

3.1 Software and App Safety

Core Concepts: Minimize Your Exposure, Protect Your Data

Malware often disguises itself as legitimate software. A free game, a helpful utility, even a security tool can hide viruses, spyware, or ransomware. The software you install is one of the largest parts of your attack surface. Knowing what's safe to install, and what to avoid, is critical.

3.1.1 Understanding Software Risks

Every piece of software you install increases your attack surface; the number of ways someone could compromise your system. Even legitimate software can have security vulnerabilities that attackers exploit.

Common ways malicious software spreads:

- Fake versions of popular software on download sites
- "Free" versions of paid software (pirated/cracked)
- Browser extensions that promise useful features
- Mobile apps that look legitimate but aren't
- Software bundled with other installations
- Attachments in phishing emails

Think before you install. Every piece of software is a potential security risk. Ask yourself:

- Do I really need this?
- Is this from a trustworthy source?
- Have I checked reviews and permissions?
- What's the worst that could happen if this is malicious?

When in doubt, don't install it.

3.1.2 The Basics

- Never use pirated software

- Use official app stores
- Verify download sources
- Watch out for bundles
- Understand app permissions

Never Use Pirated Software

This cannot be emphasized enough: Pirated or "cracked" software is one of the most common ways to get infected with malware.

Why pirated software is dangerous:

- The crack/keygen itself is often malware
- No way to verify what's been modified in the software
- Can't receive security updates
- Often bundled with adware, spyware, or ransomware
- You have no recourse if something goes wrong

Alternatives to piracy:

- Use free, open-source alternatives (LibreOffice instead of Microsoft Office, GIMP instead of Photoshop)
- Use free versions or trials to see if you actually need the paid version
- Look for student discounts or educational licenses
- Use subscription services when available (often cheaper than buying outright)
- Wait for sales and discounts

Use Official App Stores Only

App stores vet software before allowing it in their store. While not perfect, this dramatically reduces your risk.

Mobile devices:

- iPhone/iPad: Apple App Store only
- Android: Google Play Store (avoid "sideloading" APK files unless you really know what you're doing)

Desktop computers:

- Windows: Microsoft Store or directly from the software maker's website
- Mac: Mac App Store or directly from the software maker's website
- Linux: Official repositories for your distribution (apt, yum, pacman, etc.) or directly from the software maker's website

Avoid:

- Download sites like download.com, softonic.com, or similar aggregators
- Torrent sites
- Warez or "cracked software" sites
- Pop-up ads claiming you need to download something
- Email attachments claiming to be software updates

Other potentially useful software sites (use these with caution):

- Homebrew: Package manager for Mac and Linux - <https://brew.sh/>
- Open Source Initiative: Non-profit org dedicated to open source collaboration - <https://opensource.org/>
- Github: Open source software repo - <https://github.com>

Verify Download Sources

When downloading directly from a website instead of an app store, make sure you're downloading from the official publisher

Steps to verify:

- Go directly to the software maker's website, don't use download buttons from search results or ads
- Check the URL carefully, is it the real company website?
- Look for HTTPS (padlock icon) in the address bar
- Avoid third-party download mirrors unless they're official (like SourceForge for open source)

Example: You want VLC media player. Search "VLC official download" and go to videolan.org (the real site), not vlc-player-download.com (fake).

Watch for Bundled Software

Some legitimate software tries to install additional programs during installation, toolbars, antivirus trials, browser plug-ins.

How to avoid unwanted software:

- Always choose "Custom" or "Advanced" installation, never "Express" or "Recommended"
- Read every screen during installation
- Uncheck boxes for additional software you don't want

- Watch for pre-checked boxes that make the default "Install toolbar" or "Change homepage"
- When in doubt, decline everything except the main program

Understand App Permissions

Permissions tell you what an app can access on your device. Always check permissions before installing.

Ask yourself: Does this make sense?

- Photo editing app wants camera access? Makes sense.
- Flashlight app wants contacts and location? Suspicious.
- Weather app wants location? Makes sense.
- Calculator app wants microphone access? Suspicious.

Permissions to be extra careful about:

- Contacts - access to everyone in your address book
- Location - where you are at all times
- Camera/Microphone - can record you without indication
- SMS/Phone - can read messages or make calls
- Storage - access to all your files
- Install other apps - can install malware

If permissions don't make sense for what the app does, don't install it.

3.1.3 Better Protection

- Review app permissions regularly
- Uninstall unused applications and software
- Keep software updated
- Be careful with browser extensions

Review App Permissions Regularly

Apps can request additional permissions after installation. Review these periodically:

On iPhone:

- Settings > Privacy & Security
- Check each category (Location, Contacts, Camera, etc.)

- Revoke access for apps that don't need it

On Android:

- Settings > Privacy > Permission manager
- Review each permission type
- Remove permissions from apps that don't need them

On Windows:

- Settings > Privacy & security
- Review Camera, Microphone, Location, and other permissions

On Mac:

- System Settings > Privacy & Security
- Review each category and remove unnecessary access

Do this review quarterly.

Uninstall Unused Apps and Software

Software you don't use is a security risk for no benefit. Every unused app is a potential vulnerability.

Monthly cleanup routine:

- Look through your installed apps
- If you haven't used it in 3 months, uninstall it
- You can always reinstall later if you need it
- Don't keep trial software after the trial expires

How to properly uninstall:

- Windows: Settings > Apps > Installed apps > Select app > Uninstall
- Mac: Open Applications folder, drag app to Trash, empty Trash
- Mobile: Press and hold app icon, select "Remove" or "Uninstall"

Don't just delete the icon or folder: Use the proper uninstall process to remove all components.

Keep Software Updated

Software updates fix security vulnerabilities. Delaying updates leaves you exposed to known exploits.

Enable automatic updates for:

- Operating system
- Web browsers
- Antivirus software
- Mobile apps
- Any software that handles sensitive data

For software without auto-update: Check for updates monthly. Most programs have a "Check for updates" option in their menu.

Be Careful with Browser Extensions

Browser extensions have access to everything you do in your browser, every website you visit, everything you type, all your passwords.

Extension safety rules:

- Install from the official browser store only (Chrome Web Store, Firefox Add-ons, etc.)
- Check the number of users - thousands or millions is better than dozens
- Read reviews, especially recent ones
- Only install extensions you truly need
- Review installed extensions quarterly and remove ones you don't use
- Be suspicious of extensions that were recently sold or changed developers

Red flags for extensions:

- Requests excessive permissions
- Very few users or reviews
- Recent reviews mention ads or changed behavior
- Poor grammar in description

3.1.4. Extra Credit

- Use a sandbox for unknown software

Use a Sandbox for Unknown Software

A sandbox is an isolated environment where you can run software without it affecting your main system. If the software is malicious, it's contained.

Sandbox options:

- Windows Sandbox (Windows 10/11 Pro): Built-in, creates a temporary isolated environment
- Virtual machines (VirtualBox, VMware): Run a complete separate OS
- Online sandboxes <https://hybrid-analysis.com> upload files for automated analysis

This is advanced but very effective for testing questionable software safely.

Revision #1

Created 2026-07-12 21:29:31 UTC by Chris Landis

Updated 2026-07-12 21:31:15 UTC by Chris Landis