Adware: What is it & How to Prevent it

June 13, 2023

Spyware is harmful software. When installed on your device, it may send pop-up ads, redirect browsers to different websites, or secretly monitor user behavior. The hacker collects personal information, from your computer, without your consent, and sends the information to third parties to do damage or possible steal your identity.

5 Types of Spyware:

There are many different types of spyware – here are a few examples:

- Adware – displays unwanted advertisements (ads) on your device; often bundled with other software and may be difficult to remove
- Trojans – malicious programs disguised as legitimate software; once installed, may perform many harmful actions such as stealing personal information, or giving hackers remote access to your system
- Keyloggers – records everything you type on your keyboard; may include passwords or credit card numbers
- Password Stealers – designed to steal your login credentials; may capture passwords when you type them in or extract them from your device's memory
- Mobile Spyware – designed to target mobile devices and tablets; used to monitor calls, text messages, and location

Adware is the most common type of spyware; we will focus on this area below.

How does Adware work?

Adware, also known as advertisement-supported software, is created to show you ads forcibly, as a pop-up. The ads and offers you receive are based on websites you visit. The purpose is for creators and distributing vendors to make money through ads.

- Pay-per-click – paid each time you click on an ad
- Pay-per-view – paid each time ads are shown to you
- Pay-per-install – paid each time bundled software is installed on a computer

Adware quietly installs itself, onto your computer, through software. Search and browsing history may be tracked, to display ads targeted towards individuals. The hope is for you to click – accidentally or not – on the displayed ad and generate money for the developers.

Signs of Infection

If you experience any of the following symptoms, your computer may be infected with adware/spyware and/or another malicious program.

- Computer performs slower than normal and/or freezes/crashes
- Changes in your web browser homepage and/or search settings
- Difficulty loading the web browser
- Web pages do not display correctly
- Pop-up ads appear, even when you are not browsing the internet
- Internet speed is slower than normal
- Searches are redirected to sites you do not expect
- Ads appear out of context, or in places where you have not seen them in the past
- New extensions or toolbars appear on your browser
- New applications/icons appear on your computer

If you suspect your computer is infected, please take the following steps:

1. Disconnect your computer from the network
2. Disable the wireless connectivity
3. Contact the MCC Help Desk: (254) 299-8077 or helpdesk@mclennan.edu

Ways to Prevent Infection

Remember, adware is another way for cyber criminals to breach your company and cause financial or reputational harm. It is a scam, and you may be misled. To help prevent a possible infection, take the following steps:

- Keep your software up-to-date
- Turn on pop-up blocker in your browser
- Avoid free downloads, especially from questionable sources
- Avoid opening attachments/links sent via email, chat, or text unless you trust the source/sender
- Avoid clicking on pop-up window links or responding to questions in a pop-up window

Revision #2
Created 6 February 2025 21:31:35 by Laura J. Crapps
Updated 6 February 2025 21:49:50 by Laura J. Crapps