

# Adware

It displays ads on the screen automatically, usually within a web browser. It redirects search results to advertising websites and can collect user data to sell to advertisers without the user's knowledge. It is not always malware, as sometimes it is legitimate programs.

## How does it work?

It silently installs itself on end devices in order to be clicked on, whether accidentally or not. Creators and sellers make money through:

- Pay per click (PPC)
- Pay per view (PPV)
- Pay per install (PPI)

## Examples

### Fireball

It came to light in 2017 when an Israeli software company discovered that 250 million computers and a fifth of the world's corporate networks were infected with this adware. When it affects a device, it takes over the browser. It changes your homepage to a search engine, Trotus, inserts annoying ads on visited web pages, and does not allow you to modify browser settings.

### Appearch

This is a common adware program that acts as a browser hijacker. It is usually bundled with other free programs and inserts so many ads that navigating around the browser becomes a very difficult task. When you try to visit a website, Appearch.info opens instead. If you manage to open a web page, Appearch turns random blocks of text into links so that when you select a text, a pop-up window opens, inviting you to download software updates.