Can smartwatches be hacked?

Many of us do what we can to protect our computers from cybercriminals, but we often don't realize that our phones and smartwatches are also at risk.

While smartwatches are like an accessory to our main devices, they can still be exploited by the bad guys. So how easy is it to hack a smartwatch and what can you do to protect yourself?

Why hack a smartwatch?

Smart watches can store many different types of data, some of which are very sensitive. Phone numbers, email addresses, login information, and payment information can all be stored on a smartwatch, and hackers can do a lot if they succeed in stealing these information.

There may not be as much data stored on a smartwatch as on a computer or smartphone, but that doesn't mean there isn't anything worth pursuing for malicious actors. Even a single phone number or set of credentials can expose hackers to a variety of things, so don't assume that just because your smartwatch is a trivial accessory it's not compromised by hackers. hunting attack.

Smartwatches are almost always connected to smartphones, and this direct link also makes them a target for hackers. Since cybercriminals can intercept information exchanged between smartphones and smartwatches, it's easy to see why smartwatches are such a lucrative prey.

How are smartwatches hacked?

Picture 1 of Can smartwatches be hacked?

Smart watches can be thought of as mini computers. With a smartwatch, you can connect to the Internet, use Bluetooth and NFC, make calls, and send text messages. So it is clear that there are many wireless communication vectors that are supported by most smartwatches.

Therefore, smart watches are vulnerable to remote attacks. There are so many forms of remote attack that listing them all would take a long time. However, there are some main forms of attack that smartwatches are particularly vulnerable to.

Phishing is a type of cybercriminal that exploits many different types of communication channels, including email, SMS, and social media direct messages. Phishing attacks involve impersonating an official person or organization to spread malware or steal data. If you receive a phishing email and open it on your smartwatch, you are at risk.

For example, let's say you open a phishing email attachment on your smartwatch and accidentally deploy malware on your device. Once this malware is installed and active, it can record your activity, steal data and even track your location. Even ransomware, an extremely dangerous form of malware, has been known to infect smartwatches and email phishing can be used to deploy such harmful programs.

In addition, using Bluetooth on a smartwatch can be risky. Bluetooth is a short-range wireless connection technology used by many people to pair with other devices, such as wireless headphones and speakers. In the case of smartwatches, Bluetooth can be used to connect to your smartphone, so you can make and receive calls, use apps, and access more features in general. .

However, when Bluetooth is used to connect your smartphone and smartwatch, another channel opens up for hackers to exploit. Cybercriminals can compromise your connection, then eavesdrop on data sent between both devices.

Cybercriminals can also use factory default passwords to access smartwatches. Default passwords are provided to Internet of Things (IoT) devices during production. If cybercriminals can find your original default password, they can access your smartwatch through the backend. While you can change this password, it is often quite difficult to do and many people don't mind, which leaves a useful exploitation channel for hackers.

How to keep your smartwatch safe from hackers

Picture 2 of Can smartwatches be hacked?

If you're concerned about your smartwatch posing a security risk, there are a few things you can do to keep your watch safe from hackers, starting with the connections you make.

As discussed previously, there are various communication channels that a smartwatch can use, including WiFi, Bluetooth, and NFC. All of these have the potential to be exploited by an attacker, so it's wise to only keep the connections you need enabled. For example, if you don't need NFC on a certain day, turn off NFC until you need to use it again.

Also, try not to connect your smartwatch to too many devices at once, as this can also expose you to malicious attacks. For example, if cybercriminals successfully hack a smartphone, they can gain access to your smartwatch.

Connecting your smartwatch to a public WiFi network can also make you an easy target for hackers. This is a general rule for all devices, including laptops, tablets, and smartphones. If you don't use a protective protocol, such as a Virtual Private Network (VPN), connecting to a public WiFi network puts you at risk of data theft or being tracked by cybercriminals.

Updating your smartwatch's software, especially the operating system, can also play an important role in improving security. Software updates offer many benefits, one of which is to eliminate bugs and vulnerabilities that can pose a security risk. While it can be a bit inconvenient to wait for software updates to finish, they are still very important, so try to run updates as often as possible.

You should also physically protect your smartwatch from attacks. Malware can be installed directly on a smartwatch if someone has access to it, so it's important to equip your smartwatch with a strong password. so that the smart watch cannot be easily hacked.

Finally, it's important to choose legitimate and trusted smartwatch manufacturers to know that you won't be left without any security measures on your device. Cheap smartphone brands can sometimes forgo certain features, including security protocols, in order to offer their devices at a lower price point. While this isn't always the case, it's usually safer to choose a brand that has a good name, good reviews, and reputation.