How to Protect Yourself Online

#	TIP
Passwords	
1	Avoid obvious passwords that are easy to guess, like "123456."
2	Don't use passwords that can be guessed on your personal information, like date of birth.
3	Use a series of at least four unrelated words, since it's harder to crack.
4	Alternatively, mix special characters, upper and lowercase, and be a minimum of 10 characters.
5	Ideally, use a password manager to generate secure passwords and remember your logins.
6	Use two-factor authentication to make it more difficult for someone to access your account.
7	Never share your password with anyone, no matter who claims to be asking for it.
8	Don't write your passwords down; or at least not anywhere obviously accessible.
9	Change your passwords regularly to protect against data leaks.
10	Never use the same password twice; they should always be unique and unrelated.
Web browsing	
11	If you don't recognize a link, don't click on it.
12	Check the address bar to ensure you're on the website that you think you are.
13	Is the website using a secure HTTPS connection? If not, there's greater risk of data interception.
14	Check the lock icon in the address bar; is the website registered to who it should be?
15	Avoid adverts disguised as fake download links; if you're uncertain, don't click.
16	The dark web is full of scams and illegal activity, so avoid it.
17	Only download from trusted providers, and even then scan the files with anti-virus software.
Social media	
18	Everything you put online is permanent, so only share what you're comfortable with.
19	Thoroughly review all your social media privacy settings so you know what's public.
20	Never let anyone else use your social media account, nor log in on a public computer.
21	Social media is full of hoaxes and scams. Remain vigilant. If something sounds too good to be true, it probably is.
22	Do not overshare. You don't know who's looking at your information or what they're doing with it.
23	Only share information of those who have consented. Are you sure you should share pictures of your children?
Antivirus	
24	Every system is susceptible to viruses, but some more than others.
25	You don't need to pay for antivirus software. Windows Security is a great built-in option, for example.
26	Avoid dodgy downloads and opening unknown email attachments, since viruses are often spread this way.
27	Educate yourself on the difference between viruses, malware, and keyloggers.
28	The ultimate, nuclear way to clean a virus from your system is to completely wipe everything.
Data	
29	Encrypt private data and don't share the encryption key with anyone else.
30	Don't store sensitive data in the cloud; keep it entirely disconnected from the web.
31	External drives can easily be physically stolen, so be cautious about what you store on them.
32	If you're done with a drive, investigate how to securely wipe one; simply deleting the data isn't enough.
33	If you buy a used computer, factory reset it and wipe it completely from top to bottom.
34	Back up your data: at least three copies, on two different types of media, with one off-site

Email	
35	The email sender can be spoofed, so that email might not be from who it claims to be.
36	Don't recognize the sender? Not expecting that email? Don't open it and delete it.
37	If an email asks you to click a link or open an attachment that seems suspicious, trust your instincts and delete it.
38	If you're being asked to share sensitive information, don't do it. Your bank, ISP, Amazon, and so on will never ask via email.
39	If someone is trying to impose a sense of urgency for you to do something, it's probably a scam.
40	That long-lost relative who has died and wants to leave you a bundle of money? It's fake. Delete the email.
41	Your spam filter offers some protection, but it isn't foolproof, so don't assume everything in your inbox is safe.
Software	
42	Keep all the software on your computer up-to-date, to patch vulnerabilities and enjoy the latest features.
43	Install operating system updates as they come through, especially critical security ones.
44	If you no longer need software, uninstall it completely.
45	Don't install random browser extensions, and only use those from trusted publishers.
Smartphones	
46	When you install apps, check what permissions they ask for; be wary of camera, microphone, and location access.
47	Only install apps from the authorized app stores, though even then you have to be cautious.
48	Don't send and receive sensitive data over public Wi-Fi connections.
49	Protect your phone with a PIN, pattern, fingerprint, or some type of security lock.
50	Follow the same precautions you do on your computer, like avoiding dodgy sites and downloads.
51	Keep your phone on you whenever possible; this also protects against SIM card swapping.