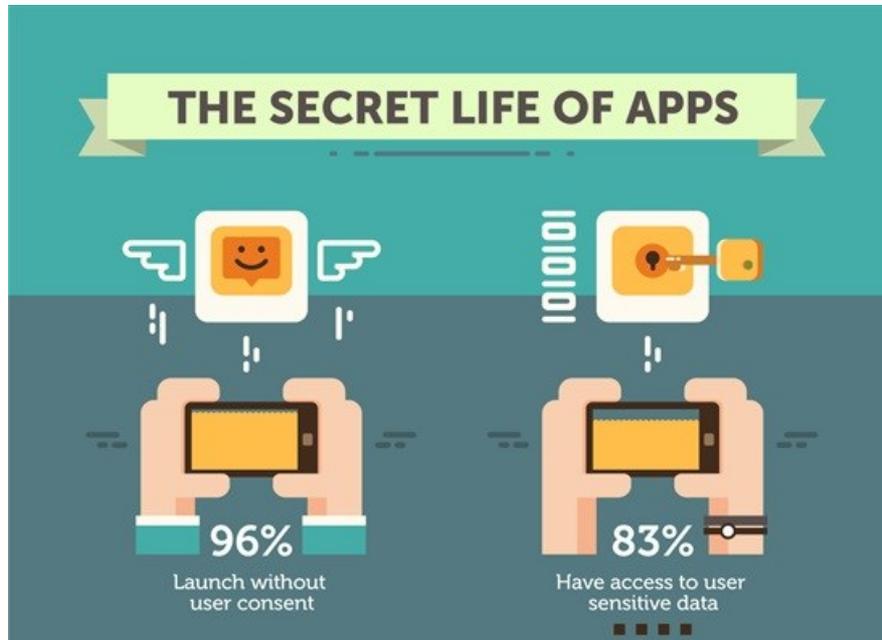


# Digital clutter makes you vulnerable to security threats

Digital clutter is growing due to an explosion in application usage and advances in the storage capacity of devices. But poor maintenance of these apps is leaving devices vulnerable to security threats. A new report by Kaspersky Lab reveals the scale of the digital clutter problem among internet users worldwide.



[click to enlarge](#)

The study found that users typically install 12 Android apps every month but delete only 10, in effect adding two apps to their device on a monthly basis. With more apps installed on devices, managing apps is important in preventing digital clutter. However, we found that in only half (55%) of cases users regularly refresh and revise the contents of their device and delete unused docs and apps.

The findings are part of a new report compiled by Kaspersky Lab called *Digital clutter and its dangers*. The study is based on insight gained from a unique combination of an online survey across 17 countries, statistical analysis from the Kaspersky Security Network (KSN) and an experiment into app performance by Kaspersky Lab internal testers.

## 28 % only update when forced

The build-up of digital clutter means that app cleansing and updating are now more important than ever in order to combat malware that use apps' vulnerabilities to penetrate devices. But the survey found that in a quarter of cases (28%) users only update apps on their devices when they are forced to, and in 10% of cases, they try not to do it at all.

One of the main dangers is that the apps themselves can put user data and devices at risk due to their everyday activity. Technical findings from Kaspersky Lab show that of 100 Android apps users can manage (i.e. install and delete), 83 have access to sensitive user data, such as contacts, messages and data, and can even make calls and send SMSs.

## Apps can operate without permission

Additional findings from KSN show how apps can operate without user permission. On average users have 66 apps on their Android device. When a representative sample of 66 of the most popular Android apps were tested, 54 launched in the background without users even touching them, consuming, on average, 22MB traffic per day without any user interaction.

App settings give users a degree of control over what the app can access and interact with on the device. However, the survey found that only 40% of people intentionally adjust the settings of each application on their smartphone. Furthermore, only 32% can refuse to install a mobile app if they are not satisfied with the content of license agreements.

Andrei Mochola, head of consumer business at Kaspersky Lab says: "Users are exposing devices and personal data to security threats by failing to undertake simple but essential care for their device that cleans and updates software and apps, adjusts settings, and uninstalls apps that are no longer used.

"The build-up of digital clutter on our devices means that we increasingly overlook the maintenance of these apps. But we do so at our peril because this can lead to a wide range of problems such as device glitches, battery life issues or malware infection. Apps have access to some of the most sensitive and personal data we have on our devices and users are often unaware this information is being shared. We urge users to put their digital houses in order. Just like a clean, uncluttered room breathes fresh energy into your home and life, in the same way, an uncluttered computer or smartphone results in a more enjoyable, and a crucially, safer experience."

## **Combat the digital clutter**

In order to combat the clutter and protect your personal data, users are advised to take the following steps:

- Understand what's stored where: take some time to go through your devices and work out what information is stored on which apps and files on your device;
- 'Spring clean' your device: spend some time to get your digital house in order by regularly clearing out and refreshing the information stored on your devices;
- App and software updates software: regular updates should be undertaken as soon as new versions are released;
- Use dedicated software: For example, software cleaners such as the one integrated into Kaspersky Lab's flagship security solutions, scan all applications installed on your device and mark those posing potential risk or are rarely used.

For more, visit: <https://www.bizcommunity.com>