

Sample report. This is a real Digitech service report shared as an example. The client name, staff names and computer name have been changed.

Summary: The front office computer (OFFICE-PC2) had adware that hijacked Google Chrome. It changed the search engine to Yahoo, set unwanted pages (loanpride.com and meouhavebeent.com) to open whenever Chrome started, and inserted ads, coupon pop-ups and redirects into web pages. Digitech found where it came from, removed every piece of it and put Chrome back to normal. **The computer is clean and Chrome is working normally.**

What the Staff Were Seeing

- Searches going to **Yahoo ("Secure Search")** instead of Google, and no way to change it back.
- Two unfamiliar sites, `loanpride.com` and `meouhavebeent.com`, opening every time Chrome started.
- Extra ads, coupon/cash-back pop-ups and redirects while browsing.

What We Found

Item	Installed	What it did	Status
"Extension Optimizer" hidden browser add-on	June 2024	The main cause. A hidden startup entry made to look like Chrome loaded this add-on every time the user signed in. It didn't show up in Chrome's normal extension list. It redirected searches, inserted ads and coupon pop-ups, and reported which websites were visited back to the adware company.	Removed
OneBrowser unwanted web browser	Nov 2025	A copy of Chrome bundled with a free download, with a background updater that ran all the time. Bitdefender flagged it as a potentially unwanted application.	Removed
PDF_Spark "free PDF tool"	Nov 2025	Installed the same day as OneBrowser. This is a common way this kind of adware gets onto a computer.	Removed
McAfee WebAdvisor leftover add-on	–	Left behind after the old McAfee software was removed. It was the source of the "Secure Search (mcafee)" Yahoo search engine.	Removed & blocked
Chrome settings	–	The adware had deleted Chrome's built-in search engines, leaving only Yahoo, and had set loanpride.com and meouhavebeent.com as the startup pages and home page.	Restored

Was Any Information at Risk?

Digitech copied the add-on safely and examined its code in an isolated environment.

- It was built to **make money from ads and search traffic**. It swapped in affiliate links, showed coupon and pop-up ads, and redirected searches.
- It **did report browsing activity** (which sites and pages were visited, and search terms) to the adware company's servers.
- We found **no evidence that it captured passwords, form entries or payment card numbers**. The code has no functions for reading typed-in data.
- Google Chrome changed how add-ons can be loaded in mid-2025, which likely stopped the hidden add-on from working after that. OneBrowser appeared a few months later and appears to be the same kind of adware's replacement.

What Digitech Did

1. Checked the computer remotely and identified every adware component.
2. Backed up the user's Chrome settings and bookmarks before making any changes.

3. Removed the hidden add-on and its startup entry, OneBrowser (including its background updater), PDF_Spark, and the leftover McAfee WebAdvisor add-on.
4. Blocked McAfee WebAdvisor from reinstalling itself.
5. Cleared website sign-ins in Chrome so that any tracked browsing sessions ended. Saved passwords, bookmarks and history were **not** affected.
6. Set Google back as the search engine, removed the Yahoo "Secure Search" entry, and replaced the unwanted startup and home pages with the normal New Tab page.
7. Checked that every component was gone and that Chrome opens normally.
8. Reviewed the Bitdefender scan results. The client's Bitdefender protection settings are being reviewed so this type of unwanted software is removed automatically in the future.

Please note: signing back in to websites. As part of the Chrome cleanup, all website sign-ins were cleared. The first time you visit sites like Gmail, Facebook, online banking, etc., you'll need to sign in again. Your saved passwords were kept, so Chrome should offer to fill them in. Sites that use a verification code may ask for one again. This is a one-time step.

Note: Chrome syncs settings through your Google account, so the corrected search engine and startup settings will also carry over to other devices signed in to the same account. If Yahoo search or those pages ever come back on this computer or another device, let Digitech know and we'll track down where it's coming from.

Helpful Tips Going Forward

- Be cautious with "free" PDF converters, download managers, coupon tools and similar utilities. They are the most common source of this kind of adware.
- If a website says you need to install something to view or download a file, check with Digitech first.
- Some sites you trust may ask again for permission to show notifications or pop-ups.

Current Status

Check	Result
Hidden add-on and startup entry	Removed
OneBrowser and background updater	Removed
PDF_Spark	Removed
McAfee WebAdvisor	Removed and blocked
Default search engine	Google
Chrome startup / home page	New Tab page
Bitdefender protection	Active