

Crime prevention advice for The Internet of Things

The term 'Internet of Things' is something which not a lot of people know about, but almost everyone will have some sort of interaction with on a daily basis in one way or another.

What is the Internet of Things?

The Internet of Things is the name given to the network of electronic devices and other items which can connect to the internet and through connectivity, enable the exchange of data.

Examples

There is now an ever increasing number of items which can connect to the internet. This brings about many benefits but also an increasing number of loop holes for criminals to exploit. Examples of the Internet of Things include:

- Fridge/Freezers that are now connected to mobile devices.
- Automatic orders from printers that are running low on ink.
- Central heating systems that can be controlled from your mobile phone before arriving into work/home.
- Watches that now connect to smartphones.

Benefits

For businesses the increase in connectivity will mean:

- Increased efficiency, especially with regard to manufacturing.
- Potentially greater business opportunities that have become available due to greater efficiency.
- Flexibility in working – location/time.

Things to be aware of

- Increased number of items/processes that could be compromised.
- Cost implications if malfunction/stolen.
- With an increasing number of electrical items that could malfunction beware of bogus calls offering to 'fix' electrical items.

Tips

- Ensure all devices are password protected.
- If you have a Bring Your Own Device policy, ensure it is strictly implemented to ensure that no viruses or malware is transferred to your business equipment.

Technology is developing at an incredibly fast pace with usability in mind, however security is always developing in reaction to this which means it is as important as ever to ensure your business stay on top of their security.

