CYBER ESSENTIALS AT HOME

This leaflet is a short overview of how you can keep yourself and your Smart Home safe from cyber attack, help you in your use of the internet and keep your new smart devices secure.

The Smart Home is here but what is it?

Increasingly our homes are becoming smarter and help look after you but this comes with security and privacy risks. This leaflet looks at these risks, and makes recommendations of the things people at home really must do to protect their homes as they become smart.

A home is Smart if it:

- ✓ is constructed to be smart, designed to help people in the home intelligently
- ✓ communicates with the rest of the world and across networks at home
- ✓ has smart equipment such as kitchen white goods, heating systems, smart lights
- ✓ manages energy by simple thermostats to smart home control to save money and CO2
- ✓ utilises and stores renewable energy and keeps the building cool with ventilation or blinds
- ✓ provides entertainment; smart TV or sound systems
- ✓ contains computers, tablets and smart devices
- ✓ provides devices that help people look after themselves at home and stay healthy and keep them secure.

Connectivity

A Smart Home requires a set of devices that are connected, they use these connections to communicate status and receive instructions. These devices are in the middle of a maze of interconnectivity with external services.

In creating the smart home, you need to consider these questions:

- ✓ How trustworthy are these devices?
- ✓ Who has (legitimate) remote access to these devices?
- ✓ How can the devices be accessed by a non-authorised person and what might they seek to do?
- ✓ What unintended harm can be caused?

What's in the Smart Home?

The Smart Home is full of all sorts of intelligent devices most of which communicate with other devices locally, or with the internet or through the internet to "Cloud" based systems. Just some of these are shown.

This means that the Smart House is awash with radio messages which can be picked up outside the home.

Although many of these messages are encrypted, often their gateways or routers can be accessed.

What are the risks?

- ✓ Personal data could be read and misused, for example identity theft
- ✓ A burglar could detect if your house is empty, for example by remotely accessing cameras
- ✓ A burglar may be able to disable your alarm, or open your doors and windows. (Police already report a proliferation of cars stolen using electronic means to open the doors and start the engine)
- ✓ All your electrical devices could be turned on while you are away, causing a hike in electricity bills
- ✓ A vandal could open windows during a storm to cause flooding inside the house
- ✓ A device could be caused to malfunction causing harm such as a flood or fire and
- ✓ A security failure in one device could be used as a route to attack others, including those holding valuable personal information such as banking details.

How to keep your guard up

In an ideal world, we could trust all the devices in our home, and they would be secure by default. History has shown we are a long way from this. The implication is we should assume the devices and systems can be accessed without authorisation as supplied, and we need to take steps to enhance the security of the system.

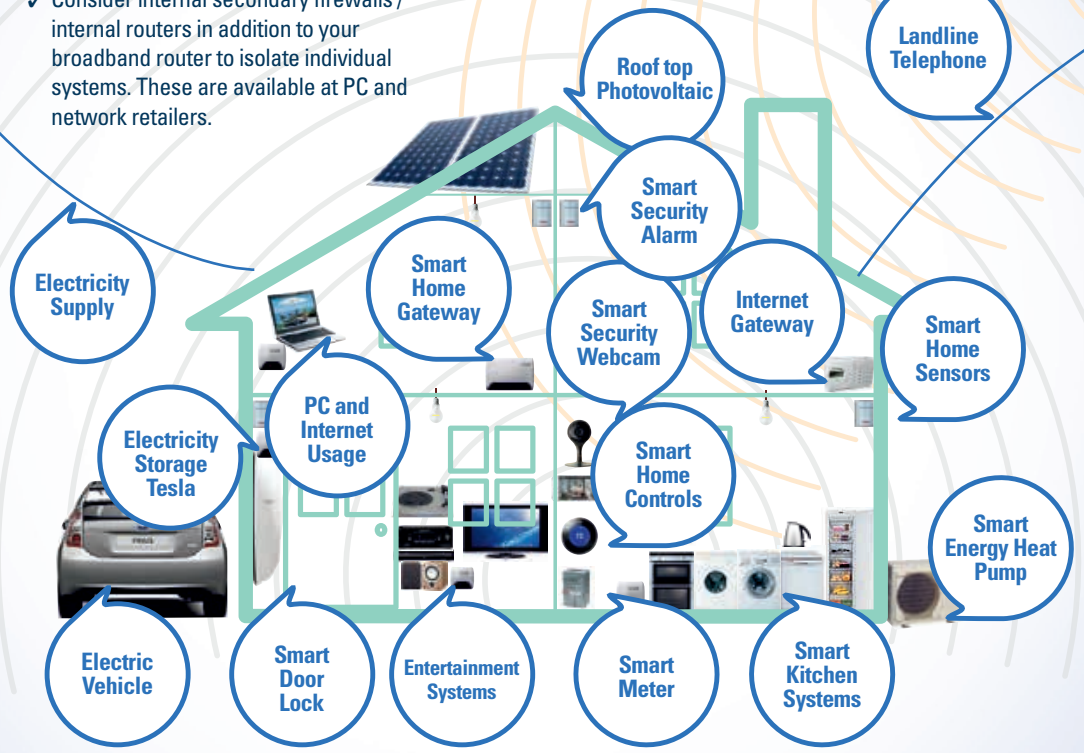
In many cases it is a trade-off. You may have to sacrifice some convenience in order to achieve protection from the risks.

Design

Good design of your overall home network is essential. No single security measure will protect you – multiple approaches are needed.

You must have a firewall between internal and external networks. These are often built into broadband routers. Key points:

- ✓ Change the default administration and WPA2 passwords to new ones that are hard to guess and that have at least 12 characters
- ✓ Ensure WiFi is configured only to use WPA2-PSK(AES)
- ✓ Consider internal secondary firewalls / internal routers in addition to your broadband router to isolate individual systems. These are available at PC and network retailers.



Configure

How you configure the devices in your home will be vital in ensuring the home's safety.

PCs, Laptops, and Mobile devices are fundamentally parts of your Smart Home security environment – they contain a rich picking of data for the hacker that can break a Smart Home device to get access to your network, bypassing firewalls.

Smart Devices

- ✓ Only enable the components of the system you plan to use. Turn other elements off
- ✓ Change default administrator passwords
- ✓ Read the manuals to see what other security settings there are – many are turned off by default
- ✓ Many devices can be configured remotely over the Internet – make sure these passwords are changed. If this mode is not to be used, turn it off
- ✓ Turn devices completely off when not in use.

Mobile devices

- ✓ Remove apps that you no longer use
- ✓ Install anti-virus technology (if available) and keep it up to date
- ✓ Turn on the personal firewall (if available)
- ✓ Only keep essential data on mobile devices.

PCs and Laptops

- ✓ Install anti-virus technology, and keep it up to date
- ✓ Turn on the personal firewall (if available)
- ✓ Disable auto-run, to prevent malware on CD's or USB's from automatically infecting your PC
- ✓ Do not routinely run logged on as the administrator – create a user account for most operations
- ✓ Use encrypted disks on laptops
- ✓ Uninstall applications you no longer use

Passwords

The UK Government have issued good advice about managing passwords. Highlights are:

- ✓ Change default / supplied administrator passwords
- ✓ Passwords should be a minimum of 12 characters long and mix capitals, lowercase, numerals and punctuation as allowed
- ✓ Don't store password as text in files, consider using a password manager
- ✓ Use pass phrase, using random words that are easy to remember – for example "green-fish-helicopter-onion"
- ✓ Use 2 step verification on services where the option is available.

In such systems, in addition to your secret password, a second code is needed. This can be sent via SMS message, or generated by an app on your phone. Google, Facebook, PayPal, LinkedIn, Microsoft and Twitter all offer this capability.

Operating your Smart Home

Having designed, built and configured your secure home, you need to keep it secure:

- ✓ Keep applying those updates. It's annoying, but is essential
  - ✓ PC / Laptop operating systems and application updates
  - ✓ Mobile operating systems and application updates
  - ✓ Other device updates (this is not as easy, and often requires time searching the Internet)
  - ✓ Make sure anti-virus software is kept up to date
- ✓ Regularly review how elements are used – are there sub systems you no longer use that should be turned off?
- ✓ Keep yourself informed, via the Internet, on developments. Attack methods evolve, and you may need to act upon advice to alter security settings
- ✓ Be wary when accessing your smart home from public places – make sure people cannot see you type in your password
- ✓ Use 4G services in preference to untrusted Wi-Fi, such as in hotels or coffee shops.

We want you to enjoy your Smart Home; buy Smart Products and use Smart Systems in you home with confidence. If you follow the simple advice in this leaflet, you and your Smart Home will remain safer from cyber attack, you can use the convenience of the Smart home to increase your comfort, save on your energy bills and keep you well and active.

This leaflet was produced by a group of experts who were brought together in the SH&BA Security Panel which exists to consider, understand and act on security issues in Smart Homes and Buildings.

Panel Members involved in creating this leaflet were:

Adam Simon – CONTEXT
Carl Shaw – Mathembedded
Colin Robbins – Qonex
Mike Windsor and Stephen Pattenden – SH&BA
Stephen Lowe – KTN-UK

The inspiration for this leaflet comes from the UK Government Cyber Essentials scheme, defining the minimum UK business ought to be doing to protect themselves and work by SmartHome Initiative Deutschland e.V. It is produced as a request for comments – please contact us with your views and suggestions how we can improve the advice.