#InsuranceTips✓

Hello Easy broker

Smart homes offer convenience in terms of home automation, security, resource efficiency and commerce: from the comfort of your couch, you can control your lights and aircon, control your home security and order next week's groceries.

Central to this are two important elements: internet-enabled devices – including appliances and smart devices – and intelligent personal assistants (IPAs). An IPA is a virtual assistant that usually works using voice commands; popular examples are Apple's Siri, for its devices, and Amazon's Alexa, which is part of the company's Echo home automation system.

But any point at which your smart home system connects to the outside world – be it via an app on your smartphone, your WiFi or internet-enabled smart appliances – it makes you vulnerable to cybercrime. If you can access the internet, anyone with nefarious intentions can access you. All of you.

The risks you face include:

- **Identity theft:** if your smart home is hacked, you stand a very real risk of having your personal and banking information being stolen and used to commit fraud

- **Data breaches:** data has value, irrespective of the source. If you and your smart home are hacked, data about you (or your employer) can be stolen

- **Cyber extortion:** criminals can block access to your device or system and demand a ransom. They could even make your life a misery, such as locking you out of your house, randomly switching lights and appliances on and off, or even spying on you

- **Cyber liability:** hackers can potentially access company systems through employees' personal devices (cellphones in particular), for which you could conceivably be held liable

Don't think you couldn't be vulnerable. Cyber security firm Kaspersky reported in 2020 that not only has cybercrime continued to proliferate, but it has also responded and adapted to the global COVID-19 pandemic. For example, new strategies such as reselling bank access and targeting of investment applications emerged, and existing trends such as ransomware and card skimming became more sophisticated.

Kaspersky also predicted future trends to be aware of, including MageCarting (stealing payment card data from e-commerce platforms), transition currencies (using multiple cryptocurrencies to cover criminals' tracks while collecting ransoms), more cyber extortion with higher ransoms, using 0-day exploits (vulnerabilities not yet found by software developers), and fraud that demands Bitcoin payments.

Your home insurance should therefore contain a strong cyber section, with covers for eventualities such as theft of funds, identity theft, data restoration, cyberstalking, cyberbullying and loss of reputation, cyber extortion, third-party liability, and data and privacy breach by a third party.

Even if your data is compromised in a data breach, you need not be a victim. Here are four simple steps you can take to contain the risk:

1. **Change your passwords**
   It's a good idea to keep changing your password on a regular basis, but in the aftermath of a data breach, it's especially important to change your passwords to something strong, secure, and unique. And you should have multiple "passwords," not just one. Do not use the same password for all of your online accounts. In general a "strong" password is at least 10 characters with a mixture of letters, numbers, and symbols but there is a move to passphrases of at least 12 characters. A password phrase is a character string that consists of mixed-case letters, numbers, and special characters including blanks. Password phrases have security advantages over passwords as they are long enough to withstand most hacking attempts and are unlikely to be written down because they are easy to remember. An example of a strong password phrase is "**I LOVE to read andlivesecurely!**"

2. **Sign up for two-factor authentication**
   In addition to changing your passwords, sign up for two-factor authentication (also known as "2FA" or "two-step verification") wherever possible. This is an added layer of security for your account logins. With two-factor authentication, your online account will require you to enter an additional level of identification to access your account – such as a code texted to your phone. This means that even if

hackers get your email and password, they can't get into your account without that second factor of identity verification.

3. **Go to the Southern Africa Fraud Prevention Service (SAFPS)**
   Should you suspect that your identity has been compromised, apply immediately for a free Protective Registration listing with Southern Africa Fraud Prevention Service (SAFPS). This service alerts SAFPS members, which includes banks and credit providers, that your identity has been compromised and that additional care needs to be taken to confirm that they are transacting with the legitimate identity holder. Consumers wanting to apply for a Protective Registration can contact SAFPS on 011 867 2234 or visit **https://www.safps.org.za/**.

4. **Watch your accounts, check your credit reports**
   After a data breach, it's essential to be vigilant and pay extra attention to your account activity – that includes your bank account and other financial accounts. Read your bank account statements and watch for suspicious transactions. Also, sign up for your free annual credit report to check your credit reports from each of the three credit reporting bureaus – or better yet, sign up for a proactive monitoring service such as those offered by the bureaus, which will send you an alert if there is any activity on your credit record.

However, prevention is always better than cure. So, what steps can you take to protect your home, your data, and your digital security? There are several, such as …

… Creating a trusted ecosystem
What this means is that all devices on your smart home network are recognised and trusted, and any other devices cannot access the network. Use strong passwords along with encryption of your devices, install virus protection on all your devices and always be wary.

IPAs come with default access and “wake word” settings; as a matter of course, you should change them. Where these are available, add additional layers of security such as PIN codes, voice recognition and fingerprint reading.
Also, only ever give completely trusted apps access to your IPA.

… ‘Deafening’ your IPA
Essentially, smart devices and the IPAs used to control them are always listening for a command. That’s what makes them so convenient – and also so vulnerable. A good, low-tech way to counter this is to switch off your IPA’s microphone when not in use.

… Controlling banking access
Don’t link accounts to your IPA. Some home automation systems cannot recognise individual voices and will give bank details to anyone who asks – from criminals to your kids.

… Being careful in general
There are lots of other simple actions you can take to secure your smart home.
For example, don’t give strangers access to your smart devices, as social engineering is still the easiest way to hack you. Keep your smart home hub away from windows because you tip criminals off that you have one. Manage your online search and shopping histories; they can give away information about you.

Most importantly, speak to your broker about how best you can tailor your insurance cover for your smart home. It’s more than clever or prudent – it’s smart.

Kind regards

The Hollard Insure team.