

# What is Bluetooth? Useful information about Bluetooth technology

Many devices today incorporate Bluetooth technology to enable wireless communication with other Bluetooth devices. Before using Bluetooth, it is important to understand what this technology is and the security risks that may come with it, as well as how to avoid or protect yourself from these risks.

Bluetooth technology is built into many devices such as laptops and phones, allowing wireless data transfer from one Bluetooth device to another. Before using Bluetooth, we should learn what Bluetooth is and the security risks that may occur with it, as well as measures to avoid or protect yourself from these risks.

## What is Bluetooth?

Bluetooth is a radio frequency-based wireless technology that allows devices to communicate with each other without cables and wires. Bluetooth supports data transfer rates of up to 720 Kbps within a range of 10 m to 100 m.

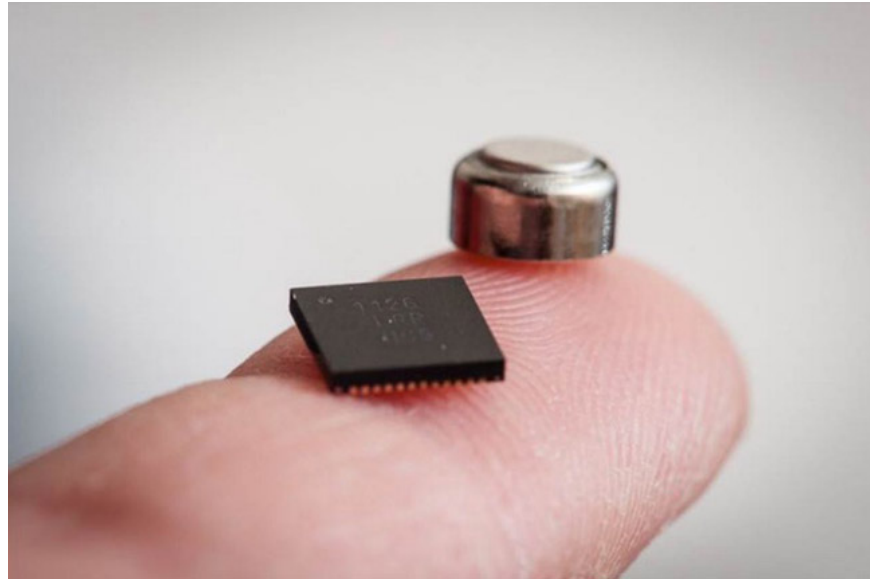
Since Bluetooth is also an electronics standard, manufacturers who want to include Bluetooth in their products must comply with the requirements of the standard. These technical standards ensure that devices can recognize and interact with each other when using Bluetooth technology.

Nowadays, there are many electronic devices that have built-in Bluetooth technology such as laptops, tablets, phones, headphones, speakers, smart watches, mice, keyboards. Thanks to Bluetooth, data transmission, synchronization, and music listening have become easier, still ensuring quality while reducing the number of connection cables.

For example, you can use a wireless keyboard, wireless mouse with your laptop, listen to music with Bluetooth headphones without having to worry about messy wires on the table.

## 6 things you didn't know about Bluetooth

### 1. Bluetooth is a wireless technology standard

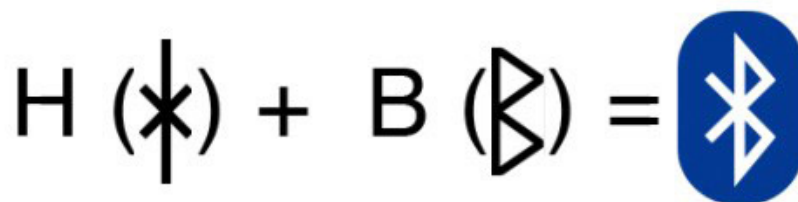


Wireless technology standards require both hardware and software. The hardware is required to be able to send the necessary signals over radio frequencies, while the software determines what is sent over that signal and how it is interpreted.

This means that, in order to use Bluetooth, a device must have a small computer chip with a Bluetooth radio. This also means that the software must be widely accepted across all devices (aka 'standard'), otherwise they won't be able to connect.

The standard is managed by the Bluetooth Special Interest Group (SIG), but the Bluetooth SIG did not choose this name, it was proposed by Jim Kardach in 1997.

## 2. Bluetooth is named after a Viking

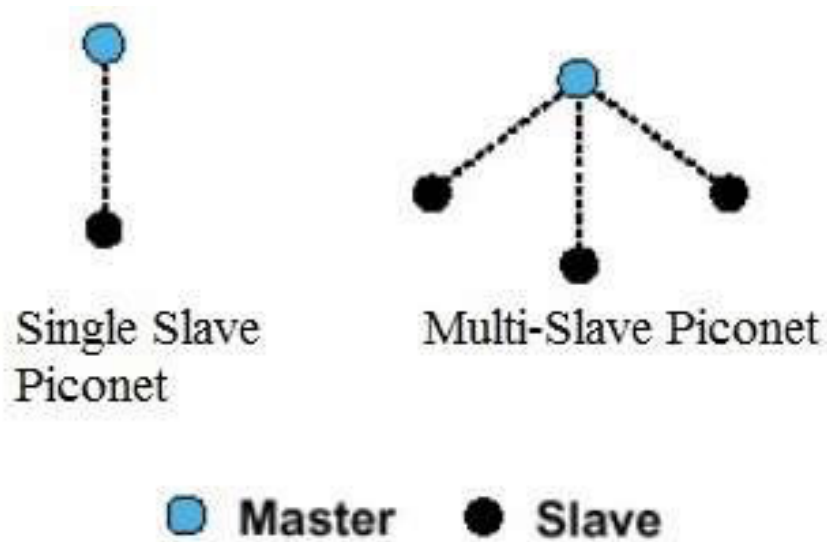


Jim Kardach read "The Long Ships" by Frans G. Bengtsson, which was set during the Viking Age and included Harald "Blåtand" Gormsson, Denmark and Norway.

The Anglified version of Harald 'Blåtand' is Harald Bluetooth. He is known for uniting discordant Viking tribes into the Kingdom of Denmark. In a similar way, Bluetooth is meant to combine multiple wireless communication protocols into one standard.

The Bluetooth logo is also a combination of Harald Bluetooth's initials, HB, in the runic script. Although it's not intentional, there's another similarity between the Vikings and Bluetooth: The Vikings used slaves (called thralls), and so did Bluetooth.

### 3. Bluetooth using Slavery mode



When Bluetooth devices connect to each other (for example, your phone and your wireless speaker), the relationship is like a master-slave relationship: One device acts as the master and the other devices act as slaves. The master transmits information to the slave, and the slave listens to information from the master.

A master can have up to 7 slaves, which is why your computer can be connected via Bluetooth to multiple devices at once (e.g. wireless keyboards, mice, printers, speakers, etc.). Devices connected to each other via Bluetooth are called 'piconet'.

A device can be a master in one piconet and a slave in another piconet at the same time. The Master-Slave relationship can also switch. That's why you need to put your Bluetooth device in pairing mode to connect. It becomes a master to establish a connection and then becomes a slave again. Part of the reason is that setting up Bluetooth connections is pretty easy.

### 4. Bluetooth is sometimes better than Wi-Fi



Wi-Fi is also a wireless technology standard, but Bluetooth and Wi-Fi serve two separate purposes. Wi-Fi (which is the brand name for the IEEE.802.11 standard) is meant to replace high-speed cables, so it takes some

setup but supports high bandwidth.

Bluetooth, on the other hand, is for mobile devices and related applications. It is great when you need to connect two devices with minimal configuration (usually just pressing a button). Also, because Bluetooth uses a weak signal, it is often subject to interference and limits the devices that can connect in 'noisy' environments.

## **5. Bluetooth is great for the Internet of Things**



In the Internet of Things, machines often need to send short bursts of data in highly noisy environments. With hundreds of sensors and devices sending data, Wi-Fi is too cumbersome to set up.

One drawback of Bluetooth is its lower bandwidth compared to Wifi , but for many industrial applications, high bandwidth is not really necessary.

Bluetooth is also useful for smart home setups. Again, many smart home devices don't need high bandwidth connections, and Bluetooth setup is much easier.

Furthermore, newer versions of Bluetooth can create a self-healing mesh network. This means that individual devices can still connect, even if one device loses power or is disconnected. If your door locks, HVAC system, washer, dryer, refrigerator, and lights are all connected, you certainly don't want them all to be disabled just because one device fails.

Another limitation of Bluetooth is its limited range. This can be an issue in a smart home depending on how large or small your home is.

## **6) We are using Bluetooth version 5**

The Bluetooth Special Interest Group officially adopted Bluetooth 5 as the latest version of Bluetooth in December 2016.

'With Bluetooth 5, Bluetooth continues to revolutionize the way people experience IoT. Bluetooth continues to embrace technological advances and push the limitless potential of IoT. '

As the Bluetooth SIG announcement makes clear, Bluetooth 5 is specifically aimed at the Internet of Things. It boasts four times the range, double the speed, and an 800% increase in broadcast messaging capabilities. It also

introduces the aforementioned networking capabilities.

Bluetooth 5 is backwards compatible with previous versions of Bluetooth, but new hardware is required to take advantage of the benefits listed above. So it may take a while to see all the benefits Bluetooth 5 brings, but it's certainly an exciting development as the Internet of Things continues to gain traction!

## Connect with Bluetooth



Many mobile devices have built-in Bluetooth radios. For example, PCs and some other devices without built-in radios can be Bluetooth enabled by adding a Bluetooth dongle.

### 1. What is Dongle?

The process of connecting two Bluetooth devices is called 'pairing'. Generally, devices announce their presence to others, and users select the Bluetooth device they want to connect to when its name or ID appears on their device. As Bluetooth-enabled devices continue to grow, it is important to know when and which device you are connecting to, so there may be a code to enter to help ensure you are connecting to the right device.

This pairing process may vary depending on the devices involved. For example, connecting a Bluetooth device to an iPad may involve different steps than pairing a Bluetooth device to a car.

## Limitations of Bluetooth

There are a few downsides to Bluetooth. First, it can be a battery drain on wireless mobile devices, like smartphones, although as the technology (and battery technology) has improved, this is less of an issue than it used to be.

Additionally, the range is quite limited, typically only extending to about 30 feet (over 9m), and as with all wireless technologies, obstacles such as walls, floors, or ceilings can reduce this range even further.

The pairing process can also be tricky, often depending on the device involved, the manufacturer, and many other factors that can lead to frustration when trying to connect.

## Bluetooth security issues

Depending on how it is configured. Bluetooth technology can be quite secure. You can see the advantages of using key authentication and encryption. However, many Bluetooth devices have a short number of digits used in PINs, and this can be dangerous for these devices.

If someone can 'discover' your Bluetooth device, they can send unsolicited messages and abuse your Bluetooth service, which can cause a lot of problems. Worse yet, a stranger can find a way to hack or modify your data. An example of this type of attack is an attacker who can use Bluetooth to steal important information from your device. Viruses or other malicious code can also take advantage of this technology to harm your device. If compromised, your data can be modified, damaged, stolen or lost. You should be very aware of who you are sending information to over an untrusted Bluetooth connection.

### How Bluetooth is hacked?

While it may seem strange that people could attack devices over Bluetooth, it makes sense when you consider that. Since all sorts of accessories can connect using Bluetooth technology, you can access all sorts of features over this wireless technology. Despite its intended purpose of facilitating communication, hackers are actively abusing Bluetooth to target all sorts of devices, regardless of manufacturer and operating system, in the following ways:

1. **Bluejacking** – One of the less serious types of attacks, it allows people to send unwanted messages to others.
2. **Bluesnarfing** – Moving on to more dangerous and common types of attacks, Bluesnarfing can access people's personal information, including photos, videos, contact lists, emails, and passwords
3. **Bluebugging** - This often occurs on phones with outdated Bluetooth protocols that allow pairing of devices without the user's consent. Attackers can exploit such vulnerabilities to take control of the phone's features. This includes listening to phone conversations, connecting to the device's Wi-Fi, or reading text messages.
4. **Bluesmacking** – Bluetooth devices are also vulnerable to DoS attacks, where devices are flooded with large data packets. This overwhelming flow disrupts normal operations, forcing the device to shut down.
5. **Car whispering** – Hackers can also exploit vulnerabilities in Bluetooth-enabled car radios to eavesdrop on conversations and phone calls or even manipulate a car's infotainment system for malicious purposes.

Scary, right? While Bluetooth technology has its flaws, it's not completely insecure. As a user, there are plenty of things you can do to prevent an attack from happening!

### So how to protect?

- **Disable Bluetooth when not in use** – Unless you enable the transfer of information from one device to another, you should disable this technology to prevent unauthorized people from accessing it.

**Use Bluetooth in stealth mode** – When you enable Bluetooth, set it to 'undiscoverable'. Stealth mode prevents other Bluetooth devices from discovering your device. This does not prevent you from connecting to other Bluetooth devices. Both devices can still discover each other if they are both in stealth mode. Devices such as

mobile phones and wireless headsets need to be set to 'undiscoverable' for the initial connection so that they will always be able to discover each other without having to search for a connection again the next time.

Be careful where you use Bluetooth – You need to be mindful of your environment when pairing your device or operating in discoverable mode. To take a concrete example: If you are in a public 'hot spot', there is a much higher risk of someone intercepting your connection than if you are connecting indoors or in your car.

Evaluate your security settings – Most devices come with a variety of features that can help you equip yourself. However, enabling certain features can leave you vulnerable to attack. So, disable any unnecessary features or connections you may not need. Review your settings, specific security settings, and select the options that are necessary for you without putting you at high risk. Make sure all your Bluetooth connections are configured with the necessary security requirements.

Take full advantage of security options – Learn about the security options your Bluetooth device offers and take full advantage of features like encryption and authentication.

See also:

1. Instructions for using Bluetooth on devices
2. How to connect Bluetooth devices on Windows
3. How to Fix Bluetooth Missing Error on Windows 10 Settings

You finished reading the article "**What is Bluetooth? Useful information about Bluetooth technology**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.