HSB

A Munich Re company

Risk management

‘Smart home’ cyber security

A guide to loss prevention

Households are becoming increasingly reliant on Internet-connected home technologies; from tablets to smart dishwashers to smart speakers. This, however, also means 'smart homes' are becoming more exposed to cyber threats and data privacy risks.

In 2020, there were more than three times as many cyber-crime incidents in the UK compared to domestic burglary offences.[1] Online security needs to be taken as seriously as physical home security, but many consumers still do not apply simple cyber security measures.[2]

This guide has been prepared to provide helpful advice on how to protect your smart home from cyber threats. Some examples of loss events are included in this document to illustrate what can happen. A list of the references used in this guide is located at the end of this document.

Any device that is connected to the Internet to store, transmit or receive data is considered 'smart'. A smart home, also known as a 'connected home', may contain many smart devices (such as a mobile phone or smart watch). There are also many smart household appliances and systems available today, including washing machines, temperature controls, kettles, air conditioning, lighting, toothbrushes, security locks and alarms; to name a few.

Vulnerability to cyber-attacks is becoming an increasing threat to smart homes. Malicious attacks on vulnerable smart home systems can cause damage or disruption, or enable criminals to gain access to the wider smart home network.

There are also risks when private information and real-time data of a resident's activities is compromised (for example, monitoring times when the person is away from home).

When that personal data becomes accessible, the victim(s) may become susceptible to cyber-crimes; which can include data hacking, fraud, email scams, telephone hacking, ransomware, etc. All such cyber-related risks can ultimately lead to financial loss for the victim(s).

Research has revealed that children can be a weak link in home cyber security. Their vulnerability may, for example, lead them to access malicious websites, download viruses, share passwords, etc.

10 simple steps for home cyber security

The principles of cyber security are not too different from how you would physically secure your home. The following provides some advice on how to protect your smart home from cyber-crime. Parents should also be proactive in educating their children about these cyber security steps.

1. Enable security protections
Wireless routers are known as the 'digital doorway' to a home. Invest in a router with strong security features from a trusted vendor.

Ensure that all built-in security protections on your devices are enabled. For example, restrict Wi-Fi access to known devices only, or make your network non-discoverable so that devices need to know your network name in order to connect to it.

Whilst in some cases it may seem more convenient to have security protections disabled, it will make your devices more susceptible to cyber-crime.

For households with children/teenagers, enable built-in parental controls on your computers/devices to prevent them from inadvertently accessing unverified websites that may harm your home network. You may also consider installing trusted third-party parental control software/apps.

2. Install anti-virus software
Ensure you install anti-virus software on all devices where possible and always keep them updated. Enable automatic scans and software updates. Leading developers of anti-virus software work tirelessly to track developments of viruses and malware to keep their software current, but this is only effective if users install the latest updates.

Using the same password for different applications is like having one key that unlocks all of the doors in your house

3. Create secure passwords
Ensure you create strong, complex passwords and change them frequently. The UK Government recommends using three random words to create a strong password.[3] Short and weak passwords with personal details (such as names) are relatively easy for attackers to determine and use to their advantage.

Create different passwords for different accounts. Using the same password for different applications is like having one key that unlocks all of the doors in your house.

4. Back-up your data
Ransomware works by locking your data, following which the cyber criminal demands a ransom to unlock that data. If you regularly back-up your data, you can easily restore your systems and avoid being held to ransom. Back-up your data regularly, and also disconnect the back-up device from your computer so that virus and malware infections cannot spread to your back-up files.

5. Install the latest operating system updates
Ensure that you install the latest updates for all operating systems on your computers and devices. Never procrastinate: updates should be installed as soon as they are made available. Where possible, enable automatic updates on your devices.

6. Only download legitimate software and apps
Only download 'apps' and software from trusted sources (e.g. authenticated app stores such as Google Play or Apple's App Store). This does not only apply to mobile phone apps – Microsoft and Apple have both introduced 'app stores' for PCs and Macs.

Never download unknown software, and always be wary of 'free' software offered through email or websites. Sites that offer free software or downloadable material that is usually not available for free should raise your suspicion.

7. Protect your online privacy
Be aware of the kind of information and opinions you are posting on social media platforms and websites. Your innocent post may potentially expose you to the threat of social engineering fraud.

8. Be vigilant
Remain vigilant and suspicious of unexpected phone calls or emails requesting confidential information (e.g. bank account details). Do not click on email attachments or links unless you are sure that it has been sent from a trustworthy source.

Even if the email looks like it came from a legitimate source, contact the alleged source directly and not through the links or phone numbers in the email. Remember: banks and other similar organisation will never ask for your PIN numbers or full passwords.

9. Monitor your various accounts
Monitor your bank accounts and emails regularly for any suspicious activity. If you spot unfamiliar activity, it could be a sign that your personal information has been compromised. Time is of the essence; the earlier you identify an incident, the faster you can respond to, and limit, the damage.

10. Be prepared
Be prepared for when a cyber incident occurs. For example, have you considered how you would continue to operate if you could not use your computer systems?

Take the time to plan ahead and make contingency plans so that you know who to contact and how to respond quickly to an incident. This can reduce the impact of financial losses and also help you get your systems back up and running faster.

Case study

Home systems damage

The chauffeur of an insured connected his mobile phone to a coffee shop's public Wi-Fi network whilst waiting to pick up his client. The phone became infected by a virus through an illegitimate file download by the chauffeur.

When the chauffeur returned to the insured's residence and connected his phone to their residential, poorly-secured Wi-Fi network, the virus spread via the phone across several devices connected to the network. This resulted in data being disrupted on a number of the insured's home devices.

Methods of home cyber crime

Protect yourself by knowing about some of the different ways cyber criminals carry out crime.

Viruses and malware

Malware is short for 'malicious software'; it is any software that invades computers or devices to carry out unwanted activity. They can be used to, for example, infect networks with viruses or steal information (passwords, log-ins, keystrokes, browsing activities, etc).

Hacking

Refers to an unauthorised attempt to gain access into networks and information systems. It can be done to obtain sensitive information and may lead to further fraudulent activity, such as identity theft or ransomware attacks.

Social engineering fraud

A broad term referring to scams used to manipulate and deceive a victim into giving out confidential information. These scams can be carried out online (e.g. through social media or emails) or on the phone, coaxing victims into giving out confidential information (such as passwords or bank details).

Phishing scams

The most common type of social engineering fraud, phishing scams typically target a large audience to get as many victims as possible to give out confidential data. Attacks are usually delivered in the form of malicious websites, or a mass email distribution pretending to be from a legitimate source.

Spear phishing scams

In contrast, a spear phishing attack is a type of social engineering fraud specifically targeted at the victim. The attacker may obtain their victim's private information by studying information available on the public domain (for example, Facebook or LinkedIn). They may then design an attack by impersonating someone the victim knows (e.g. an email from their Finance or HR department) and attempt to obtain confidential information such as their log-in details or passwords.

Authorised Push Payment (APP) fraud

Authorised push payment fraud (APP fraud) is a form of fraud in which victims are manipulated into making real-time payments to fraudsters, typically by social engineering attacks involving impersonation.

Denial of Service (DoS)/Distributed Denial of Service (DDoS) Attack

Deliberate paralysation of a targeted network by overwhelming it with data sent from one computer (DoS attack) or simultaneously from a number of computers (DDoS attack) so that the network crashes. Hackers can take over a household's smart home systems and utilise them to carry out a DDoS attack on a third party.

References and guidance

(1) The Crime Survey for England and Wales shows 1.674 million computer misuse offences against individuals and 533,000 domestic burglary offences were committed in the year to December 2020. Cybercrime includes all computer misuse offences, such as hacking and viruses. However, these are experimental statistics based on telephone interviews conducted between May and December 2020.

https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/june2017)

(2) https://www.ncsc.gov.uk/cyberaware/home

(3) https://www.ncsc.gov.uk/cyberaware/home

(4) Get Safe Online. https://www.getsafeonline.org

Disclaimer: The guidance in this document refers to industry best practice loss control advice. Adoption of the advice contained within this document does not imply compliance with industry, statutory or HSBEIL guidelines, nor does it guarantee that related losses will not occur.

HSB-LCE-RGN-018 Rev: 0 Date: December 2017

HSBEI-1846-0622-2

Picture credits: Getty Images

www.hsbeil.com

HSB

A Munich Re company