How to avoid PUPs

If your users are downloading software onto their computers, chances are they're unknowingly cluttering their machines with PUPs. A little user education could free up some time spent cleaning (not to mention computer resources).

Here's what they—and you—need to know about PUPs.

What is a PUP?

WHAT IT IS NOT:
a baby dog.

WHAT IT IS:
the acronym for Potentially Unwanted Programs.

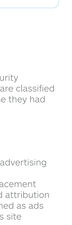
A PUP is a software program that users likely **didn't want** installed on their computers.

WHAT IT DOES:

- slows the computer down because of various background processes
- displays numerous annoying ads
- adds toolbars that steal space on the browser
- some collect private information

HOW YOUR USERS GET THEM:

PUPs often come bundled with software that users did, in fact, want. By swiftly clicking through an installation, it's easy to miss the fine print and "agree" to the extra applications.



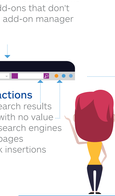
Types of PUPs include spyware, adware, and dialers.

PUPs are sometimes called bundleware, junkware, or PUAs (Potentially Unwanted Applications).

PUMs are Potentially Unwanted Modifications. These are unwanted changes made to a computer's default settings.

PUMs can be made by legitimate applications and malware, though changes made by malware are more likely to cause problems.

Your users probably don't even know the changes took place.



Backstory

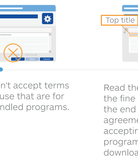
The makers of PUPs felt that since they included all the information necessary for consent in the download agreement, PUPs shouldn't be lumped in with spyware or other forms of malware.

DOWNLOAD

("Cause everyone reads download agreements, right?) Therefore, McAfee came up with the softer, less malicious-sounding term "Potentially Unwanted Programs."

PUP Criteria

In order to determine whether a program is a PUP, security engineers examine a list of bad behaviors. Some apps are classified as PUPs for having multiple infractions, others because they had one serious violation.

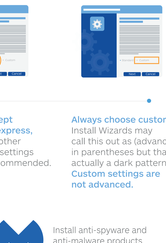


Advertising infractions

- Obtrusive or out-of-context advertising
- Pop-ups or pop-unders
- Ad insertion, overlay, or replacement
- Ads with no clearly identified attribution
- Ads that are not clearly defined as ads
- Redirection to a competitor's site

Download infractions

- Excessive shortcuts on desktop
- Bundling
- Pre-populated check boxes
- Liberal use of "recommended" next to an option
- No or difficult uninstall procedure
- Non-standard install locations
- Browser add-ons that don't show up in add-on manager



Web infractions

- Altered search results
- Toolbars with no value
- Hijacked search engines or home pages
- Bookmark insertions

Blacklisted programs

- Registry cleaners, optimizers, or defragmenters
- Driver optimizers or updaters

Tips to Avoid PUPs

Recognize dark patterns

Dark patterns are user interfaces that are deliberately designed to trick the user.

Look out for pre-populated check boxes (Software programs such as Unchecky scan third-party software agreements and uncheck options that result in PUPs, but they may not catch everything.)

Beware of those adding an unofficial "seal" as a credibility indicator.

Watch out for emphasis of a desired path (gray out the "skip" button, use bright color for "next" button).

Be wary of misdirection: Companies may try to hide free or cheaper options.

Read through EULAs carefully

Don't accept terms of use that are for bundled programs.

Read the top title above the fine print to be sure the end user license agreement (EULA) you are accepting is only for the program you originally downloaded.

If it isn't, you can decline and still move forward in the install process.

Read through Install Wizard instructions carefully

Read the information in the top navigation bar of the install Wizard to catch names of unwanted programs.

Do not accept standard, express, default, or other installation settings that are recommended.

Always choose custom. Install Wizards may call this out as (advanced) in parentheses but that's actually a dark pattern. Custom settings are not advanced.

Level up on security

Install an ad blocker/pop-up blocker

Install anti-spyware and anti-malware products

Learn more at malwarebytes.org/resources/

Malwarebytes