Antivirus & Security Software

Why antivirus software is needed: Viruses, spyware, ransomware and other "malware" are malicious programs that can steal data or damage your device. **Antivirus (AV)** software scans your computer for these threats and removes them. Modern operating systems have some built-in protections (for example, **Windows Defender** is included with Windows 10/11 and is enabled by default), but it's important to ensure you have **active antivirus protection** on your system.

Free vs. Paid antivirus: You can choose between free antivirus programs or paid security suites. Both will help catch viruses; the main differences are in features and support:

- **Free Antivirus:** Provides *basic protection* against common viruses and malware. It usually includes virus scanning, real-time protection, and automatic virus definition updates. This is often enough for many users. Examples: **Microsoft Defender** (built into Windows), **Avast Free Antivirus**, **AVG Free**, **Avira Free**, etc. Free AV is great at core security, but typically **lacks extra features** and may occasionally show you ads or prompts to upgrade.
- **Paid Antivirus/Security Suite:** Includes the basics plus *advanced features* such as a firewall, phishing protection for web browsing, sometimes a VPN (virtual private network) for privacy, password managers, identity theft monitoring, and parental controls. Paid suites also usually come with **24/7 customer support** if you run into issues. Examples: **Norton 360**, **McAfee Total Protection**, **Bitdefender Premium**, **Kaspersky**, **Trend Micro**, etc. These require an annual subscription, typically ranging from $20-$80 per year depending on features and number of devices.

Free vs. Paid Antivirus – What's the Difference?

Free Antivirus gives you basic virus and malware scanning, real-time protection, and automatic updates to catch new threats. This is sufficient for many people who just need essential security. However, free tools usually *don't include extras* like a firewall, identity protection, or tech support – and they might show upgrade ads.

Paid Antivirus Suites offer broader protection: they often add a firewall to block hackers, secure web browsing (anti-phishing), possibly a VPN for online privacy, password manager, and identity theft monitoring. They also come with customer support if you need help. You pay a yearly fee, but you're getting an all-in-one security bundle and peace of mind with those additional layers.

Choosing what's right for you: If you **only need basic protection**, using the built-in **Windows Defender** on Windows or a reputable free antivirus is fine. Just remember to

keep it updated (Windows Defender updates through Windows Update automatically, and other AVs will update themselves too). On a Mac, many people rely on the system's built-in security and safe browsing features; Macs have had fewer widespread viruses, but they are not immune – installing a free AV for Mac (like Avast or Bitdefender Free for Mac) can add assurance.

If you want **extra features** or are not very tech-savvy (and would value technical support), a paid suite from a well-known company might be worth it. For example, some suites include a one-click **"vulnerability scan"** that checks for missing updates or unsafe settings, which can be handy. They might also include **phone support** if you run into a virus you can't remove on your own.

No matter which you choose: **use only one antivirus program at a time.** Having multiple AV programs active can cause conflicts and slow your computer. It's okay to supplement your main antivirus with an occasional manual scan using another tool (for instance, running a Malwarebytes free scan once in a while), but don't try to run two full antivirus products in real-time concurrently.

Beware of fake antivirus alerts: Unfortunately, scammers often take advantage of people's fear of viruses by displaying **fake security warnings**. You might see a pop-up in your web browser that says something like " ⚠️ URGENT: Your computer is infected! Call this number now!" or it claims to be from Microsoft and prompts you to download a "cleanup" tool. These are **scare tactics (scams)** known as **"scareware"**. **Legitimate antivirus software will *never*** ask you to call a phone number for help, or demand immediate payment to fix a sudden problem. If you see a random virus alert in your browser, **do not click it** – it's usually a malicious ad. Close the browser tab or window. If it won't close, use Task Manager (on Windows) or Force Quit (on Mac) to exit the browser, or as the FBI advises, disconnect from the internet if a suspicious pop-up takes over your screen. Then run a scan with your actual antivirus program for peace of mind.

Similarly, if you ever get an **unsolicited phone call** claiming to be "tech support" (from Microsoft, Apple, etc.) saying your computer has a virus: hang up! **Real tech companies do not call customers out of the blue about viruses.** This is a common scam (more on that in the Scams section).

Stick to trusted brands: When installing security software, use known companies' products (Microsoft, NortonLifeLock, McAfee, Bitdefender, Kaspersky, Sophos, etc.) or reputable free ones. Avoid random "antivirus" ads or downloads from unknown websites. If in doubt, ask someone tech-savvy or check reviews from sources like PCMag or Consumer Reports.

Antivirus & Security Checklist:

- ☐ My computer has **antivirus software installed and active** (Windows Security or another trusted AV).
- ☐ I **ignore** unsolicited virus alerts or scary pop-ups – I only trust the alerts from my own AV program (everything else is likely a scam).
- ☐ I download security software or updates **only from official sources** (the company's website or app store, never from a random pop-up or link).