
INTERNET OF THINGS
POTENTIAL RISK OF CRIME AND HOW TO PREVENT IT
WHAT IS THE INTERNET OF THINGS?
INDIVIDUALS AND HOUSEHOLDS
BUSINESSES
STEPS TO PREVENT CRIME

WHAT IS THE INTERNET OF THINGS?

The Internet of Things is an increasingly important development. It presents great new opportunities and real benefits to society.

The Internet of Things is the term used to describe the increasing connectivity of electronic smart devices and systems, whereby smart devices and systems are able to communicate with each other and share data. Usually the smart devices and systems will be connected wirelessly to local networks and the Internet, and they will communicate with each other without the need for human intervention.

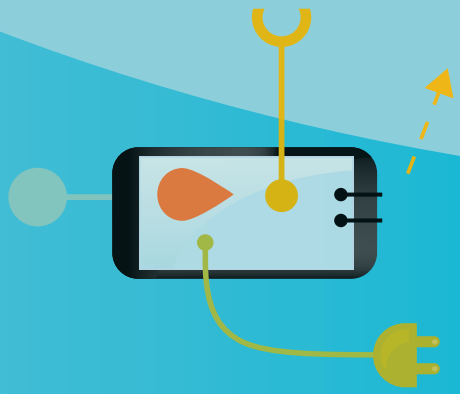
The development of smart technologies will increasingly link up and make existing systems and household goods “smart”. It will not be too long before the Internet of Things allows your smart central heating system to communicate with your smart window or door security and both are able to communicate directly with the sensors in the tablet or smart phone you are carrying, which tells them where you are.

The scale of the Internet of Things is increasing all the time as the number of connected smart devices increases. It is estimated that there will be 25 billion connected devices by 2020, and this is thought to be a conservative estimate.

WHY GUIDANCE?

The Internet of Things presents great and increasing opportunities to society through transforming the way that the world works around us, as technology and the way we use it develops and changes. However, in the same way as other changes in technology, we have to be aware that it also provides new opportunities for criminals to exploit and we need to take sensible precautions wherever possible.

The purpose of this guidance is to provide general advice to the public and businesses about some of the potential crime risks posed by the Internet of Things and the steps they can take to avoid becoming a victim of crime. More detailed advice about steps to safeguard your home or business should be sought from the product manufacturer, system installer, or service provider. You can refer to **cyberstreetwise.com** for further security advice. The police can also provide advice on general crime prevention and you should refer to **police.uk**.



POTENTIAL CRIME RISKS - INDIVIDUALS AND HOUSEHOLDS

Apps on your smart phone and/or tablet or other systems can provide information on you, for example:

- personal details
- your whereabouts and daily routines
- financial information, such as bank accounts

Apps can also be used to operate other smart systems you have, for example:

- car security
- home security
- home infrastructure
- TV/home entertainment systems

Smart infrastructure systems in your home can similarly provide information on you and your whereabouts.

Infrastructure systems in your home can operate, for example:

- door and window security
- alarms
- wifi and Internet access
- central heating
- lighting

Apps and infrastructure systems can all be subject to disruption and intervention by another person, whether through malware[1] or other means, if precautions are not taken to protect access to them and ensure they can be made secure.

This type of disruption or intervention can leave you vulnerable potentially to **different types of fraud** as information is gathered about you personally and/or your financial transactions, **theft** if your house and/or car have their security compromised, or even **threats** to your personal safety.

However, the risk of this happening will be reduced if you take sensible precautions.

---

[1]Malware is short for “malicious software” and includes viruses, “worms”, “trojan horses” and any other unwanted software designed to access or disrupt or unknowingly gather information.

POTENTIAL CRIME RISKS - BUSINESSES

Apps used by businesses to engage with their customers via tablet or smart phone can provide personal information about customers, when and where orders are being delivered, and their preferences including lifestyle choices.

Communication systems provide information about deliveries being made, what is in the delivery and its value, and where the deliveries are being sent and by which vehicle.

Communication systems can also provide information about how and where payments are made and by whom.

Smart infrastructure systems in your business premises can operate, for example:

- door and window security
- alarms
- wifi and Internet access
- heating, ventilation & air conditioning
- server room chillers and power supplies
- lifts
- lighting
- refrigeration

Apps, communications and infrastructure systems can all be subject to disruption and intervention by another person, whether through malware or other means, if precautions are not taken to protect access to them and ensure they can be made secure.

This type of disruption or intervention can leave your business vulnerable potentially to **attacks against the business itself** as systems are manipulated to damage stock or interrupt services, **different types of fraud** as information is gathered about your business and/or customers, **theft** if your business premises, vehicles or deliveries have their security compromised, or even **threats** to the personal safety of your staff.

However, the risk of this happening will be reduced if you take sensible precautions.

STEPS TO PREVENT CRIME

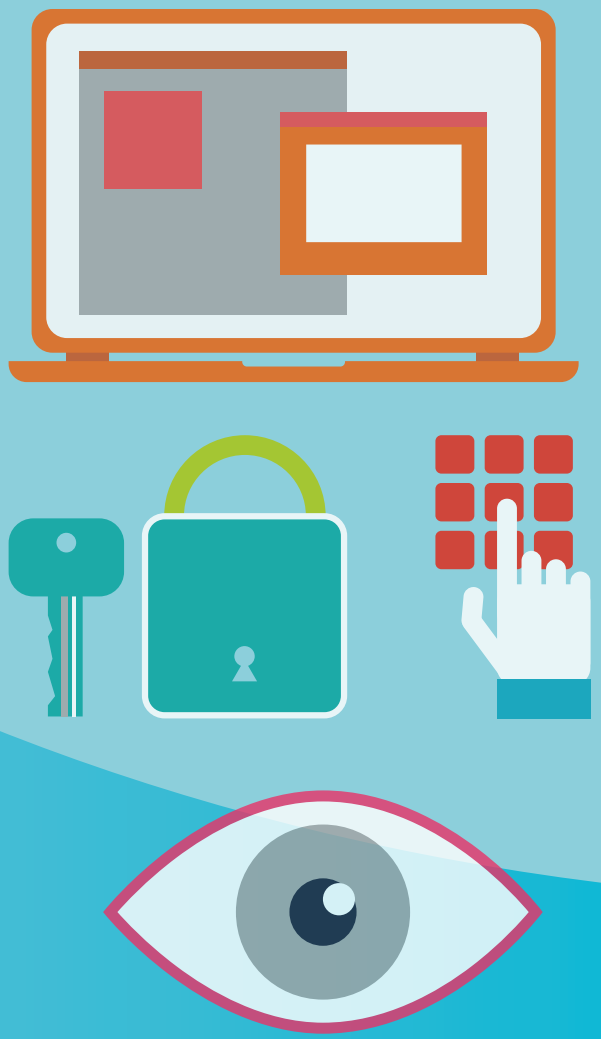
It is very important that households and individuals and businesses take sensible precautions to prevent themselves becoming victims of crime through their use of the Internet of Things being open to disruption or intervention by another person.

One: The best means of protection is to ensure **all** your smart devices and systems are protected by strong passwords which are not disclosed.

Two: You should also ensure that you **accept the latest updates** to your smart devices and systems as this should incorporate the latest security including protection from malware and other viruses.

Three: When buying and installing smart systems or devices, **always check what security they offer** and ask questions if this is not clear so you can make the decision about what is best for you. Also make checks on businesses that may carry out the installation through talking to them about the security of the system, asking for references or checking consumer websites, so you have confidence that security is taken seriously.

The Internet of Things is an increasingly important development which offers real benefits and has potential to transform the way we live our lives. However, it is important we are aware of the potential risks so that we can all take action to ensure our smart devices and systems are secure. If we do this we are much less likely to be a victim of crime, and we can have much greater confidence in the benefits the Internet of Things will bring us.



This guide has been produced by the Home Office and UCL (University College London)

Home Office