

Putting trust at the heart of the digital home

EY annual survey of 2,500 UK households reveals consumer attitudes towards data privacy, protection and security.

We are immersed in the online world but there are signs of saturation

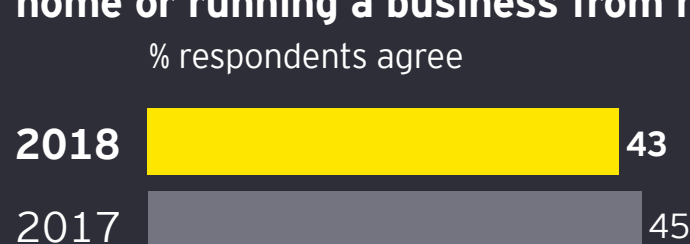
The proportion of households that see the internet as fundamental to their social lives has peaked

The internet is fundamental to my social life



We're seeing a downtick in the number of households that consider the internet critical to working from home

The internet is very important for my household for working from home or running a business from home

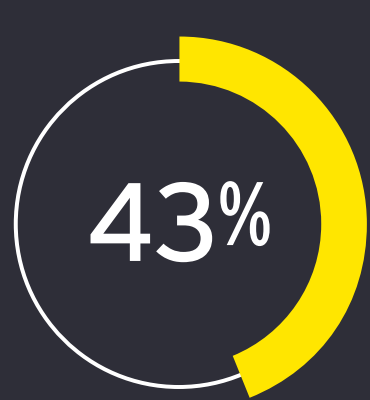


Data protection remains a critical concern despite new regulation – and many new households believe it's impossible to keep their data secure

New data protection regulation is now in place but awareness is limited and only 43% of households believe it will help



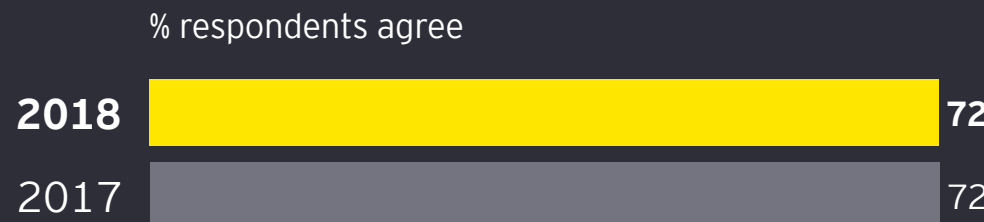
of consumers are **aware of 2018 data privacy regulation** and what this means for how their data is stored, managed and used



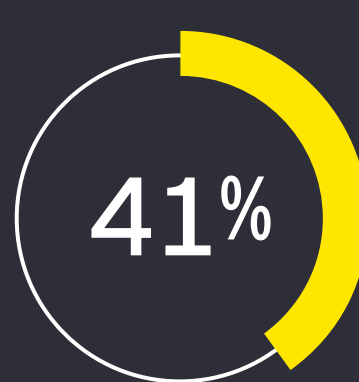
of consumers believe that the changes resulting from **GDPR will significantly improve the security of their personal data**

Online data disclosure remains an anxious activity for consumers, even if they are interacting with trusted brands

I am very cautious about disclosing personal details and financial information on the internet, even if the website is from a brand I trust



Many consumers have lost hope – four in ten households don't believe their personal data can ever be fully secure



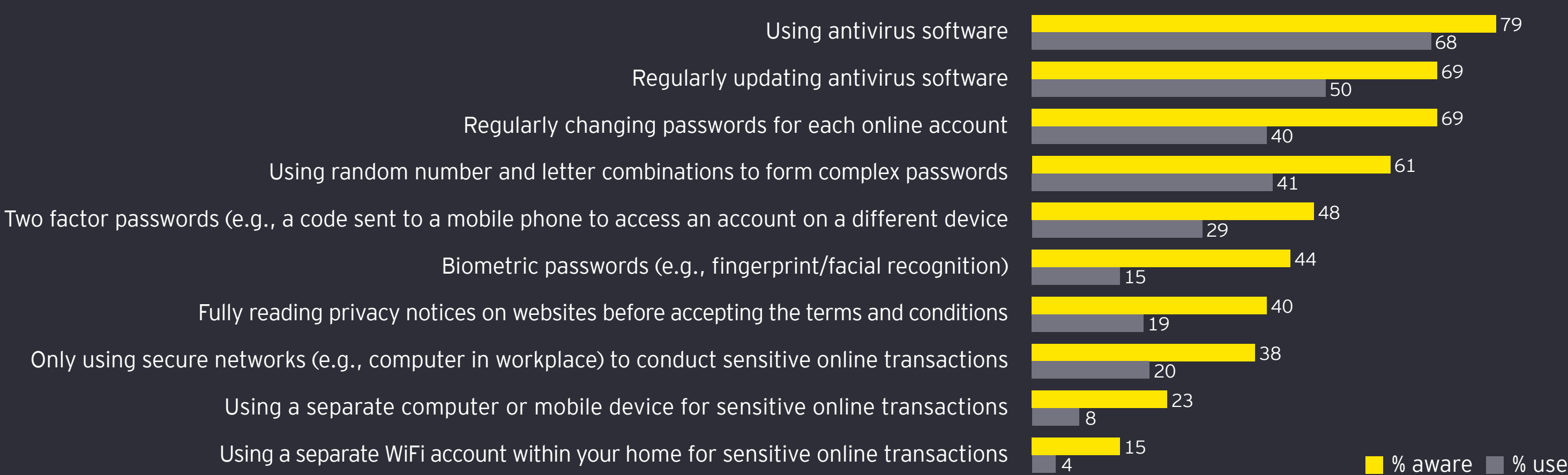
of consumers believe **it is impossible to keep their personal data secure** when using the internet or internet-enabled devices

There is a significant gap between awareness and actual usage of data protection best practices

Many households are aware of long-standing methods of protecting their data online, such as using and frequently updating antivirus software as well as changing and choosing more complex passwords

However, usage stands lower. Antivirus software aside, less than 50% of households use the methods cited in the survey. The gap between awareness and usage is particularly pronounced for newer forms of data protection, such as biometric passwords, while less than one in five consumers fully read privacy notices.

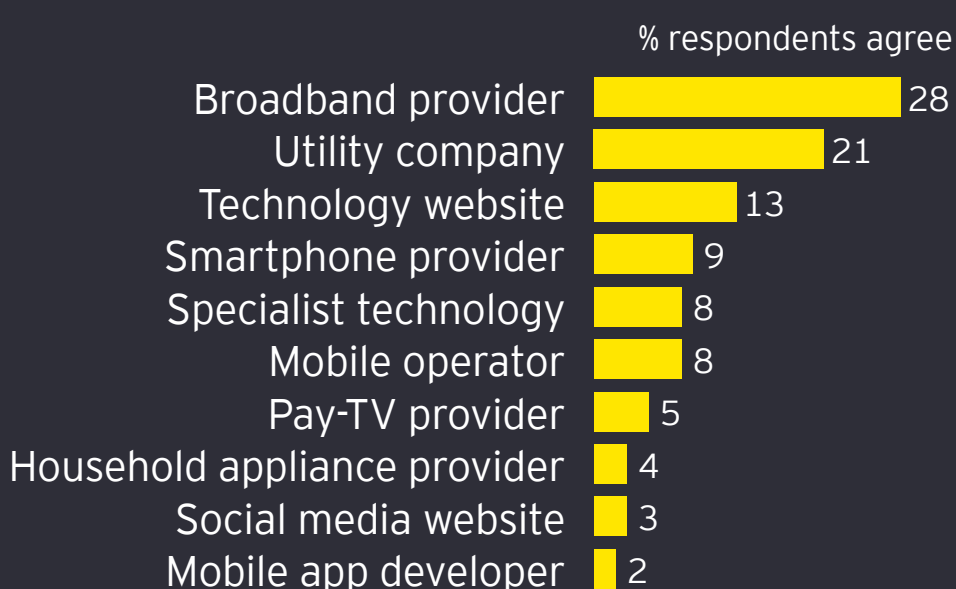
Which of the following are you (a) aware of as a method of protecting your data online and (b) is a method that you currently use to protect your data online?



Broadband companies rank ahead of other service providers as data custodians but genuine trust is still in short supply

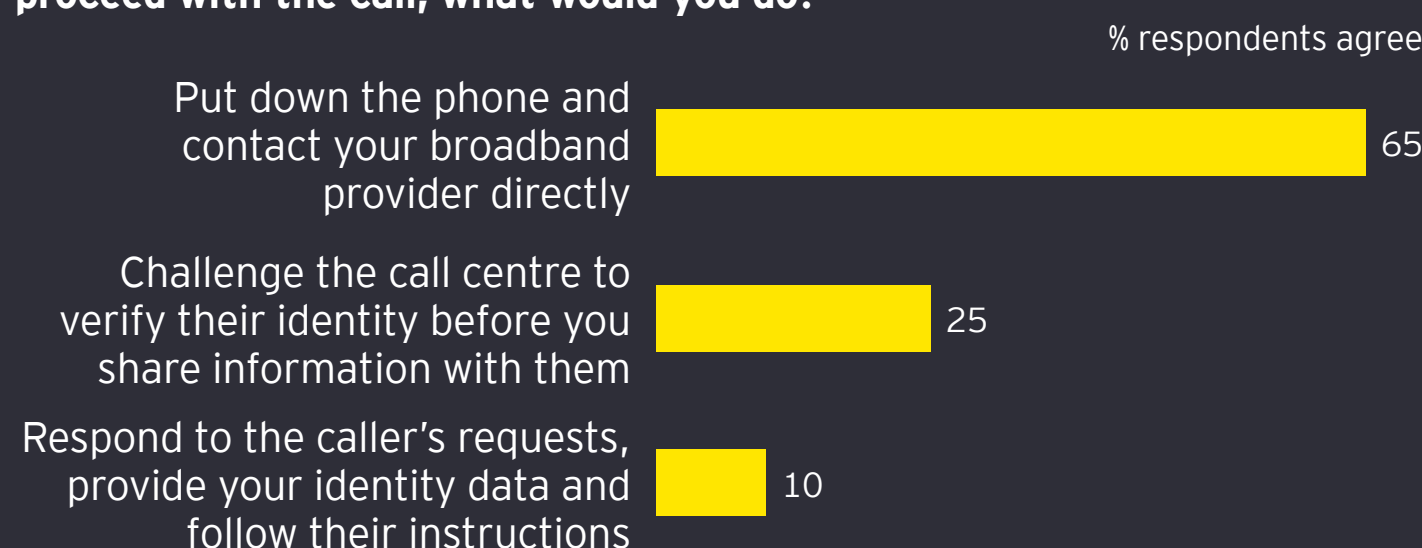
Twenty-eight percent of households view broadband companies as preferred data custodians among a range of entities. Other service providers rank further back, with social media platforms and mobile app providers the least trusted

Which of the following types of company do you think would best keep your personal data secure and use it appropriately?



Even so, just 10% of consumers would react positively if contacted by their broadband provider to provide personal details. This underlines a latent lack of trust that requires attention

If your broadband provider were to call you about a security issue and ask you to provide personal identification information before they can proceed with the call, what would you do?



What does this mean for TMT providers?

1
Put trust at the heart of all your customer interactions

Data protection and security is an overriding feature of consumer sentiment as they engage with the digital world. Ensuring that data privacy and security lies at the heart of your value proposition is critical. Educating customers is just as important as reassuring them, particularly given the gap between awareness and usage of the steps they can take to protect their own data.

2
Communicate about security with purpose, clarity and consistency

Clear and consistent communication at all stages of the customer journey, from discovery to purchase to delivery, is vital. This rigour is also essential as service providers interact with partners and their broader peer group. Common industry positions on ethical data management will become ever more important as the digital society matures.

3
Create an ethical innovation framework for your organization

Service providers should ensure that ethical data management drives their innovation agenda. "Security by design" should be an informing principle of all future products and services. For this to happen, service providers must build clear relationships between their customer and stakeholder interactions, and the innovation activities underway across their organizations.

For more insight into the digital home and how to serve it, please contact:

Praveen Shankar
EY UK&I Technology, Media and Telecommunications Leader
pshankar@uk.ey.com

Adrian Baschnonga
Lead Analyst, EY Global Telecommunications
Twitter: @Baschnonga
abaschnonga@uk.ey.com

Martyn Whistler
Lead Analyst, EY Global Media & Entertainment
Twitter: @MartynWhistler
mwhistler@uk.ey.com

Andy Edge
Assistant Director, Economic Advisory
Ernst & Young LLP
aedge@uk.ey.com