NEWSLETTER

Anything that can be turned on or off can be connected to the internet thanks to the Internet of Things (IoT)

Welcome to the 'Internet of Things'

You arrive at home and the door unlocks because it knows who you are, sensing the key in your pocket. The lights switch themselves on and your favorite music begins to stream gently through the living area. It's already the perfect temperature, and as you head for the fridge, you notice an alert on the screen congratulating you on meeting your exercise goal today and suggesting a tasty snack.

Okay, it sounds like a scene from a movie, but it's actually reality today thanks to the Internet of Things (IoT). Almost anything that can be turned on or off is now able to be connected to the internet. An entire industry has popped up to help users create a custom experience designed around their unique needs. Electronic locks, lights, healthcare wearables and household appliances are just the beginning. IoT goes beyond devices you can use to surf the web – it's a global revolution.

Adapters can transform even the most random appliance into a connected gadget, as well as add new layers of functionality. Cloud software is creating piggy-back connections, resulting in not just a new experience, but a new way of interacting with the data produced. It may all seem impossibly futuristic, but IoT is less about technology and more about

enhancing relationships between people-people, people-things and things-things.

Millions of people are wearing a Fitbit or Jawbone to track steps and calories, while others are letting their fridge order groceries! The practical applications are almost endless, commonly including: GPS trackers on pets, home security via webcam, patient monitoring of blood pressure/heart rate, weather monitoring, and remote power points. No more worrying all day if you left the iron on, just push a button on your phone and know for sure it's turned off.

Of course, with all this connectivity comes risks. While the idea of having your toaster hacked is a bit mind-boggling, technology connected to the internet is open to exploitation. The webcam that allows you to monitor your pets may also allow other people to glimpse inside your home, but only if it's not secured properly. Unfortunately, it only takes one small gap for a cyber-attack to get through, and once in, all connected devices are at risk.
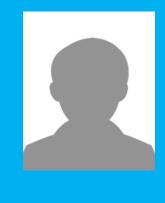
Having your lights taken over by a far-away prankster may seem like a small risk, but gaps allow them into your computers, phones and tablets too.

That's the part the movies skip over – the networking protections that exist in the background, shielding against attacks.

Taking the time to properly secure your IoT device is essential to making sure you get the whole, happy future-tech experience. We're big fans of IoT and can't wait to see what comes next!

Got an IoT device? Give us a call at 0113 2579992 to help you set it up securely.

In this newsletter, we talk about how just about anything can be connected to the Internet. This can bring great convenience but also great danger.

ALERT: Your Antivirus May Be Letting You Down

The best way to avoid a computer virus is by using common sense, but that doesn't mean you'll be safe from attack. Even the most careful user can find themselves infected in an instant and spreading the virus faster than a sneeze in flu season. It's why antivirus software is still the first package we install on all systems – because you never know when you'll be attacked. But should you choose free or paid antivirus?

Advertising: Much like a free app making its fortune with in-app purchases, the free antivirus software will push for payment. Expect popup boxes pestering you to sign up to the paid version at least daily. Some free options will also try to change your browser home page and default search engine, an inconvenience you may be stuck with. Paid options are more respectful and largely invisible unless they've detected a problem.

Effectiveness: It's fair to expect your antivirus to detect malware, and testing showed that in a head-to-head battle free and paid are about equal at catching known infections. And therein lies the kicker: generally speaking, free antivirus needs to have recorded a virus to its library before it can detect it. Paid antivirus is more likely to identify and stop a new virus. It essentially bases the detection on suspicious behavior, source and attributes, a far more effective method of detection.

Features: Free antivirus options are usually created from the paid version, taking out everything except the bare minimum. In your paid version, you can expect advanced features like spam filters, firewalls, parental controls and secure web browsing. Some paid antivirus will also update your other software packages, forming a more secure protection against attacks. For example, you might view a malicious image file that takes advantage of an exploit in your PDF software. Unfortunately, hackers have advanced beyond simple tactics and it's not just about avoiding email attachments anymore.

Support: Free antivirus options are the most popular choice because they're… free. Obviously. This also means there's generally no support available. If there's a problem or conflict with another program, you may find yourself without protection until it can be resolved. Paid antivirus options usually include telephone support, ready to help with problems ranging from installation to system diagnostics.

Ease of use: Depending on what you use your computer for, this may be an important concern. Free antivirus options are easy to install and use, but are very limited in their flexibility. They come as-is, meaning you can't pick and choose what it monitors or how it reacts. For example, users occasionally find it necessary to disable ALL protections in order to install a network game. Paid versions are more likely to allow you to adapt the way it runs, switching features on and off as required.

Free antivirus is fine for very basic protection, those on a budget or those with an older PC. In these cases, something is always better than nothing. But we generally recommend you go with a paid antivirus to defend you from the new attacks that are released daily, and to ensure you've got solid protection that will make a real difference to your digital safety.

Talk to us about upgrading to a paid antivirus.

Emerald ICT
Complete Computer Solution

Unit 39g, Springfield

Bagley Lane

Farsley, Leeds LS28 5LY

0113 2579992

info@emeraldict.co.uk

www.emeraldict.co.uk