Potentially unwanted program (PUP)

What are Potentially unwanted Programs (PUP)?

A **Potentially Unwanted Program (PUP)** or **Potentially Unwanted Application (PUA)** is software that a user may consider unnecessary, undesirable, or potentially harmful. The terms are commonly used by antivirus, endpoint security, and parental-control products as subjective classification criteria.

PUP's and PUA's are not necessarily classified as traditional malware. However, they may exhibit behaviors that compromise user privacy, reduce system security, degrade performance, or interfere with the normal operation of a computer.

Examples of potentially unwanted behavior

- Displaying intrusive or excessive advertisements (adware).
- Tracking a user's Internet activity or browsing habits and potentially sharing the collected information with advertisers (spyware).
- Injecting advertisements or other content into websites viewed by the user.
- Changing browser settings, search providers, or the default home page without clear consent.
- Installing additional software that the user did not explicitly request.
- Using premium SMS or other paid services that can result in unexpected charges.
- Installing components that weaken the security of the operating system or browser.

Software bundling

One common method of distributing PUP's and PUA's is known as **software bundling**. In this model, a user downloads a legitimate or desired application, but the installer also offers or installs additional software.

For example, a software developer may distribute an application through a third-party download site. That site may use a custom installer or wrapper that presents additional applications during installation. These applications may be unrelated to the software the user originally intended to install.

In some cases, the installer may provide a clear option to decline the additional software. In other cases, the opt-out mechanism may be difficult to find, misleading, preselected, or otherwise

designed to encourage the user to accept the installation. Such practices are commonly associated with *dark patterns* because they can undermine informed user choice.

Risks towards infrastructure security

Certain unwanted applications can modify system or browser settings, weaken security controls, or install components that make the system more vulnerable to attack.

A particularly serious example is the installation of an untrusted root certificate. Root certificates are part of the trust infrastructure used to establish secure HTTPS connections. If an unauthorized certificate is installed and trusted by the operating system or browser, it may potentially allow an attacker or malicious component to intercept encrypted communications without generating the security warnings that users would normally expect.

For this reason, security experts and government agencies have advised users to remove insecure or unauthorized root certificates when they are identified.

About third-party software download websites

Third-party software-download websites can be a significant source of bundled PUP's and PUA's. A download page may advertise legitimate software while providing an installer that has been modified to include additional applications.

Open-source software projects have frequently expressed concern about this practice because third-party distributors may modify or repackage their software without the project's knowledge or authorization.

The safest approach is generally to obtain software directly from the **official project website**, a reputable package manager, or an established application store whenever possible.

In focus

Users can reduce their exposure to potentially unwanted software by following measurable security practices:

- **Download software from official sources.** Prefer the application's official website, a trusted package manager, or a reputable app store.
- **Avoid unfamiliar download portals.** Third-party download sites may repackage legitimate applications with additional software.
- **Use custom or advanced installation options.** These options often reveal additional applications or configuration changes that may otherwise be hidden.
- **Read installation screens carefully.** Do not automatically click *Next*, *Accept*, or *Install* without reviewing what is being offered.
- **Decline unnecessary additional software.** Pay particular attention to preselected checkboxes and offers for browser extensions, system utilities, or security products.

- **Keep antivirus and endpoint protection enabled and up to date.** Security products can detect and block many known PUPs and PUAs.
- **Keep the operating system and applications updated.** Security updates help address vulnerabilities that unwanted software could otherwise exploit.
- **Review installed applications regularly.** Remove software that you do not recognize or no longer need.
- **Check browser extensions.** Remove extensions that were installed without your knowledge or that have unnecessary permissions.
- **Be cautious about security warnings.** Unexpected certificate warnings, browser changes, or requests to install certificates should be investigated rather than automatically accepted.
- **Review trusted root certificates when necessary.** If an unfamiliar certificate has been installed by unwanted software, consult the operating system or browser vendor's security guidance before removing it.
- **Use reputable package managers where available.** Package managers can provide a more controlled and verifiable method of installing software.
- **Do not rely solely on antivirus detection.** Some PUPs may not be malicious enough to trigger traditional malware classifications, so safe download and installation practices remain important.
- **Back up important data.** Maintaining reliable backups can help reduce the impact of unwanted or malicious software installations.

Training summary

PUP's and PUA's occupy a category between legitimate software and clearly malicious malware. While some may provide a legitimate function, their installation methods or behavior can create privacy, security, performance, or usability concerns.

Software bundling and deceptive installation practices are common ways for unwanted applications to reach users. Obtaining software from trusted sources, carefully reviewing installation options, maintaining updated security software, and regularly reviewing installed applications can significantly reduce the risk of unwanted software being installed.

About this article

- Written by Gary Phatt, a TheOpenRoad Support employee.
- Still need help? Please write to us in the comment section below or contact TheOpenRoad support.

TheOpenRoad™

Please rate your experience with this article today:

When you select a number, *1 being the lowest and 9 being the highest*; the page will refresh and your feedback will be submitted to TheOpenRoad.

1 2 3 4 5 6 7 8 9

Revision #2
Created 2026-10-07 06:18:02 UTC by Gary Phatt
Updated 2026-10-07 07:36:07 UTC by Gary Phatt