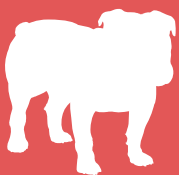




Consumer Guide

to the Internet of Things



We keep you safe and we keep it simple.



What is IoT?

IoT stands for Internet of Things – the current ‘buzz’ term for connected or ‘smart’ devices. It relates to any gadget, appliance or device that is connected to the internet and can communicate with other devices without human intervention.

Here are some examples:



A fitness tracker

that sends data on your daily activity to online servers, which could then be viewed on your smartphone.



A security camera

that sends a feed to an online server so that you can view it on a smartphone, tablet, or another computer when away from home.



Smart thermostats

that learn and adapt to your lifestyle, adjusting temperatures in the home for comfort or energy efficiency.



Smart lighting

that can be set to switch on or off at certain periods, or that can be controlled remotely from a smartphone.



A Smart TV

that can stream music, videos or photos from online services or other computers in the home. It can also interact with other smart devices, for example, displaying content from baby monitors and security cameras.



If you're using any of these connected devices, you're already involved with the 'Internet of Things.'





How IoT devices work

Connected devices typically connect to the internet through a home Wi-Fi network and router.



Connected devices can sometimes talk to other related devices on the same home network and act on the information they get from one another. People can interact with the connected devices to set them up, give them instructions or access data, but the devices do most of the work on their own without human intervention.

All of this is made possible by tiny, embedded mobile components that allow almost anything to become 'connected.' They rely on the always-online nature of our home and business networks, and often process data online via cloud-based software where huge amounts of data from many different users can be analysed together.





What else can IoT do?

Internet of Things devices have an extremely broad range of applications across almost all industries.

The sort of devices described above show how IoT can add convenience to our lives, automate time consuming activities, and ultimately offer us more control over the things we interact with every day.

In a broader sense, IoT is set to offer massive benefits across a wide range of areas.



Engineering

An IoT device in an engineering plant can alert maintenance personnel to an impending failure, averting a breakdown.



Security

A smoke or security alarm that is connected to the internet can remotely inform someone that it has been triggered when they are not present.



Smart cities

IoT is also considered to be fundamental technology for smart cities, including smart traffic signals that monitor use and smart bins that signal when they need to be emptied.





Industry

Within an industry, IoT can be used for all sorts of processes, such as supply chain tracking or crop monitoring.



Healthcare

In healthcare, smart pills and connected monitoring patches are already available that offer the potential to save lives. Others gather important data – such as monitoring how much Parkinson's sufferers shake. The activities of elderly or ill people can be tracked to detect dangerous anomalies, and people with heart disease can be monitored for abnormal heart rhythms.



These are just a few examples of how connected devices and the Internet of Things are set to shape our future. For a great many of us who are already involved with IoT, the future is now, and as with many technological advances, the issue of security is paramount to it being a success.



Are we ready for IoT?

One of the biggest issues surrounding the Internet of Things is security.

In a broad sense the industry seems to be a little too eager to embrace the benefits of this new wave of technology and has done so before a set of established security protocols are in place.

As a result, there have been a number of high profile incidents which have shown just how vulnerable connected devices are to hackers.

Here are just a few examples:



Smart TVs

Researchers discovered a flaw in smart TV transmissions and launched something called a 'red-button attack,' in which the smart TV data stream was hacked and used to take over apps shown on the TV.

For example, the hackers were able to post content onto the smart TV owner's Facebook page.



Smart cars

A number of security researchers have shown how smart cars can be hacked and controlled, ranging from killing the brakes to making the car swerve from left to right.

Students in China hacked a Tesla Model S electric car and made the doors fly open, the wipers wiped and the horn honked automatically.

Apparently they simply cracked the password for the car's mobile app.





Toilets

A connected toilet seat controlled via an Android app was hacked by researchers, causing the toilet to repeatedly flush, raising the water usage. The attackers could also cause the unit to unexpectedly open and close the lid, and remotely activate bidet or air-dry functions.



Baby cams

There have been a number of incidents in the US in which internet connected baby monitors have been hacked. The hacker has then screamed at the child to wake up, or posted video feeds of the child onto the internet.



Buildings

Hackers shut down a floating oil rig by tilting it, while another rig was so riddled with computer malware that it took 19 days to make it seaworthy again.



Heating

Cybercriminals managed to penetrate the thermostats of a state government facility and a manufacturing plant in New Jersey, and were able to remotely change the temperature inside the buildings.



Industry

Hackers breached a steel plant and compromised numerous systems, including components on the production network. As a result, mill personnel were unable to shut down a blast furnace when required, resulting in "massive damage" to the system.





Thankfully, most cases of IoT 'hacks' to date have been benign and largely go to show what could have happened had the malicious party been looking to cause real damage. But they illustrate on a larger scale that steps need to be taken to establish better security around IoT as a whole.



Importantly, this general concern has also made its way through to the consumer market.

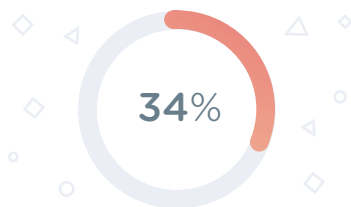




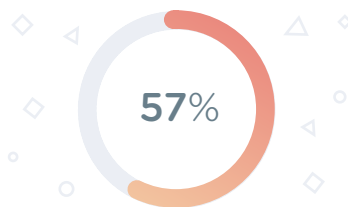
Consumer concern

In 2016, BullGuard conducted a large scale survey of over 6,000 UK consumers, and discovered that while many had not heard of the term 'Internet of Things', they were already using connected devices.

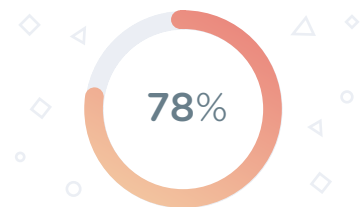
Notably, there was also a great deal of concern about security:



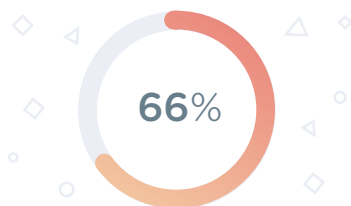
have already experienced a security incident or privacy problem in the past



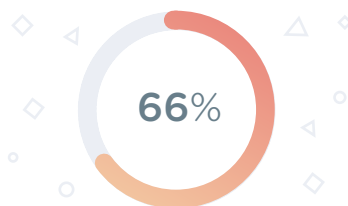
are also anxious about privacy breaches



express concern about security risks such as viruses, malware and hackers.



of consumers are 'very concerned' or 'highly concerned' about potential hacking and data theft carried out against their connected devices



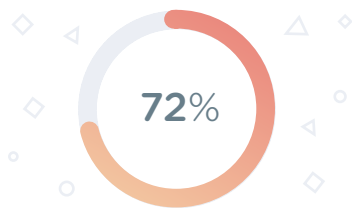
are worried about data collected by device manufacturers being inappropriately used or stolen



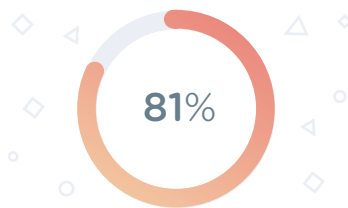


The rise of the Internet of Things has taken many by surprise, and despite this high level of concern, modern consumers are far less prepared to protect themselves from hackers and malicious users.

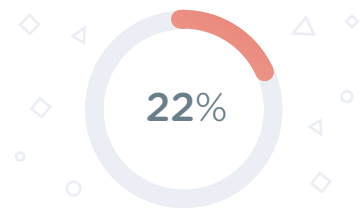
This is illustrated by further statistics from the survey. The majority of respondents – 63 per cent – described their technical skills as ‘intermediate or advanced,’ yet:



do not know how to configure a router to keep a home network secure



are capable of setting up their own router, 63 per cent have not changed their router's password. 49 per cent say they don't know how to do this



of consumers with advanced technical skills are not confident in their ability to keep their connected devices secure





What could happen to me?

Given the wide range of connected devices that are currently available, there are a great many things that hackers could do once they have gained access to them. Here are some of the ways they could do so, and an example of what could go wrong:



Access to an **Unsecure smartphone**

How do they do it?

If a smartphone is lost or stolen and doesn't have a key lock or login security of some kind, it would allow someone to potentially access any smart devices that are controlled by that smartphone, along with any associated data.

What can happen?

If the smart phone is used to control heating systems, burglar alarms, security cameras or other IoT devices they could be easily tampered with. At the same time the home network could be accessed, allowing someone to browse computers and other devices and steal sensitive personal information.



Access to a **Wireless network**

How do they do it?

If not configured with some form of security a wireless network is essentially 'open,' and can be connected to by anyone in range. Inadequate security and poorly chosen passwords are also ways that someone might gain access.

What can happen?

A hacker is essentially sitting in your digital front room, seeing what you are doing, which websites you are visiting, what purchases and payments you make online, which email accounts you have, the private messages you send and so on.





Access My router

How do they do it?

Service providers often set up routers with a default login name and password – it is then up to the user to change this to something more secure. Unfortunately many are not told they need to do this, or how to, resulting in many routers being easily accessible to hackers who have some basic information about the user's network.

What can happen?

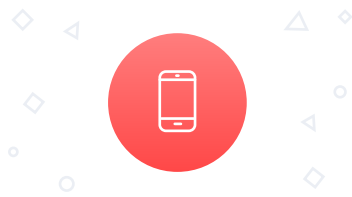
A hacker could login to the router's setup page and covertly access data such as the wireless password, granting them access to the user's network, or change the router login to prevent the user from accessing it themselves. They could then go on to roam around the network at will, plucking out banking details, passwords and other information, and even make purchases using the payment details of the person who the network belongs to.





How to stay secure

The Internet of Things brings with it a wealth of connected devices that can add convenience, comfort and excitement to our lives. But as with any new technology trend, it's important to be aware of the risks and make sure you and your devices are secure.



Set up a key lock on
a Smartphone



Change the default
password on a router



Change a wireless
password





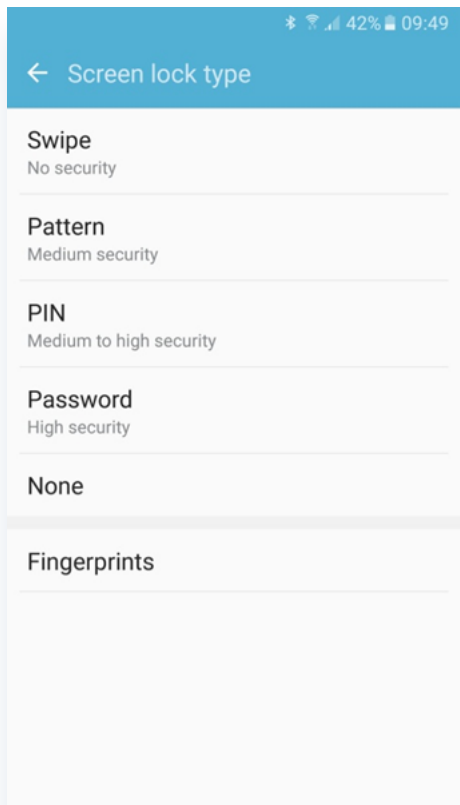
How to stay secure

Set up a keylock on your smartphone

Why it's important

If a phone is lost or stolen it could be accessed and used by anyone if not protected by some form of security. This could mean connected devices that are accessed via the smartphone are open to hackers.

How to do it



Most smartphones offer a number of different types of security for accessing a device.

Choose one that reflects how likely you think it is that your device might be stolen, and the amount and type of sensitive information stored on it.

Depending on the phone type, browse the settings menu for an entry labelled “security,” or “screen lock” or similar and view the options available.

Typically the more complex the type of security, the more difficult it is to “guess,” but this can also make it more difficult to remember.

Some modern phones include fingerprint protection, which is a safe and simple alternative, though this will usually involve choosing an additional form of security as a backup option.





How to stay secure

Change a router password

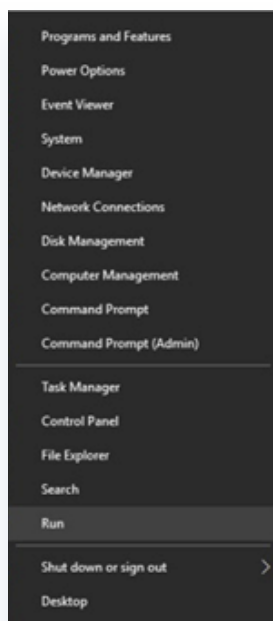
Why it's important

A hacker with access to your router would also have access to your network and any connected devices. Sensitive data such as banking details, passwords, browsing history and other personal information could then be found and used for a number of illegal activities.

Hackers have clever ways to work out who your internet provider might be based on the name of your network along with the type of router being used, so it's not a stretch to assume that they may also know the default password.

The first thing you need is the IP address of your router. If this wasn't noted down or bookmarked during initial setup, you'll need to find out what it is.

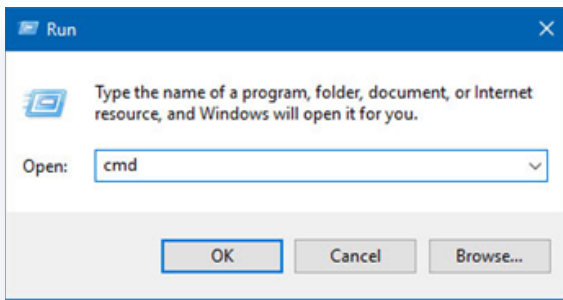
How to do it (PC):



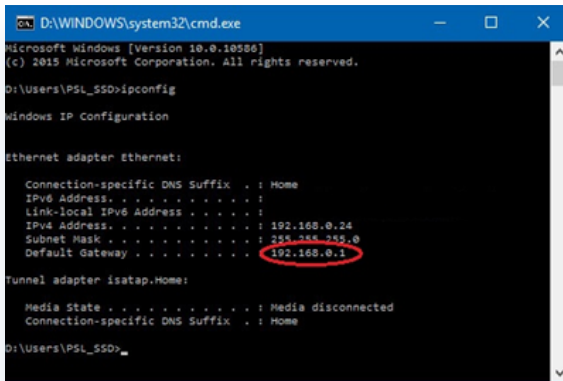
The simplest way to do this in Windows is to find the Run command in the start menu.

Depending on the version of Windows you are using, you may see it immediately when you click the Start menu, or you may need to right-click and select it from the list that appears.





The Run box should now appear.
Type cmd in the box and hit enter.



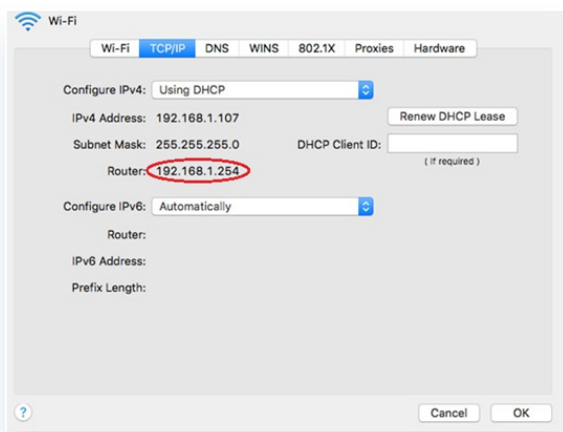
When the command prompt appears in a black window, type ipconfig and hit enter.

You will see a line that begins with 'Default Gateway' towards the end of the text that has appeared. The number on this line is the IP address for your router.

How to do it (Mac):

Finding a router's IP address on a Mac is quite straightforward.

- Open System Preferences in the Apple menu
- Click on 'Network Preferences' under the 'Internet & Wireless' section
- Select 'Wi-Fi' and click on the 'Advanced' button in the bottom right corner.
- Click on the 'TCP/IP' tab.



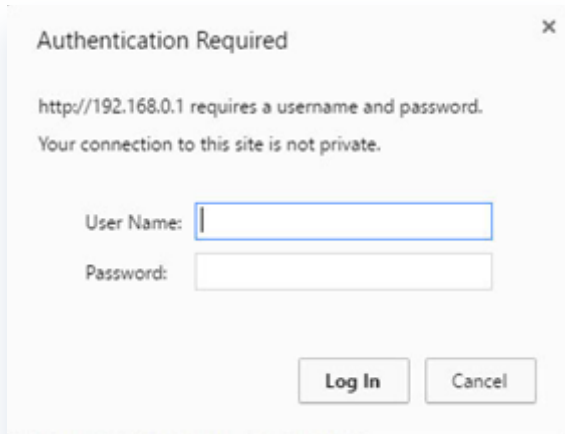
You should now see a screen like this.
The router's IP address is clearly shown alongside 'Router', as shown in the image.



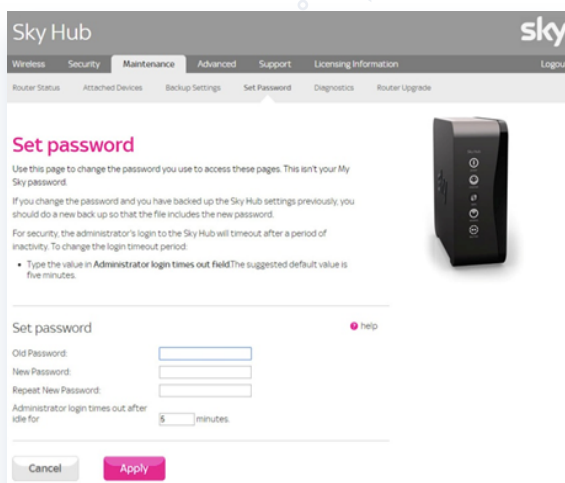


Loading your router setup page (PC & Mac)

Once you have your router's IP address, type it into any web browser in the same way you would a website address. Feel free to bookmark this address to make it easier to access settings at a later time.



You may then see either a web page or a dialog box appear requesting your user name and password. If you have not changed this, it will be set to the default used by your provider. If you're not sure what this is you will need to contact your ISP to find out.



If you have not changed your default password, you may then be taken to a page that requests that you set a password. Doing so now will help to ensure that your router is better protected against outside attack.

If you have already changed your password you may be taken to the standard home page for your router. If you still want to change your password, search for a 'set password' or 'change admin password' or similarly worded link.

This may be listed under 'Account' or 'User settings' or 'Maintenance' or a similar section of the router settings page.





How to stay secure

Change your WiFi password

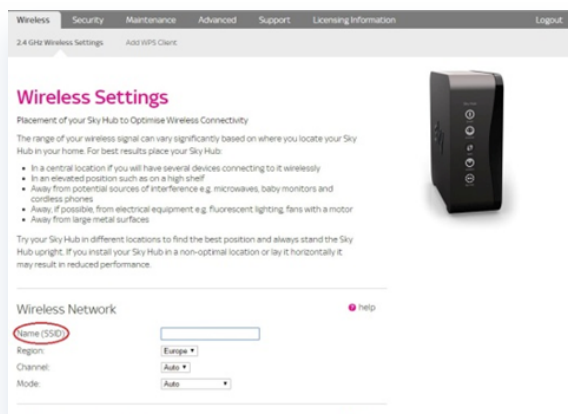
Why it's important

Your wireless password is even more important than your router password.

Though most ISPs now provide users with complex passwords by default, it's always worth double-checking and of course, some users may have changed their password to something simple and easy to remember.

If a hacker can guess your wireless password, they can access your personal WiFi network. This may allow them to view and control attached devices, exploit network vulnerabilities, open ports and gain access to your files and operating system.

How to do it

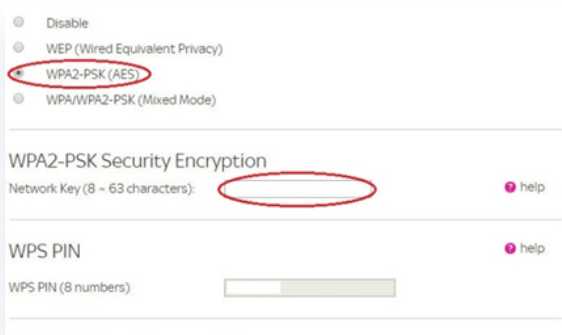


Once you have changed the default password for your router, you may want to also change your wireless password, especially if you're using one that is easy to guess.

If you are logged in to your router settings, as described in the previous guide, search for a menu option that reads 'Wireless' or similar.

On this page you'll see a range of different settings for your wireless network. Note that the name of the wireless network, or SSID, is the same one you choose when you add new devices.





Scroll down this page if necessary and search for an area that shows security options, along with your current wireless password.

This is the 'key' that's used to allow new devices to connect to your wireless network. First of all, make sure WPA2 (AES) is selected as the preferred security option.

This is the most recent, and most secure, standard. Next, enter a new wireless key, ensuring that it's not easy to guess, and apply the new settings to complete your wireless password change.



By completing these three steps you've made sure that your smartphone, router and wireless network are well protected from hackers and outside parties.





How to set strong passwords

Changing default passwords is an important first step towards a more secure network, but if the new passwords are easy to guess it won't take long for hackers to find a way through. Read on for advice on how to choose passwords, what constitutes a 'strong' password and how to remember them.

Three tiers for strong passwords

In an ideal world we'd all have a unique and hard to guess password for every website we log in to. Realistically this is very difficult to accomplish, but a good middle ground is to prioritise websites based on the importance of the personal data they store.



Tier 1

Sites that contain highly sensitive data such as banking, payment or business details or very personal information



Use a strong, unique password for each



Tier 2

Sites that may contain some personal data that you'd prefer others didn't see but is unlikely to compromise you in any way



Use two or three variations on a strong password that are still difficult to crack



Tier 3

Sites that don't contain any particular personal data or information that is likely to compromise you in any way



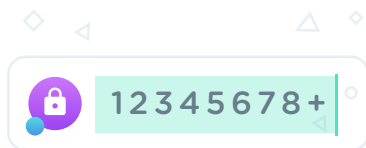
Use the same one or two passwords



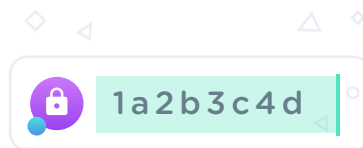


How to choose a strong password

Picking a strong password requires:



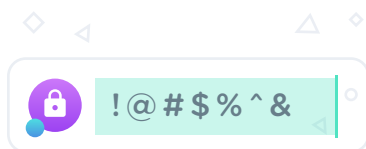
A minimum of 8 characters



A mix of alphabetical and numeric characters



A mixture of upper and lowercase – passwords are case sensitive

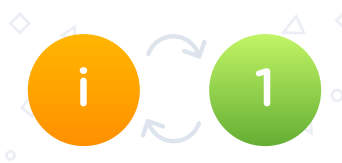


Use of symbols if possible
(spaces shouldn't be used as they aren't recognised by some password systems)

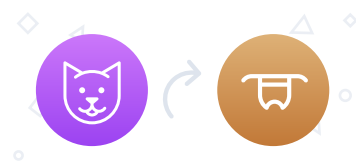
But really you should avoid:



Words or phrases that include personal details about you that could be found online. For example: mother's maiden name, place of birth, the street you live in, part of a telephone number, where you went to school, favourite sports team



Lazy substitutes – while it's a good idea to swap letters for symbols, don't think just swapping an 'i' for a '1', or an O for an '0' is enough – you need to get more creative.



Using real words or combinations of words, or obvious phrases such as 'CatInAHat'





Memory aids

A good rule of thumb is to replace one or more letters with a symbol or number. This makes passwords more secure, but can make them difficult to remember. Here are some ways to avoid coming unstuck:



Try an acronym for an easy to remember quote or phrase - for example 'I love Marmite on toast' could become ILuvMM80T



If you're struggling with one too many letter and number combinations, get personal. The main question to ask when choosing a word or phrase for a password is "do lots of people know this about me or could they easily find it online?" Pick a habit, pet hate or fear that hardly anyone knows about – for example IHateBrownSnails. This is a good idea for solid 'Tier 3' passwords.



When it comes to 'security questions' for resetting passwords, don't enter the correct information. Instead choose something funny and memorable – for example Place of Birth: TheMoon, Mother's Maiden Name: TheQueen



Visualise a bizarre image that could be turned into words and use it to create a password. For example, a duck wearing a top hat sitting in a bucket could become 'Quack, hat, bucket' and therefore: Qu4ckHatB0kit



If you prefer to write down passwords, try instead writing down a hint to the password that only you can decipher





Poor Passwords

Even if you don't have the best password in the world, make sure you don't choose one of the worst. Here's a list of the most common (and therefore easiest to guess) passwords of 2015*.

Top 10 Worst Passwords (descending order)

| | | |
|----------|----------|-----------|
| 123456 | password | 12345678 |
| qwerty | 12345 | 123456789 |
| football | 1234 | 1234567 |
| baseball | | |





The (worst of the) rest

| | | |
|---------|------------|------------|
| welcome | 1234567890 | abc123 |
| 111111 | 1qaz2wsx | dragon |
| master | monkey | letmein |
| login | princess | qwertyuiop |
| solo | passw0rd | starwars |



*Passwords from TeamID's SplashData, compiled from 2 million leaked passwords in 2015

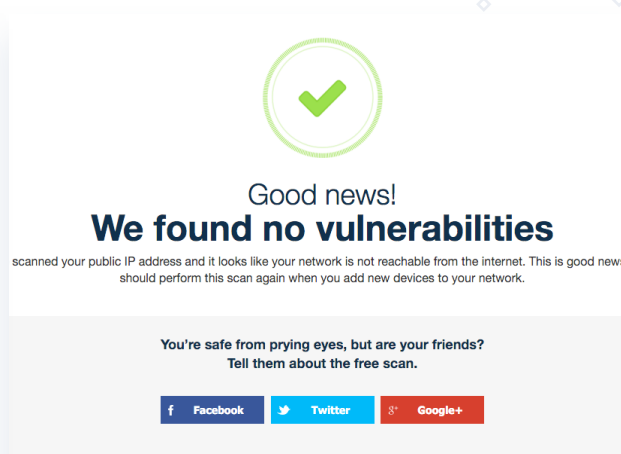




BullGuard IoT scanner

Manufacturers and security vendors can work together to ensure a better standard of security for IoT devices, and can also provide consumers with the tools and knowledge to help protect themselves.

BullGuard has developed a new free IoT Scanner for just this purpose – it allows anyone to scan a home network for smart devices that are exposed to the internet and could be vulnerable to hackers.



If a smart device is flagged as being insecure, further details about the specific issues are revealed, allowing users to take steps to remedy the problem.



Be sure to run the BullGuard IoT Scanner periodically and when any new connected devices are installed in and around the home, just to be on the safe side.

→ Go to iotscanner.bullguard.com to scan for free

