Smartwatches and the security of our physical performance data.

Candela Zurita

Smart watches have become an essential tool for anyone who wants to keep track of their daily physical activity. To this end, these devices collect information on heart rate, movement, and even the level of oxygen in the blood of their users through their different sensors. However, despite the advantages that these technologies bring to the development of an active and healthy life, they also create new and greater risks for the protection of our personal data. Transparency, awareness and technical security must be essential in the use of these devices.

Sneakers, keys and "start". Thousands of people repeat these steps every day, and smartwatches are increasingly becoming part of our sports routine.

Far from just telling the time, these devices allow us to track our daily physical activity, from counting how many steps we take per hour to recording our heart rate. They have therefore become essential for everyone looking to monitor their exercise habits.
In 2021, the smartwatch market recorded around 102.5 million units sold and statistics forecast that sales will surpass 200 million units worldwide by 2027.

The ability of smartwatches to connect with other devices and tools allows all the data to be fed into different applications that generate, among others, statistics and metrics on our daily performance.

These devices belong to what is known as the Internet of Things, IoT for short, which is the process that enables the connection of everyday physical objects to the Internet. The development of 5G and the consequent Internet of Things make it easier for digital devices such as smart watches to collect our data through their different sensors and send it to other devices or applications. The devices themselves are developed thanks to these technologies and allow more and more sophisticated tools to be developed that can respond to the different needs of their users.

However, despite the advantages that the use of these devices can bring to maintain an active and healthy life, the development of these tools also generates new and greater attacks on our personal intimate sphere.

In the case of the use of smart watches during our sports routines, the main problem in terms of privacy refers to the amount and sensitivity of the data collected, in particular, health and location data. In addition to this, there is a loss of control over the privacy of our personal data due to the lack of information provided by the manufacturers of the devices or the owners of the sports performance applications, as well as the possible violations to which our personal information is exposed, especially in relation to the transfer of data to third party applications.

If we do a quick search to find the best sports performance measurement apps, Strava's name immediately pops up.

Far from just telling the time, these devices allow us to track our daily physical activity, from counting how many steps we take per hour to recording our heart rate.

Strava is an app that is compatible with a number of GPS devices that track heart rate data, including smartwatches from Garmin, Fitbit, Apple Watch, Polar and Suunto. The app is focused on athletes and, according to its own website, is used by more than 100 million people spread across 195 countries and allows its users to measure their progress, record the calories they consume in each activity and share their results with the rest of the users.

The application has a global heat map that collects the most frequent locations for training of its users, i.e., it allows users to mark their physical activity, provide others with the most common routes and compare their times, which becomes an incentive to improve their records.

Strava's heat map records are anonymous, however, a study by North Carolina State University has revealed that, by cross-referencing data with public personal data from Strava profiles, the home address of some of the app's users can be revealed.

This is not the first time that its heat map has exposed unexpected data, in November 2017 the publication of the heat map containing more than three trillion GPS data points allowed to unveil military bases and secret facilities of the armies of several countries.

Given the sensitivity of the data collected through these devices it is alarming that unauthorized persons can access this data, but special care must also be taken regarding the use made by authorized third parties of this personal information.

Therefore, in order to ensure the protection of personal data, it is essential that all data controllers involved in the data lifecycle have an adequate basis of legitimacy for their processing, both for the collection of data by the watches and for their storage and communication to third parties. As well as, a strict compliance with its duty of transparency, which involves transferring to the user at the time their data is collected information about the processing of their personal information and the circumstances in which it is processed, distinguishing whether they have been obtained directly from the person concerned or not.

However, despite the advantages that the use of these devices can bring to maintain an active and healthy life, the development of these tools also generates new and greater attacks on our personal intimate sphere.

The privacy of the data processed on these devices depends largely on the robustness of their security. Smartwatches are subject to similar risks as other IoT devices, so their main risk is their connected technology.

Applications linked to smartwatches are one of the main avenues of attack, since, regardless of the levels of security that the device can guarantee, the

applications may contain vulnerabilities in their programming that can expose user data. There are also malicious applications that simulate other legitimate applications so that the user, trusting that it is a legitimate application, provides his personal information directly. Similarly, a weak authentication method or encryption is a way of accessing personal information shared with the device.

Smartwatches are subject to similar risks as other Iot devices, so their main risk is their connected technology.

In line with this last point, when connecting a smartwatch with other devices via Bluetooth technologies, it has been found that there are vulnerabilities in data encryption that allow connections to be brute-forced and tapped.

Therefore, the various suppliers and developers of these devices should endeavor to implement sufficient technical measures to mitigate the risk to which their users are exposed. Likewise, users of these devices must be aware of the sensitivity of the information they share with these devices (health data, location data, passwords, messages, etc.), the misuse of which could have a major impact on their rights and freedoms.

Despite the many vulnerabilities found in these devices, not all of them depend directly on their technical configuration and programming and users can become aware and implement the following measures to avoid exposing themselves to unnecessary risks:

- Configure device security and block connections and/or to unauthorized pairings.
- Set up two-factor authentication.
- Use only official applications.
- Update the device and the various applications to their latest versions.
- Use a virtual private network (VPN) connection.
- Set a PIN code or unlock password.
- Scan only QRs and codes from trusted sites located in a real environment and ensure that browsing standards are secure.