



MEGHALAYA
RURAL BANK
Scheduled Bank Owned by Government

Cybersecurity Digest

Bi-Weekly update by the O/o CISO of Meghalaya Rural Bank

Date : 01.07.2026

Volume 3 Issue 7

Bloatware



The joy of purchasing a new device is liberating. Now you can work, learn, and play faster — along with enjoying ample storage space. So, the last thing you'd expect is your appar-

ently safe device being exposed to vulnerabilities, or "bloat."

Exposure to unwanted software can derail its performance and hog its storage within a few months of usage.

Types of bloatware

- **Pre-installed software:** These are apps or programs installed by the manufacturer. While some may be useful, many are rarely needed and often cannot be easily removed.

- **Trialware:** These are trial versions of paid software, like antivirus programs, that come pre-installed. Once the trial ends, they prompt you to pay for the full version.

- **Adware:** This type of bloatware generates ads or pop-ups, slowing down your device and creating a poor user experience.

- **Toolbars and plugins:** Often installed during the setup of other software, toolbars and plugins clutter browsers and slow down performance.

Why is Bloatware a problem?

Bloatware can cause various issues, making it a nuisance for most users. Here are some of the main reasons why it's a problem:

- **Takes up storage space:** Many bloatware programs are large, eating up valuable storage space on your device. This limits the amount of data, photos, and useful apps you can have.

In technical terms, such pieces of software are referred to as bloatware. Bloatware has the potential to attack PCs with Microsoft systems and Android devices. It can also attack Apple iPhones and Macs although their systems tend to be built with a bit more protection.

Bloatware, also called Junkware or Potentially Unwanted Programs (PUP), are third-party programs that slow down the performance of your device

and lay it bare to cybersecurity risks. Manufacturers initially introduced bloatware to provide users with more utility, but the programs led to device issues. Software programs that identify as bloatware run in the background, and locating them is not child's play.

Bloatware finds its way into your device in two ways: it comes pre-installed or through programs downloaded from the internet.

or data.

Hard to remove: Many bloatware apps don't offer an easy way to uninstall them. In some cases, they're "baked" into the operating system and require advanced steps to remove.

Slows down devices: Bloatware often runs in the background, consuming system resources like memory (RAM) and CPU power. This slows down your device and affects its overall performance.

Annoying notifications and ads: Adware and trialware can bombard you with annoying pop-ups, notifications, and reminders to buy software or services.

Security risks: Some bloatware, especially outdated or unpatched programs, can create security vulnerabilities. Hackers can use these to access your device



How to detect bloatware

Identifying bloatware on your device can help you decide what to keep and what to remove. Here are some ways to detect it:

1. Check installed apps: Go through the list of installed apps and programs on your device. Look for apps you don't recognize or use. If you didn't install it yourself, it might be bloatware.

2. Monitor system performance: If your device has suddenly slowed down, check which programs are using the most resources (CPU, RAM, storage). Bloatware is often a big consumer of

resources.

3. Watch for pop-ups: Frequent pop-ups or prompts to buy software could indicate trialware or adware on your device.

3. Use a performance tool: Some antivirus or system monitoring tools can scan for and identify bloatware.

How to prevent bloatware

The best way to deal with bloatware is to prevent it from becoming a problem in the first place. Here's how you can do it:

1. Buy from trusted manufacturers

Some manufacturers are known for including lots of bloatware in their devices. Research

before buying and choose brands with fewer unnecessary pre-installed apps.

2. Perform a clean install of the operating system

On a PC, you can do a clean installation of Windows or other operating systems. This removes all pre-installed bloatware and gives you a clean slate.

3. Use "Debloat" software

There are tools available that can help identify and remove bloatware automatically. Tools like PC Decrapifier for Windows 10 Debloat can simplify the process.

4. Be careful when installing software

During software instal-

lations, many programs offer "optional" toolbars, plugins, or trialware. Always select the "custom installation" option to prevent these from being installed.

5. Uninstall apps you don't use

Regularly go through your list of apps and uninstall anything you don't use or need. For mobile devices, you can often disable apps you cannot uninstall.

6. Install a good antivirus program

A good antivirus program can detect and block adware and other bloatware. This helps prevent unwanted software from being installed without your knowledge.



How to remove bloatware

Removing bloatware can be challenging, especially if it doesn't offer a straightforward uninstall option. Here's a step-by-step guide to getting rid of it:

Step 1: Uninstall normally

- On Windows: Go to **Control Panel > Programs > Uninstall a Program** and select

the bloatware you want to remove.

- On Android: Go to **Settings > Apps** and tap on the app you want to uninstall. If it cannot be removed, you may be able to "disable" it instead.

Step 2: Use third-party tools

Tools like **CCleaner** or **IObit Uninstaller** can force uninstall stubborn programs that don't offer a regular uninstall option.

Step 3: Disable system apps

For apps that can't be uninstalled on mobile devices, go to **Settings > Apps** and select "disable." This prevents the app from running

or using resources.

Step 4: Edit the registry (Advanced users)

Warning: This is for advanced users only. Editing the Windows registry can remove deeply rooted bloatware, but it also comes with risks if done incorrectly.

Step 5: Root your de-

vice (mobile)

For Android users, rooting your device allows you to remove system apps that can't normally be uninstalled. However, this can void warranties and introduce security risks, so proceed with caution.

Ensure to use different passwords for different accounts

