**How Malicious Extensions Can Harm Users**

Malicious browser extensions are often disguised as useful tools (e.g., ad blockers, video downloaders), but they can be very dangerous. Here’s how they can affect your device and data:

* Stealing Sensitive Information

Some extensions request access to “read and change all your data on the websites you visit.” This allows them to capture:

* Login credentials
* Credit card numbers
* Personal messages
* Browsing habits
* Tracking and Surveillance

They can secretly track:

* The websites you visit
* How long you stay on pages
* What you search for
* This data can be sold to advertisers or even used for identity theft.
* Redirecting Traffic

Extensions can manipulate what you see by:

* Injecting fake ads
* Redirecting you to phishing sites
* Altering legitimate pages (e.g., adding fake login boxes)
* Installing Malware or Spyware

Some may download and install additional malicious files in the background without your permission.

* Cryptojacking

Certain extensions secretly use your computer’s resources to mine cryptocurrency, which slows down your system.

To avoid these risks:

* Always download from official stores (like Chrome Web Store or Firefox Add-ons).
* Read recent user reviews and check the developer’s credibility.
* Avoid extensions with vague descriptions or too many permissions.

Steps Taken and Extensions Removed:

Extensions Reviewed:

Reviewed 10 extensions including AdBlock, Grammarly, and Dark Reader.

Suspicious Findings:

One extension called 'Ad blocker' had very broad permissions and poor reviews.

Extensions Removed

Removed: Video Speed Booster Pro (unknown developer, required full data access).

Performance after Cleanup:

After removing unnecessary extensions, browser startup was noticeably faster and no unexpected pop-ups appeared.

Tools/Methods Used:

Used Chrome extension page (chrome://extensions/) and Chrome Web Store reviews for validation.