Computer and Internet Survival Guide

February 15, 2026 – #computerclub

Trilogy at Vistancia - Technology Q&A

Buying and upgrading

1. Buy quality equipment from reputable companies with good support and a real market presence.
2. Buy a bit more memory and storage than you think you will ever need to extend your computer's useful life.
3. When your computer can no longer run a current, supported operating system, start planning an upgrade.
4. Keep your operating system and apps up to date (you can delay big updates a week or two if you worry about stability).
5. Avoid "too good to be true" free offers on hardware and software; they often come with tracking, ads, or poor security.

Security basics

6. Your behavior is more important than paid antivirus. Windows and macOS already include pretty good built-in protection.
7. On Windows, the built-in Microsoft Defender is usually enough; extra paid antivirus is often unnecessary for careful users.[cite:28]
8. Never open unexpected or suspicious links in texts or emails. Never.
9. Do not install apps you don't need, and uninstall apps you don't use. Fewer apps means fewer problems.
10. Each person using a shared computer should have their own account. Do not share accounts.
11. The first step in troubleshooting is almost always: reboot.

Home network and router

12. Consider replacing your router about every 5 years, or sooner if it no longer receives security updates.[cite:14][cite:28]
13. Change the default admin password and WiFi password on your router as soon as you set it up.[cite:28]
14. Disable remote management from the internet (WAN side) unless you truly need it; manage the router only from inside your home network.[cite:28][cite:14]
15. Do not buy a router that gives you no control over WiFi behavior; you should be able to separate 2.4 GHz and 5 GHz networks if needed for older or IoT devices.[cite:14]
16. Use ethernet instead of WiFi whenever it's convenient for non-portable devices (desktops, TVs, printers, NAS).
17. Consider using a VPN on public WiFi, especially on networks with no password. At home, a VPN is usually not necessary unless you have a specific privacy or location need.

Safer browsing and DNS

18. A good ad blocker can remove clutter and reduce data usage. Brave browser includes strong ad blocking by default.
19. Using a safer DNS service can help block malware and adult content:

- Quad9 (9.9.9.9) focuses on blocking known malicious sites and uses multiple threat-intelligence feeds.[cite:7][cite:21]
- Cloudflare "1.1.1.1 for Families" (1.1.1.3 and 1.0.0.3) offers options to block both malware and adult content.[cite:19][cite:12]

20. Your default DNS is usually your internet provider, but you can override it in your router or on each device.

Printing

21. Brother black-and-white laser printers are economical and have good, well-supported drivers.

22. Inkjet printers tend to clog in a dry climate unless they are used regularly.

Email, backups, and cloud

23. On Apple devices, iCloud Mail is a good default; on Windows and Android, Gmail is a good default.
24. Legacy providers such as AOL and Yahoo are fading; plan your exit. For Canadians, Rogers/Shaw email is not as robust as iCloud or Gmail.
25. Keep at least two separate backups of your important data; keep at least one backup offline to protect against ransomware.
26. Occasionally test restoring a few files from your backup so you know it actually works.
27. Cloud storage costs money but is usually worth it for automatic off-site backup of critical files and photos.

Learning and organization

28. Keep yourself up to date by watching YouTube “training” videos from reputable channels.
29. Organize your files and photos so that someone else could find things if they had to.
30. Keep records of software licenses and registrations in one safe place (digital or paper).

Passwords and accounts

31. Use 2-Factor Authentication (2FA) wherever you can, especially for email, banking, and your password manager.
32. Use whole-disk encryption on laptops in case they are lost or stolen; modern encryption doesn’t noticeably slow down current hardware.
33. Use a reputable password manager to store your passwords and generate strong ones; use exactly one manager so things don’t get scattered.
34. Bitwarden is a free, well-regarded password manager and works on most platforms.

35. Browser-saved passwords are convenient but are harder to move if you switch browsers or devices.
36. Make sure your spouse and executor can find your accounts and passwords. Many password managers can print a list—store it securely with your will.

Money and subscriptions

37. Use a restricted-use or virtual credit card (such as Privacy.com or bank-issued virtual cards) for automatic recurring charges when possible.

Social media and "free" services

38. Facebook, Twitter, and similar platforms can be bad for your time, mood, and attention. Take a walk, read a book, or take a nap instead.
39. "Free" invitation and messaging services (like Evite) often make money by putting you and your friends on marketing lists.

Home automation and cameras

40. Home automation systems are getting more reliable and can help with security, convenience, and energy savings.
41. Do not rely on automation alone for critical functions like basic lighting—always have a simple manual fallback.
42. Install outside cameras so they do not point at a neighbor's windows or private areas; respect privacy as you would want yours respected.