prpl

SMART HOME SECURITY REPORT™ 2016

Research Findings

- *Smart device adoption has reached a tipping point - the smart home is already here*
- *The smart home is woefully insecure due to users' failure to follow best practices*
- *Smart home users prefer security to usability and are prepared to take more responsibility*

A prpl Foundation Study
September 2016

Executive Summary

Even just a decade ago few people could have predicted the impact the Internet of Things (IoT) would have on our lives. Networks of 'smart' internet-connected sensors and embedded computers exchanging information with each other may not sound particularly exciting to those outside the technology industry. But the use cases are virtually limitless.

From on-board aircraft guidance systems to driverless vehicles, and life-saving smart drug infusion pumps to smart city public safety systems, the IoT is everywhere. And it's making our lives better in the process. It has the power to make us happier, more productive, safer and even more healthy citizens. And from a corporate perspective it's even more developed – helping to make businesses more agile, while cutting costs and driving performance improvements and efficiencies.

But what about the IoT in a domestic context? Little research has been done on a large enough scale to uncover the level of penetration of smart devices in the home, and more importantly, the security implications. Are consumers aware of the risks of the connected home? What are they? How can they be mitigated? And will homeowners ultimately take responsibility for securing this new cyber domain, just as they would their physical front door?

The non-profit prpl Foundation set out to answer these questions and more in the following global report. For the first time ever, over 1000 consumers across three continents and six countries took part, to provide the kind of global insight into this world we've never had before. The findings should be food for thought for anyone with an interest in IoT and the security implications of the smart home.

Key findings

❑ The smart home isn't coming, it's already here. And device adoption in certain cases has reached a tipping point

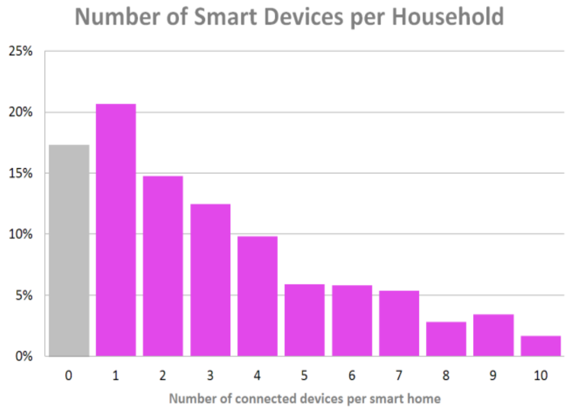
❑ The smart home is woefully insecure due to users' failure to follow best practices

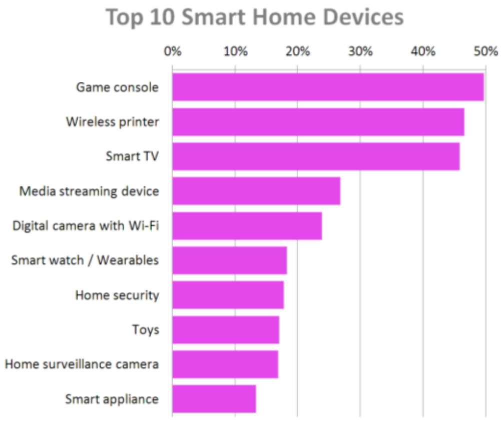
❑ Consumers prefer security to usability, and they're prepared to take more responsibility if it means living in a safer home

The smart home has reached a tipping point

The first thing we can say for sure is that the smart home has definitely reached that much-talked about tipping point. Only 17% of respondents claimed to have no connected devices in their home, which puts penetration of smart technology at an impressive 83%. And more than 47% of respondents claimed they had three or more devices in their home.

That's doubly impressive when one considers that we didn't include traditional computing devices such as laptops, smartphones and tablets on our list of smart home devices to choose. Games consoles, wireless printers and smart TVs were the most popular. Security concerns have been raised about all three over recent years. In the case of Smart TVs, researchers have not only demonstrated how hackers could infiltrate devices to steal credentials or spy on users but also install ransomware to extort money from the TV owner.





As these devices become more prevalent in the home, cybercriminals will inevitably follow the profits and turn their attention more fully towards them. At present connected cars are not in the top 10, but this category could also be targeted as time goes on.

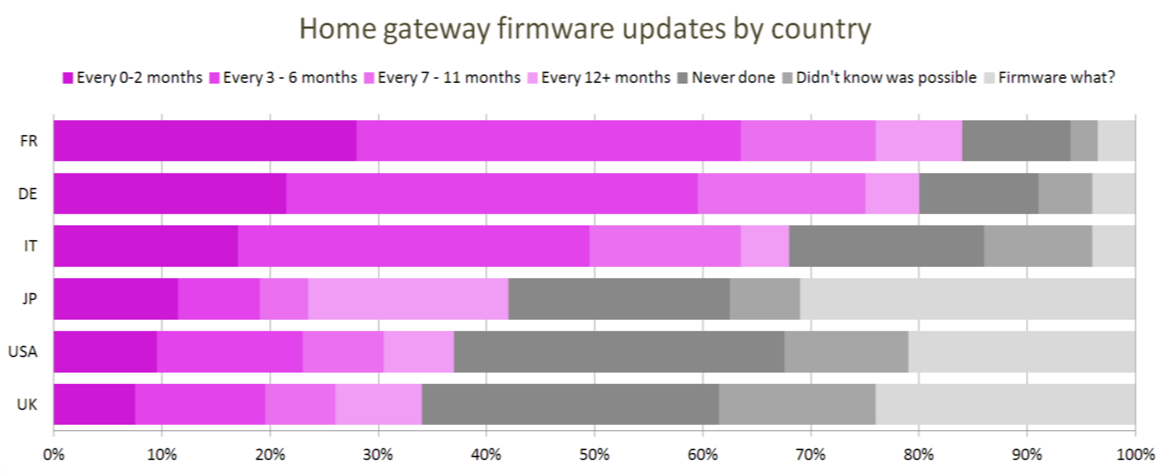
Geographically speaking, adoption of smart devices was strongest in the continental European nations of France (5.8), Italy (5) and Germany (4.5), with the UK (2.6) and US (2.4) around the same level as each other. Japan disappointed with an average of just 1 smart device per home. Despite the stereotype of the country as a hi-tech nation, perhaps this stat is a reflection of a rather more conservative society than many expect. It could also reflect the relatively elderly population less inclined to embrace technology.

Smart homes are not secure

So the smart home has most certainly arrived. But is it being secured? Unfortunately, the answer is a resounding “No!”

The equivalent of your front door in the cyber world is the home router. It is the conduit through which passes all of your domestic internet traffic from all over the world. But while no homeowner in their right mind would leave their physical front door open, many are doing the equivalent with their smart home by failing to take care of their router. Failure to patch vendor updates could leave critical vulnerabilities present which hackers can take advantage of to eavesdrop on traffic and hijack smart devices.

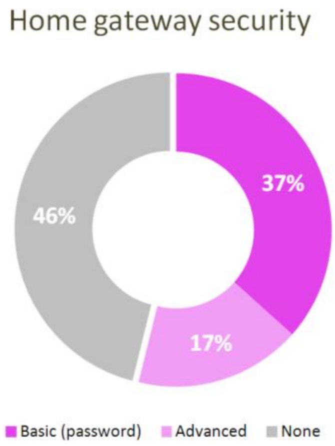
With IoT security we’re not just talking about data loss either. As some disturbing examples of smart device hijacking have already proven, this is also about the physical security of your family.

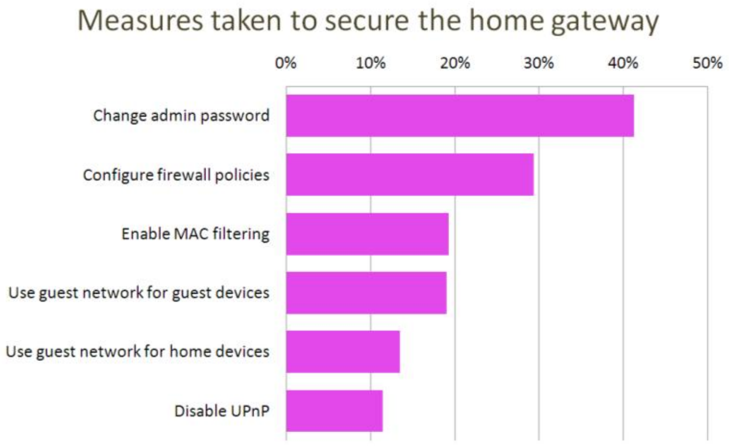


Over half of respondents (57%) said they updated the router firmware “at least once a year.” But shockingly, 20% have never done so, and 23% didn’t even know if was possible.

There was bad news for the UK – letting down its European neighbors dreadfully. In fact, over 20% of British respondents didn’t even know what firmware is – revealing a general ignorance about security best practice which can be seen to an extent in all regions. That figure was surprisingly highest (30%+) in Japan.

Respondents failed pretty alarmingly to fulfill anything but the most basic steps on our checklist of best practices for home router security (see below). Just a third (37%) said they changed the default password. Most alarming was the 46% who claimed to have carried out none of the steps needed to keep the bad guys out. Just 17% carried out some of the 'advanced' steps recommended below.


Home gateway security

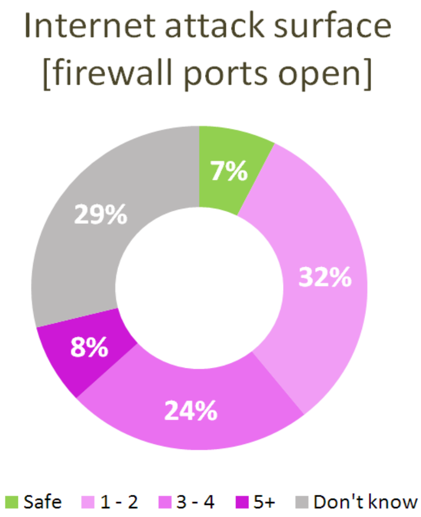

Measures taken to secure the home gateway

The UK once again shamed itself, with nearly 70% claiming to have taken no action to secure their router. Italy topped the list with over 80% carrying out some form of basic or advanced action.

Our findings also reveal that where there's a trade-off between security and usability, the latter sometimes wins. For example, of those 17% of advanced users, just over 10% claimed to disable UPnP. Although it's a security risk to the smart home, turning it off can make it harder to share digital content around the house. Similarly, only around 12% said they used a guest network for home devices. It will create "security by separation," but on the minus side for users means devices can't 'talk' to each other.

Firewall ports should never be opened. Yet users often think they need to be in order for their internet-connected home services to work. Service providers are failing them by reiterating this message. It's no surprise then that only 7% of respondents said they have no ports open. More worrying still, 29% don't know – highlighting once again a lack of engagement with security on the part of many smart homeowners.

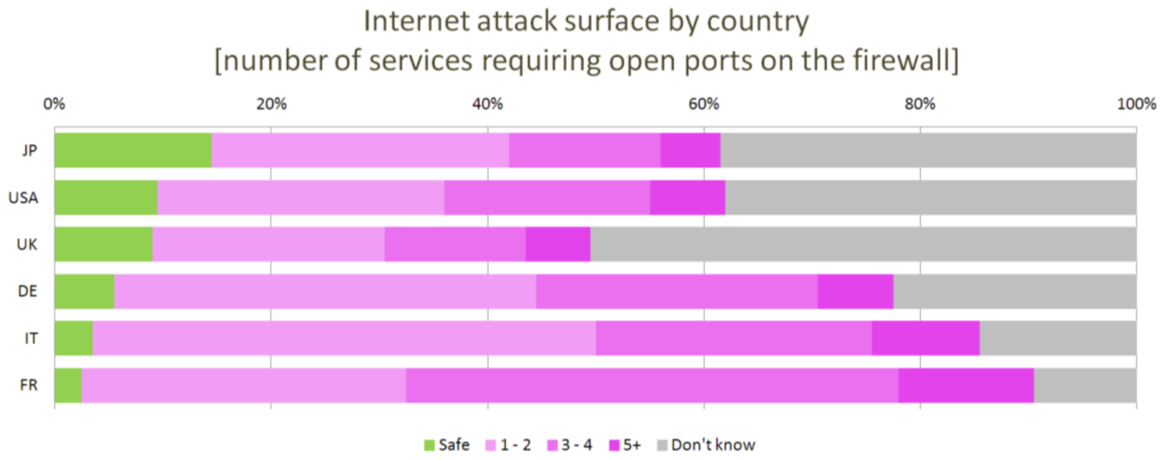
The Japanese here are doing best when it comes to firewall ports. And the European countries of France, Germany and Italy are worst performing. It's possible that Japan's tech users are more risk averse, with Europeans more ready to believe (incorrectly) they need more ports open to access more services.



Internet attack surface [firewall ports open]

Firewall ports should never be opened in a typical home installation. Listening ports are only required to access from the Internet server resources hosted in the home – not a common situation. Yet users often think they need to be in order for their internet-connected home services to work. Service providers are failing them by reiterating this message. It's no surprise then that only 7% of respondents said they have no ports open. More worrying still, 29% don't know – highlighting once again a lack of engagement with security on the part of many smart homeowners.

The Japanese here are doing best when it comes to firewall ports. And the European countries of France, Germany and Italy are worst performing. It's possible that Japan's tech users are more risk averse, with Europeans more ready to believe (incorrectly) they need more ports open to access more services.

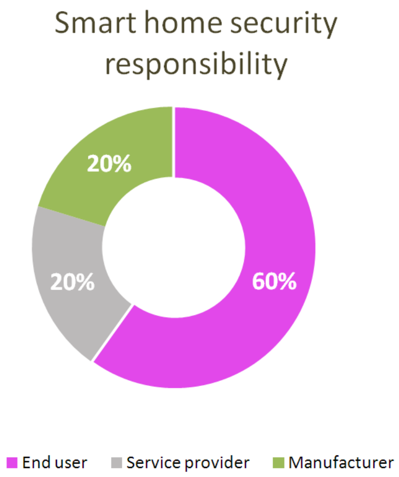


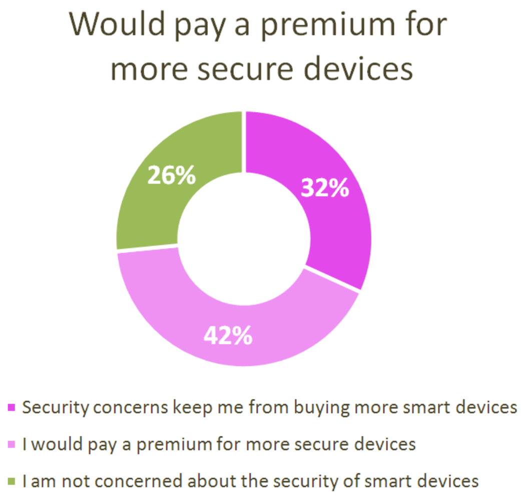
Internet attack surface by country [number of services requiring open ports on the firewall]

The misunderstood consumer

Consumer electronics makers have always acted on the basis that security interferes with usability – that it's commercial suicide to release more secure devices or systems which are slightly less user friendly. But our study shows that an overwhelming number of consumers would favor security over ease-of-use – with some opting for a happy medium where they can tweak kit themselves.

It's heartening to see consumer attitudes shifting somewhat, and something the IoT industry in general would do well to take note of. Interestingly, UK respondents are most keen on security – with close to 60% choosing this option.





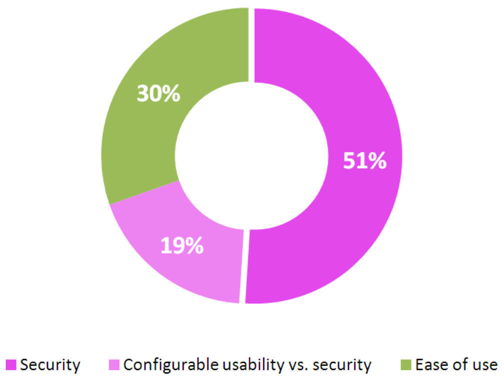
Users are also prepared to take more responsibility for security. Some 60% told us they think the home user should take ownership of securing their connected devices, versus the manufacturer (20%) and service provider (20%). Interestingly the UK is bottom of the pile here, with just under 55% of respondents feeling they have a responsibility on security. This could either be out of laziness, or because many trust their carriers more to carry out this role.

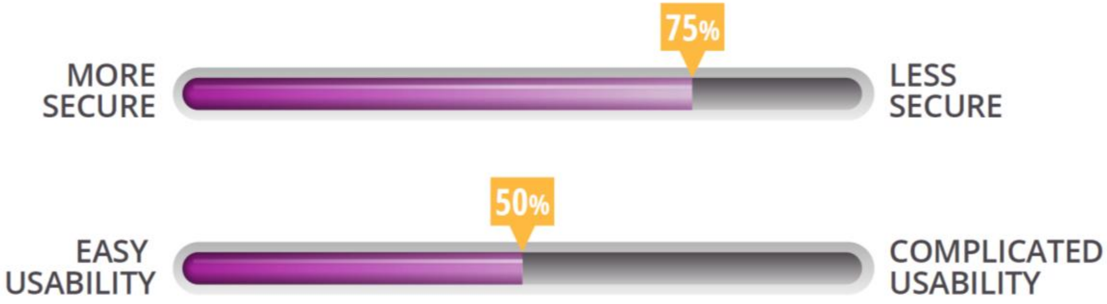
Finally, consumers would generally prefer to pay more for more secure devices (42%), and would buy if there was more secure kit on the market (32%) – turning on its head the old myth that security doesn't sell. Just a quarter (26%) aren't concerned about the security of devices, and we hope that number will reduce as awareness improves.

UK and Japanese consumers appear to be the least concerned about security at the moment. However, in the UK at least that's balanced out because more respondents than in any other country said they would buy more smart devices if they were more secure.

The key takeaway here is that security in the smart home shouldn't be a black or white issue. Think of security more as a "slider" which can be moved to the position that represents the right trade-off for a user's specific security vs. usability needs. For example, a wireless printer could be made more secure – if a little less 'convenient' – by using a USB to connect it directly into a PC. And by putting most of your home devices on the guest network you can achieve security by separation. It's slightly inconvenient but protects against malware targeting local IP addresses from inside the firewall.

Consumer choice - security vs. ease of use





Our recommendations below for users to improve the security of their smart home are not simply based around theoretical issues. For example, in October 2015 it emerged that attackers exploited a Netgear bug to change DNS settings on some devices, allowing them to snoop on users or even redirect them to malicious sites. Those failing to update the firmware would remain vulnerable. And in 2014 a Team Cymru report detailed how attackers could hack routers by using default credentials or brute-force password-guessing – stressing the importance of changing default router credentials.

Recommendations

We hope this report has offered some global insight into a still little known area of security: the connected home. It's clear from the respondents we spoke to that the smart home has most definitely arrived, and as devices get ever more pervasive we can expect cybercriminals to increasingly turn their attention towards them. What's also clear is that there's still a certain lack of awareness among consumers about exactly how to secure their smart homes.

But most importantly, consumers emphatically favor security over usability when given the choice, and in the main are prepared to both take responsibility and pay for it themselves.

From the railroads to aviation to automobiles, the history of man is littered with industries that had to learn the hard way before taking safety and security seriously. The message to the industry at large should be clear. It's time to get serious about smart home security and give our customers what they want. With consumers prepared to pay a premium for more secure products, the commercial argument that security doesn't sell simply doesn't stick any longer. Now is the time to take that next step and begin thinking of exactly how to design-in that much-needed security to protect smart home-owners, their data and their families around the world.

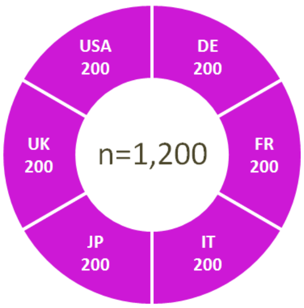
Top tips for better smart home security

1. Regularly check router firmware updates
2. Change default admin password on router
3. Configure firewall policies – close all ports
4. Enable MAC filtering
5. Use guest network for guest devices
6. Use guest network for all home devices
7. Enable wireless isolation
8. Disable DNS setting via DHCP
9. Disable USB file sharing
10. Disable UPnP

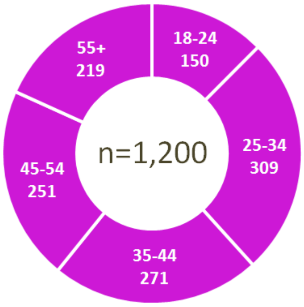
Survey Methodology

These online surveys of 200 UK, US, French, Italian, German and Japanese adults with Wi-Fi routers in their home was commissioned by prpl Foundation and conducted by OnePoll, in accordance with the Market Research Society code of conduct. Data was collected between 22.06.2016 and 01.07.2016. All UK participants in the survey are double-opted in to take part in research. They are paid per survey (the payment differing depending on the length/time taken). The non-UK surveys were carried out using the panel of OnePoll trusted research partners. This survey was overseen and edited by the OnePoll research team, who are members of the MRS.

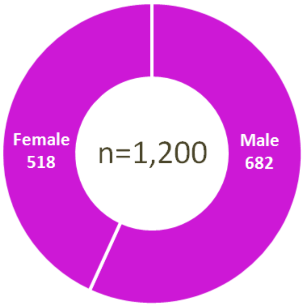
Sample by country



Sample by age group



Sample by gender



About the prpl Foundation

The prpl Foundation (pronounced "Purple") is a non-profit organization promoting the development of open source software for the Internet of Things. prpl represents leaders in the technology industry investing in innovation, portability and compatibility for the good of a broad community of developers, businesses and consumers - http://prplFoundation.org