Security tips when browsing online

You need to be careful when browsing online. You need to browse secure websites, only download from trusted sources, and use different passwords for every service.

While web hosting companies and domain registrars may set rules, that doesn't mean you can always browse the web safely. There are unscrupulous people out there trying to take advantage of you - infecting your system with viruses, stealing data, hacking your accounts, etc.

It is for that reason that you need to be careful when browsing online. You need to browse secure websites, only download from trusted sources, and use different passwords for every service.

To help you, TipsMake has put together this guide full of helpful tips to consider as you browse online. The article will cover advice on passwords, social networks, email, etc.

Useful security tips when browsing online

Password

1. Avoid obvious passwords that are easy to guess, like "123456".

2. Do not use a password that can be guessed based on personal information, such as date of birth.

3. Use a series of at least 4 unrelated words, as such passwords are harder to crack.

4. Also, mix special characters, uppercase and lowercase, with a minimum of 10 characters.

5. Ideally, use a password manager to create secure passwords and remember logins.

6. Use two-factor authentication to make it harder for others to access your account.

7. Never share a password with anyone, no matter who is asking for it.

8. Don't write down your password, or at least don't write it anywhere that can be easily seen by others.

9. Change your password regularly to avoid data leakage.

10. Never use the same password twice. Passwords should always be unique and unrelated.

Browsing

11. If you don't recognize a link, don't click it.

12. Check the address bar to make sure that you are visiting the website you intend to visit.

13. Does the site use a secure HTTPS connection? Otherwise, there is more risk of data theft.

14. Check the padlock icon in the address bar.

15. Avoid ads disguised as fake download links, if you're not sure, don't click.

16. The dark web is rife with scams and illegal activities, so avoid it.

17. Only download from trusted vendors and then scan the files with anti-virus software.

Social network

18. Everything you put online is permanent, so only share what you feel comfortable with.

19. Scrutinize all social media privacy settings to see what's public.

20. Never allow anyone else to use your social media accounts, nor log in on a public computer.

21. Social media is full of hoaxes and scams. Always be cautious!

22. Don't share too much information. You don't know who is viewing your information or what they will do with it.

23, Be careful with the information you will share. Are you sure you should share pictures of your children?

Virus removal

24. All systems are vulnerable to viruses, but some systems are more susceptible than others.

25. You don't have to pay for anti-virus software. For example, Windows Security is a great, free integration option.

26. Avoid downloading and opening unknown email attachments, as viruses often spread this way.

27. Learn the difference between viruses, malware and keyloggers.

28. The most extreme, but effective way to clean viruses from the system is to completely delete everything.

Data

29. Encrypt private data and do not share encryption keys with anyone else.

30. Don't store sensitive data in the cloud, keep them completely disconnected from the web.

31. External hard drives can be easily stolen, so be careful what you store on them.

32. If you're done using a drive, learn how to securely erase the drive. Just deleting data is not enough.

33. If you bought a used computer, do a factory reset and erase everything.

34. Back up data (at least 3 copies), on two different media types and one hard copy.

Email

35. The sender of the email can be spoofed, so the email may not be from the intended sender.

36. You don't recognize the sender? You didn't expect that email? Don't open and delete that email.

37. If an email asking you to click a link or open an attachment seems suspicious, trust your instincts and delete it.

38. If you are asked to share sensitive information, do not do it. Banks, ISPs, Amazon, etc. will never ask for this information via email.

39. If someone is trying to create a sense of urgency, forcing you to do something, it could be a scam.

40. Long-lost loved one and want to leave you some money? It is fake. Please delete email!

41. The spam filter offers some protection, but it's not effective, so don't assume everything in your inbox is safe.

Software

42. Keep all software on your computer up to date to patch security holes and enjoy the latest features.

43. Install operating system updates as they appear, especially important security updates.

44. If you no longer need the software, uninstall it completely.

45. Do not install random browser extensions and only use browser extensions from trusted publishers.

Smartphone

46. ??When you install apps, check what permissions they ask for, beware of apps that ask for access to camera, microphone, and location.

47. Only install apps from authorized app stores, though you still have to be cautious.

48. Do not send and receive sensitive data over a public WiFi connection.

49. Protect your phone with a PIN, pattern, fingerprint, or some other kind of security.

50. Follow the same precautions you take on your computer, such as avoiding suspicious websites and downloads.

51. Hold on to your phone whenever possible. This also protects against SIM card swapping.

Protection against malware and phishing

You'll never be completely safe when browsing online - that's the nature of the web for anyone to accept - but you can greatly reduce your risk by browsing through trusted sites. Of course, following the tips above will help you be better protected.

One of the important things you need to watch out for online is malware and phishing. Be on the lookout, don't be fooled by scams!