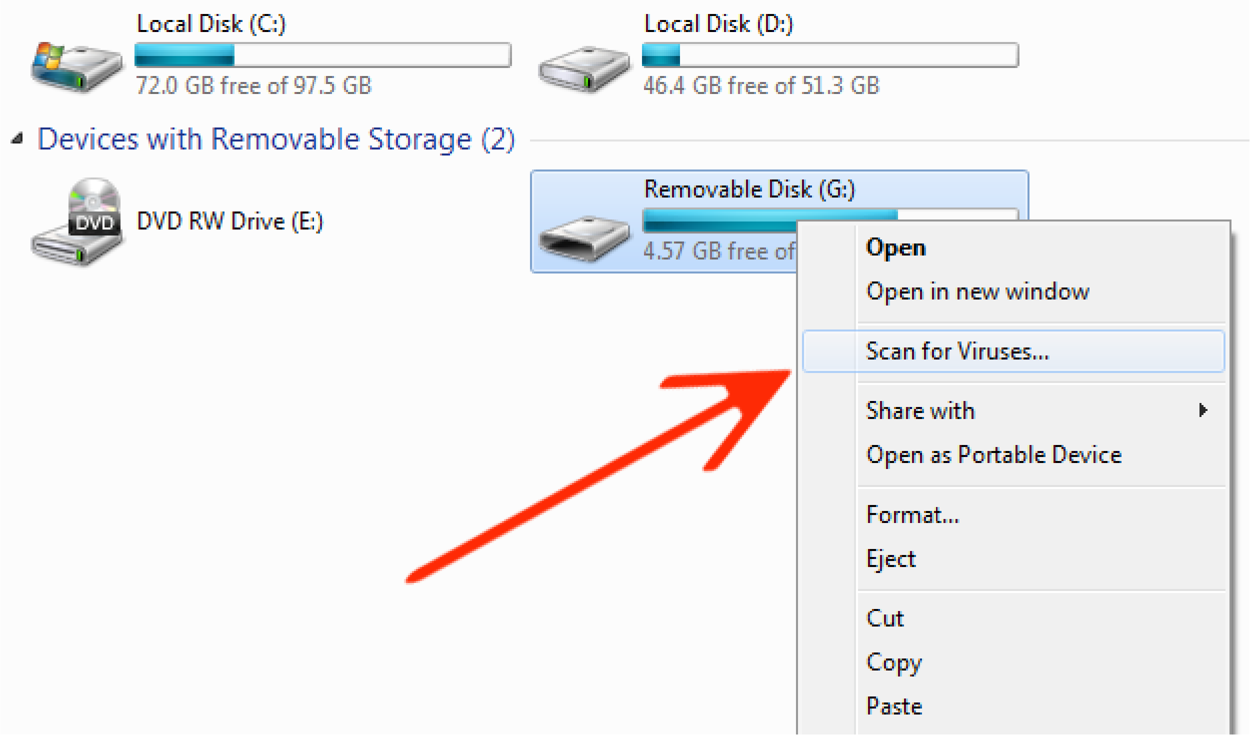
☑ Allow this file to have contents indexed in addition to file properties

Compress or Encrypt attributes

□ Compress contents to save disk space

☑ Encrypt contents to secure data

18. Always scan all removable media with antivirus.



Local Disk (C:)

72.0 GB free of 97.5 GB

Local Disk (D:)

46.4 GB free of 51.3 GB

Devices with Removable Storage (2)

DVD RW Drive (E:)

Removable Disk (G:)

4.57 GB free of

Public Terminal

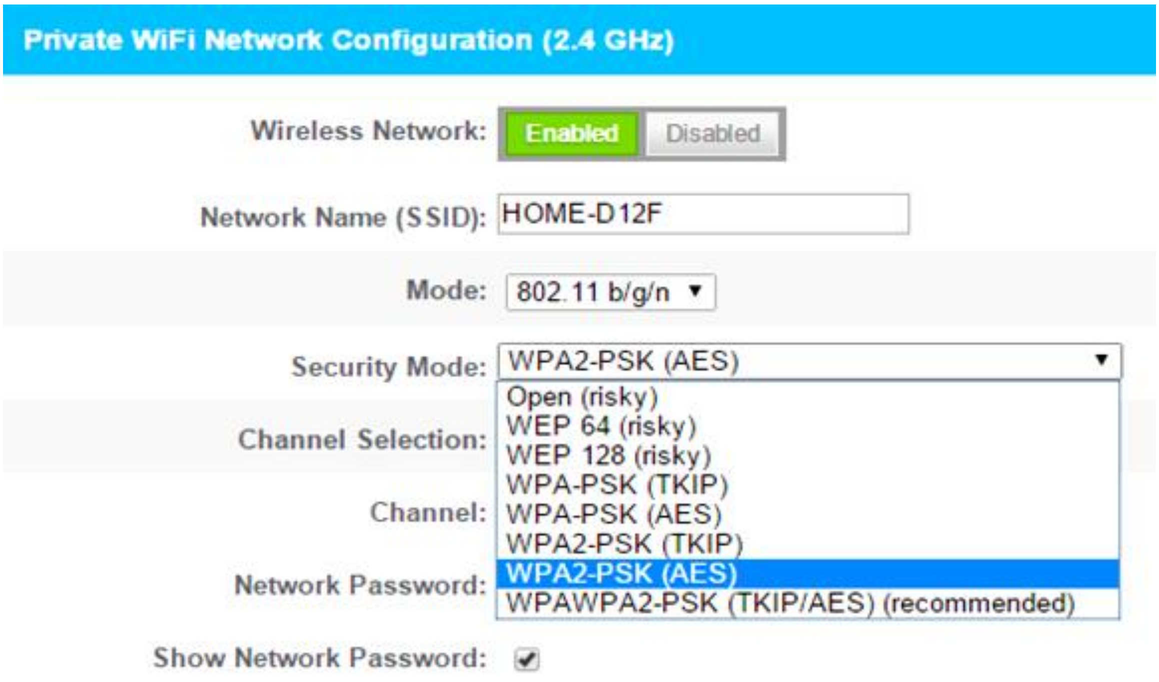
19. Don't let others watch over your shoulder while logging in or doing online transactions.

20. Don’t keep files open containing personal or confidential information on your desks.

Before you leave 1. Tidy your desk
2. Lock your screen
3. Put away sensitive documents

Wi-Fi Network

21. Always use WPA2 or higher encryption in wireless routers/devices.



Private WiFi Network Configuration (2.4 GHz)

Wireless Network: Enabled Disabled

Network Name (SSID): HOME-D12F

Mode: 802.11 b/g/n

Security Mode: WPA2-PSK (AES)

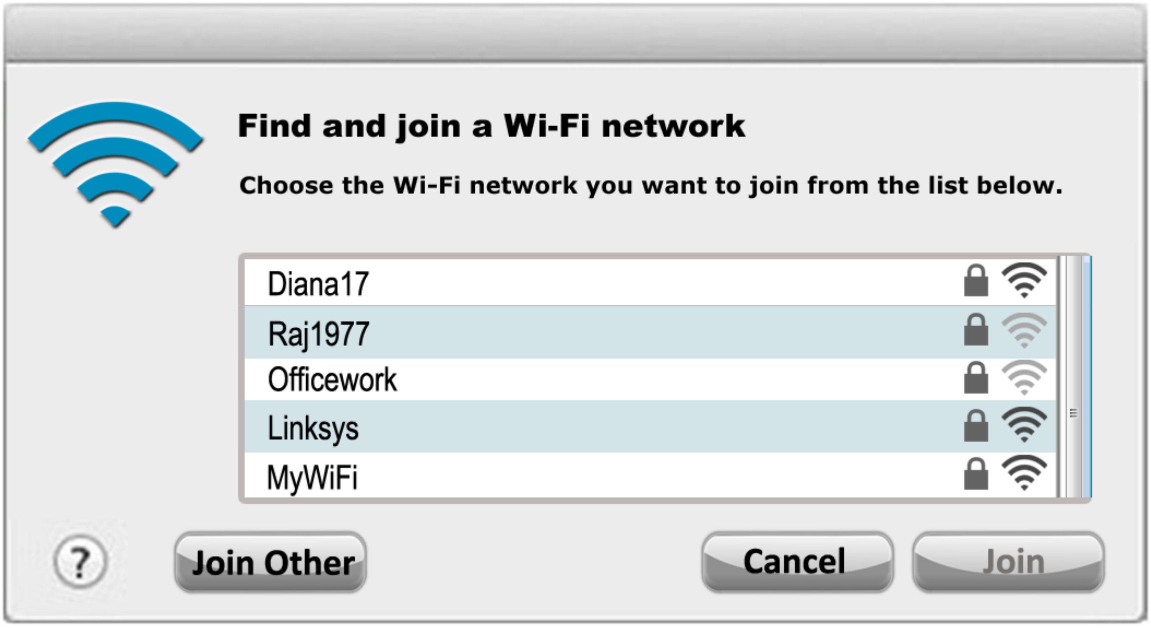
Channel Selection:

Channel:

Network Password:

Show Network Password: ☑

22. Don't disclose your identity, and change the default network device name /SSID (service set identifier) on regular basis.



Find and join a Wi-Fi network

Choose the Wi-Fi network you want to join from the list below.

Diana17

Raj1977

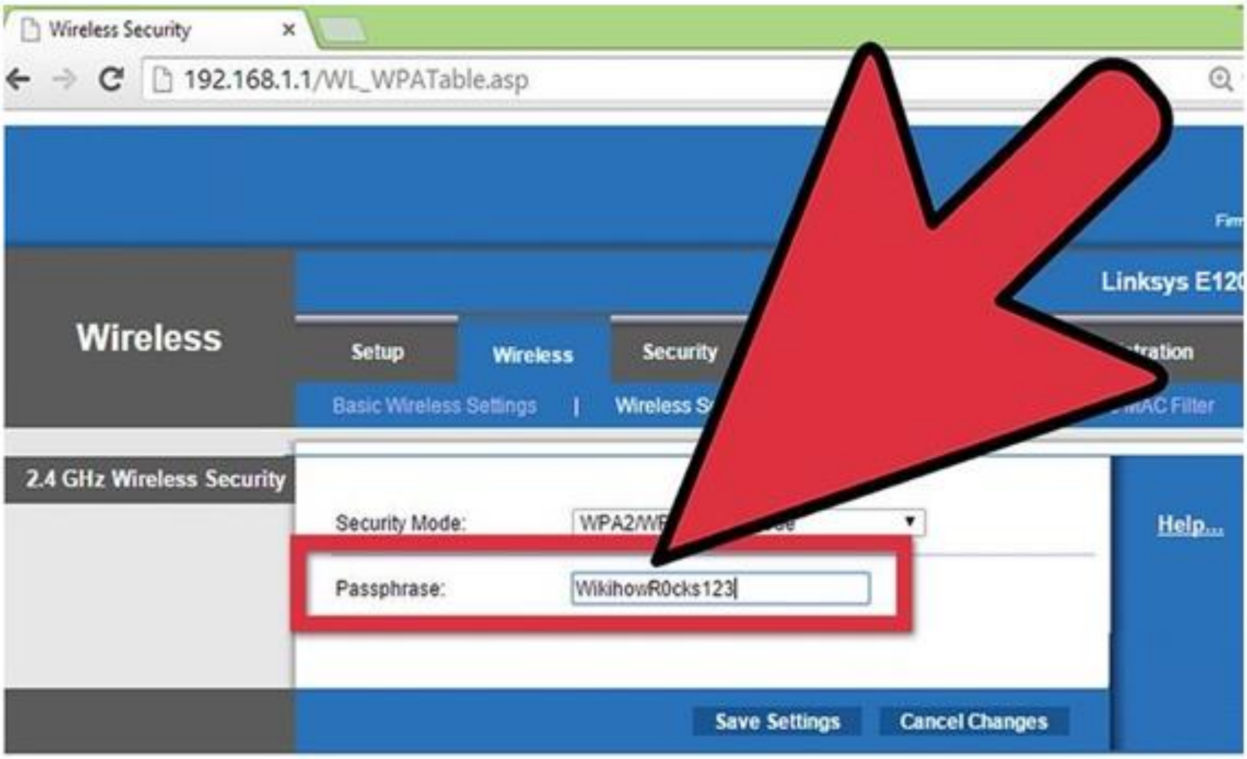
Officework

Linksys

MyWiFi

Wi-Fi Network

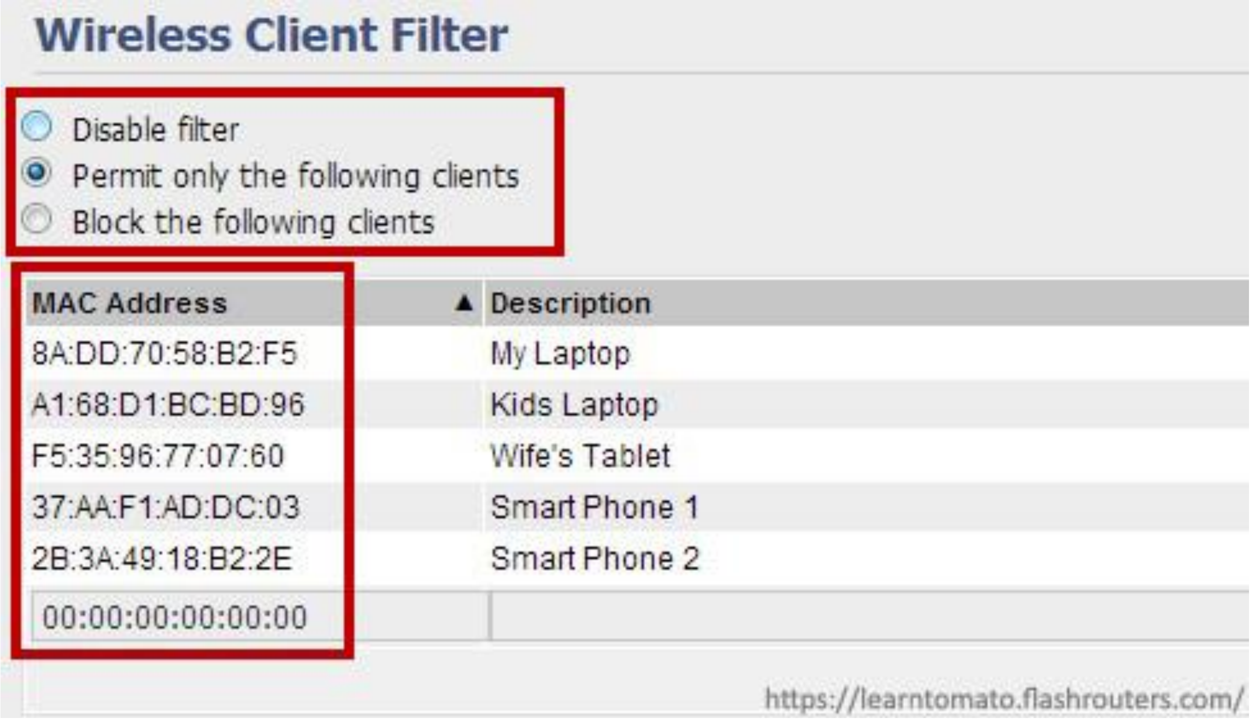
23. Change the default password of network device.



Security Mode: WPA2/WE

Passphrase: WikihowR0cks123

24. Activate MAC id filter to avoid unauthorized access.



Wireless Client Filter

○ Disable filter
● Permit only the following clients
○ Block the following clients

MAC Address ▲	Description
8A:DD:70:58:B2:F5	My Laptop
A1:68:D1:BC:BD:96	Kids Laptop
F5:35:96:77:07:60	Wife's Tablet
37:AA:F1:AD:DC:03	Smart Phone 1
2B:3A:49:18:B2:2E	Smart Phone 2
00:00:00:00:00:00	

https://learntomato.flashrouters.com/

Social Media Usage

25. All employees, contractual staff, consultants, partners, third party staff etc. working in Government offices or on Government projects **MUST NOT disclose official information on social media portals or applications.**

Preventing Social Engineering Attacks

26. Avoid disclosing/ sharing any official information on untrusted phone calls, meetings or email messages. Attackers often pose as genuine people to gain confidential official information to cause a data breach.

Preventing Social Engineering Attacks

27. Avoid phishing attacks – do not open untrusted emails. Do not open email attachments which do not seem relevant to any ongoing official communication. If any message or email conveys a sense of urgency and/or seems to apply high pressure sales tactics, be careful while opening or clicking on any link/ attachment.

28. Avoid vishing attacks – do not reveal any sensitive information over phone calls unless the source is completely verified and trusted. Ask for some information / verifiable credential, such as the name of immediate senior (if the caller poses as an official of another Government Department). Try to get a full assurance as to the identity of the caller prior to disclosing any vital information.

Preventing Social Engineering Attacks

29. Be careful of honey traps/ quid pro quo scams where attackers pose as genuine person and make a data theft attempt which seems like a fair communication.

30. Avoid phone calls/ emails/ SMS regarding unknown inheritance, foreign lottery, fund transfer requests from foreign country, etc. These are just examples of scams to get some money or information from you.

Some more domain specific usage awareness

General Computer Usage

1. Don't leave computer unattended with sensitive information on screen.
2. Always lock your computer when leaving it unattended with [windows + L] or [ctrl+alt+del]
3. Do not download unnecessary programs.
4. Avoid using public computers/ cyber cafes for office work.
5. All documents downloaded on public computers for any reason should be deleted with [Shift+Delete]

General Internet Browsing

6. Always use pre-installed or approved and updated web-browsers.
7. Do not store/share any information on any system that is connected to Internet.
8. Don't select the "Save password" option prompted by browser.
9. While browsing, avoid disabling the popup blocker/always turn ON the popup blocker in the browsers.
10. Don't perform any financial transaction by using public computers and public Wi-Fi connections.

Password Management

11. Create strong password with a minimum length of 10 characters using the combination of letters, numbers and special characters.
12. Use different passwords for different accounts. If one password gets hacked, your other accounts will not be compromised.
13. Change your password immediately if you suspect that it has been compromised.
14. Always decline the use of "Remember Password" option.

Removable Information Storage Media

15. Don't take removable media out of office without permission.
16. Erase/remove the contents of removable media after use.

Public Terminals

17. Don’t leave without closing all browsers and logging out from the public computers.

Wi-Fi Network

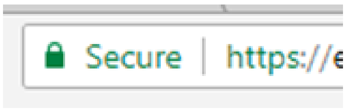
18. Regularly update the firmware of wireless device.
19. Disable remote management feature in routers to protect against unauthorized access.

Preventing Social Engineering Attacks

20. Do not click untrusted URL. Check the certificate validity of “https” icon before opening any link.
21 If any message or email conveys a sense of urgency or seems to apply high pressure sales tactics, be careful of opening or clicking on any link/ attachment.
22. Avoid phone calls/ emails/ sms regarding unknown inheritance, foreign lottery, fund transfer requests from foreign country, etc.
23. Immediately change your password if revealed to anyone for any purpose.

Preventing Social Engineering Attacks

24. Make sure that anti-virus is installed in your mobile/ computer.
25. Never disclose your mobile/net-banking credentials to anyone.
26. Always use very safe and un-guessable passwords containing letters, numbers and special characters.
27. Always make use of virtual key-pad for logging into your net-banking account.
28. For mobile banking – make sure you download only verified mobile banking application of your bank.
29. Do not set common PIN for mobile banking which can be easily guessed.
30. Be aware of phishing emails from unsolicited email addresses.
31. Make sure that the padlock “https” symbol is ”secure” and green - not amber or red in color.


Secure | https://e

32. Do not use public wi-fi for logging onto net-banking.

33. Do not use internet café or public computers for logging onto net banking.
34. On becoming aware of any fraud transaction, immediately report to bank through phone call and email.

Safe use of E-Mails

35. Do not share your e-mail login credentials with anyone.
36. While using public/ multi-user systems, make sure that you always log out before leaving the system.
37. Follow password best practices.
38. Always verify the sender not only through name but also through email address.
39. Do not click on any attachment or link if the e-mail address appears suspicious or un-trustworthy.
40. Do not click on any link which promises you of a lottery win or unclaimed inheritance.
41. Never share your credit or debit card details; or net-banking details with anyone through e-mail.

Safe use of Social Media

42. Always use only one social media account for each platform (ie, WhatsApp, Facebook, Twitter, Instagram, Google Plus, etc).
43. Do not share your login credentials with anyone.
44. Only add and communicate to real persons through social media platforms whom you know outside of social media.
45. Many of the social media profiles may actually be fake and created to extract information through social engineering.
46. Do not communicate any sensitive personal/ private information of yourself and others through social media messenger or chat services.
47. Be aware of attractive profiles of the opposite sex, they may be meant to lure you into divulging personal information – do not add and communicate such profiles without verification.

Propagation of fake news through social media

48. Social media platforms are continuously being used for the propagation of fake news and images.
49. Do not accept any image/ video or news received by social media to be true unless the genuineness has been verified by other sources.
50. Various un-desirable incidents of "public outrage" and "mob lynching" have happened due to the viral propagation of fake news through WhatsApp and Facebook.
51. Do not forward any controversial image/video/news without verifying its genuineness or you may be criminally liable.

Safe use of Credit and Debit cards

52. Do not share your credit/debit card number, CVV2 code or PIN with anyone.
53. When making online payments, make sure that the green padlock and "https" symbols are active and valid. Do not enter card details in any unverified website/ application or portal.
54. When using card in ATM or POS machines, ensure that the device where the card is being used has not been tampered with.
55. Always read and follow your banks' guidelines on using debit or credit cards.
56. On becoming aware of any fraud transaction, immediately report to bank through phone call and email.
57. Do not share your card PIN or CVV number with anyone, over telephone, email or any other means, even if someone says they are from bank call center.
58. Do not share any image of your card with anyone – do not store anywhere, as well.
59. Never write your card PIN in any piece of paper for a transaction – neither disclose to anyone ever anywhere.
60. In case of loss or theft of card immediately report to bank for blocking and file a complaint to police as early as possible.

Safe use of Laptops/mobile devices

61. Always use genuine vendor software and operating system.

61. Always use password protection for your laptop/ mobile device.
62. Always use licensed anti-virus software.
63. Do not download any software from untrusted sources.
64. Do not keep any applications or software which you do not regularly use.
65. Do not give your phone/ laptop for use to anyone, especially untrusted people.
66. Run virus scan your laptop/ mobile on a regular basis.
67. Make sure all vendor updates to the applications/ software you are using is getting updated on a regular basis.
68. Use of internet resources safely and in acceptable manner.
69. Always use trusted browsers like Google Chrome, Mozilla Firefox, Internet Explorer, etc. for web-browsing.
70. Do not visit any untrusted/illegal web-site.
71. Do not click on any unsolicited download links without verifying the content and source.
72. Always check for genuine "https" and green padlock to ensure that you are not being re-directed to a fake website.
73. Do not use torrents or download illegal content – it is a criminal offence.
74. Always ensure that you close and delete your browsing content when using public computers.

Cyber Crime related awareness

Cyber identity theft and cyber impersonation

What constitutes the crime and punishment involves –

75. Creating a fake account in someone else's name or misusing login credentials of someone else.
76. It is a crime under section 66C and 66D of the Information Technology Act, 2000.
77. Punishment for carrying out such a crime is 3 years in jail and fine up to Rs 1 lakh.

How to avoid (Public information) -

78. Follow password best practices.
79. Identify phishing emails and avoid phishing.
80. Use safe net-banking/mobile banking practices.
81. Make sure that Credit/ Debit card PINs are kept secret.
82. Use of social media in a safe manner.

Sending and publication of obscene or sexually explicit material

What constitutes the crime and punishment involves -

83. Is an offence under sections Section 67 and Section 67A of the Information Technology Act, 2000.
84. Under section 67, publishing or transmitting obscene material is liable to imprisonment of 3 years with fine up to Rs 5 Lakhs.
85. Under section 67 A, publishing or transmitting sexually explicit material is liable to imprisonment of 5 years with fine up to Rs 10 Lakhs.

How to avoid (Public information) -

86. Do not send anyone any defamatory, offensive or obscene messages which may cause any individual or group of people a negative impact
87. Do not transmit any sexually explicit material through WhatsApp group, messenger, etc.
88. Immediately delete such messages so that there is no scope of unintentional forwarding.
89. Follow safe browsing habits.

Violation of privacy through capturing, publishing and transmitting image of private area of a person without consent

90. Such an act constitutes a crime under section 66E of the Information Technology Act, 2000.
91. Punishable with 3 years of imprisonment and 2 lakh rupees of fine.

92. Child pornography – sexual abuse, creating video clip, publishing, transmitting or facilitating these in any way, of any person under 18 years of age, is a crime under section 67B of the Information Technology Act, 2000.
93. Section 67B stipulates 5 years imprisonment and 10 Lakhs rupees fine for first instance, which goes upto 7 years imprisonment and 10 Lakhs rupees fine for repeat offences.

How to avoid –

94. Do not capture yourself/or allow anyone else to capture your private images, using any electronic device.
95. Do not capture photo of anyone's physical private space.
96. Be aware of possible cameras in public spaces such as trial rooms of retail stores or malls.
97. Do not trust anyone – no matter how intimate the relationship is – to capture your private images/ videos.

<u>Cyber terrorism, threatening unity, integrity, security or sovereignty of India</u>

98. Cyber terrorism is an offence under section 66F of the Information Technology Act, 2000. It is punishable with imprisonment for life.
99. Cyber terrorism, as the name suggests, is any activity related to computer resources (including mobile phones), which:
    - may lead to the death or injuries to any person.
    - may lead to disruption of critical public services.
    - may lead to negatively affect the relationship of this country with any foreign state.
    - can harm national security or integrity or sovereignty

<u>Awareness plan for citizens</u>

100. Be vigilant for any cyber activity which may threaten the unity and integrity of the country and society.

Dos and Don’ts for Approvers and mid-level officers

1. All classified works should be done on standalone computers.
2. Take backup of all important information and files.
3. Do not enable remote access or file sharing from remote accounts.
4. Use secure deletion software for safe file purging.
5. Use private browsing mode on public computers.
6. Don’t store the information on private cloud services like Google drive, Dropbox, icloud etc.
7. Store information only on organization allocated removable storage media.
8. Always reboot when required to use public computers.
9. Clean up cache files after use.
10. Regularly update the firmware of wireless device.
11. Disable remote management feature in routers to protect against unauthorized access.

DOs and Don’ts for System & Network Administrators

1. Administrator login should be restricted through account management.
2. Update software patches regularly on all systems.
3. DON'T use the built-in Windows Administrator account for administrator functions/activities.
4. DON'T use generic/normal user accounts as service accounts.
5. DON'T reboot a system if:
    - you don't know who's logged onto it
    - you don't suspend the system monitors
6. Take regular backups of all critical systems.
7. Regularly check your log files for any errors and warnings, so they can alert you on problems before they become a threat.

8. Power supply should be controlled through UPS or Surge Protector.
9. Do not install computer systems in dusty environments.
10. Implement strong security protocols and policies.
11. Always enable the option in computers with "Show hidden file and folders".
12. Implement a workflow process with proper documentation.
13. All system changes should be only on the basis of documented approval.
14. Do not take up tasks which may not be completed on time - Beware the Late Friday Afternoon Task.
15. Do Perform Regular Security Audits and Tests.
16. Do Consistently Update and Patch Your Network and Devices.
17. Disable the Auto run/Auto play feature for insecure/downloaded software applications.
18. Create and Implement Policies and Procedures:
    - A Mobile Device Security Policy
    - A Computer Use Policy
    - A Social Media Policy
    - A Password Policy
    - An Email Policy
    - A Least Privilege Security Policy
    - A Business Continuity (BC) Plan, and
    - A Data Backup and Disaster Recovery (BDR) Plan.

19. Do remind Users to Use hard to guess and uncommon passwords.
20. Don't use Your Admin Account for non-admin purposes.
21. Don't leave Your Network at the Mercy of Password Protection.
22. Ensure that regular cyber-security updates are received by all employees.
23. Keep the anti-virus updated. Follow CERT-In and receive frequent bulletins about new exploits and hacker attacks.
24. Don't allow your e-mail programs to "auto open" attachments.

Remote Connection Scam

A new kind of scam has been going on that could result in looting the victim's entire bank balance by using remote connection methodswhich allow users to access a network or computer remotely via internet connection or telecommunication. The scam involves installing device controlling applications like AnyDesk, TeamViewer, etc. on the victims phone to gain remote access and get hold of OTP and other passwords.

Modus operandi:

- The fraudster will call the victims by impersonating himself as bank manager, company executive etc. and convince them to install remote connection applications by creating a false scenario like KYC expiration, Linking of bank account with phone number etc.

- Once the victim installs the application on their device, the scammer asks for the application ID and password for enabling the connection.

- On successful connection the fraudster will be able to see and control the victim's device.

- On gaining the access, the fraudster will monitor victim's actions and record information about banking application number, transaction pin, OTP, and other sensitive information and can use it for unauthorized transactions.

Precautions:

- Do not entertain calls asking you to install any remote-control applications.

- Make sure such applications are not running in background before performing any bank transactions.

- Do not share any banking information like account number to strangers.

- Any Desk or TeamViewer are not malware itself. They are just misused by fraudster to gather information from victim.

- Please report such incident without fear on **www.cybercrime.gov.in** and **www.reportphishing.in**

Cyber Safe Bengal – Cyber Safe India

* * *

Image courtesy :https://pixabay.com

Cyber Security Centre of Excellence
Webel Bhavan, Ground Floor
Block - EP & GP, Sector – V, Bidhannagar
Salt Lake, Kolkata – 700 091
Phone No.: 033 2357- 5218
Email :cscoe[at]wb[dot]gov[dot]in