

White Paper



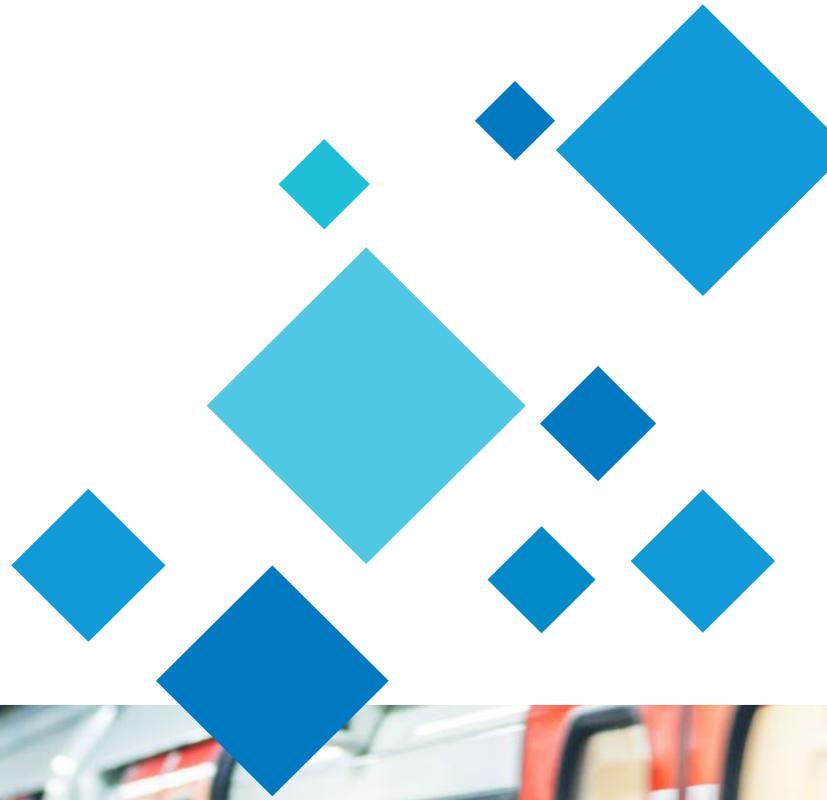
Circles of Trust: How the UK Public Perceives Digital Risk

Creating Trust in
the Digital Society

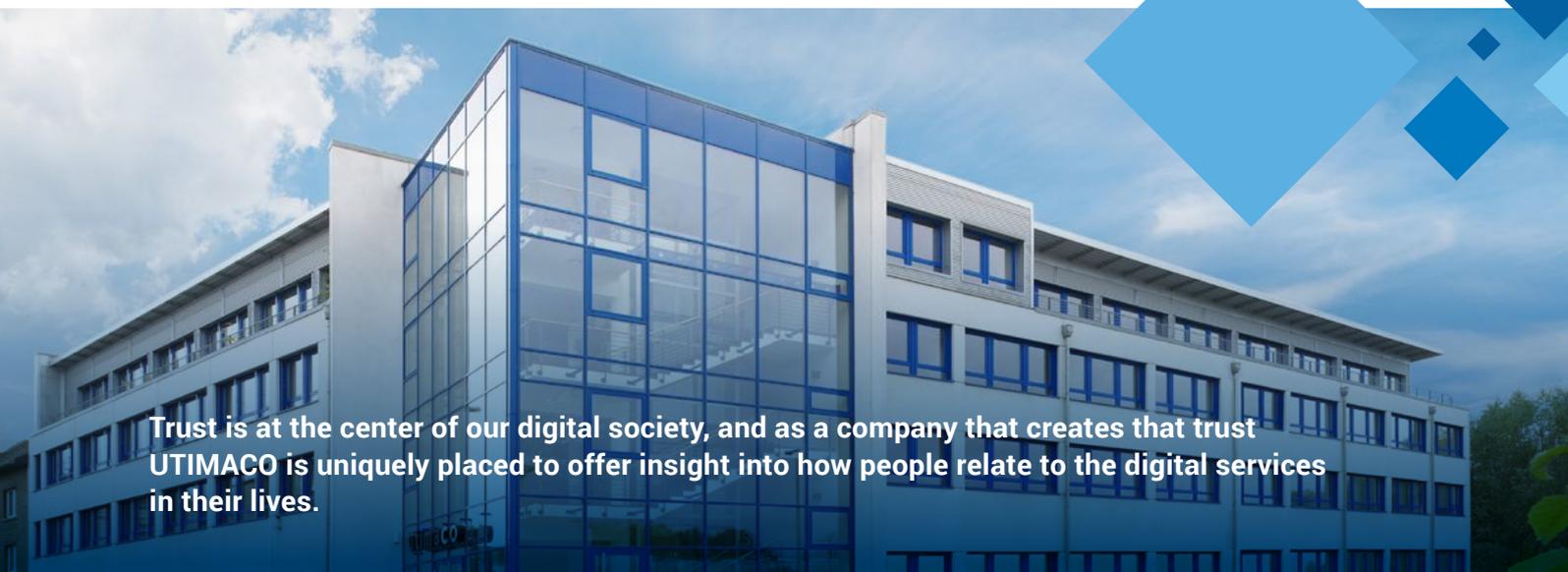
utimaco[®]

Table of Contents

- 3 Introduction
- 4 Summary
- 5 Trust in a Digital Society
- 7 Trust and Knowledge
- 8 Trust in Automotive
- 10 Trust in Healthcare
- 13 Trust in the Public Sector
- 16 Conclusion



Introduction



Trust is at the center of our digital society, and as a company that creates that trust UTIMACO is uniquely placed to offer insight into how people relate to the digital services in their lives.



For almost all of human history, the vast majority of interactions were conducted face to face, person to person. ‘Great Surveys’ like the Domesday Book represented early attempts to record and store what we would now call data, but they were inaccurate, incomplete and difficult to copy. Questions of who owns what and whether a person is who they say they are were settled with paper documents and wax seals.

Everything has changed in the last few decades. The capacity for gathering, transforming, and storing data has increased dramatically, so now each person with even the slightest online presence has a file on their activity stored at Google that is larger than the information gathered on the entire country when the Domesday Book was written. Combined with the information held on us by governments and the dozens or even hundreds of online services that the average person interacts with, our personal data footprints could extend into terabytes.

Living anything like a normal life in the modern world requires us to trust that the companies and government departments that hold data on us have our best interests in mind and are protecting that data from those who would misuse it. At UTIMACO, we have been at the forefront of providing the hardware and software that is used to secure data for several decades, all through this sea-change in the way human beings interact with the world. This means that we are uniquely placed to ask the question of whether people really trust the important digital services that they interact with.

Ansgar Steden
Chief Revenue Officer – UTIMACO



“ Our hardware and software are used to secure data for several decades, all through this sea-change in the way human beings interact with the world. ”

Summary

Surveying internet users across the UK, with other surveys carried out in Germany and Spain, we found a central paradox to life in the digital age: on the whole, people want to use digital technology in important areas like healthcare, driving and interacting with their government. They do not, however, always trust these digital services to keep their data safe or to be upfront about what this data is used for.

While these attitudes are contradictory, they are understandable. Using digital services is essentially mandatory: modern cars will have 'connected car' technology built in, communicating with your general practitioner (GP) usually takes place over email, and accessing several important government functions, like Universal Credit, can only be done digitally. We've become used to this, but despite the general lack of data leaks and other negative consequences of digitalization, the survey results show that worries still persist.

This indicates that governments and companies need to do more to communicate how their users are kept safe online and to work with security providers to build up top-tier defenses – a single breach could destroy any trust that has been built up.

We also find that there are noticeable differences between and within populations. As expected, we find that older demographics have less trust in digital technology, but surprisingly this is mirrored by the youngest demographic, the true digital natives. This could mean that younger users need to be won over with better explanations of how they are being kept safe, and that they need to be shown the value of digital services.

However, the overall results show a positive picture of trust in a digital age, although work needs to be done to match that level of trust to the enthusiasm the public has for digital services.



People across the UK do not always trust digital services to keep their data safe or to be upfront about what this data is used for.

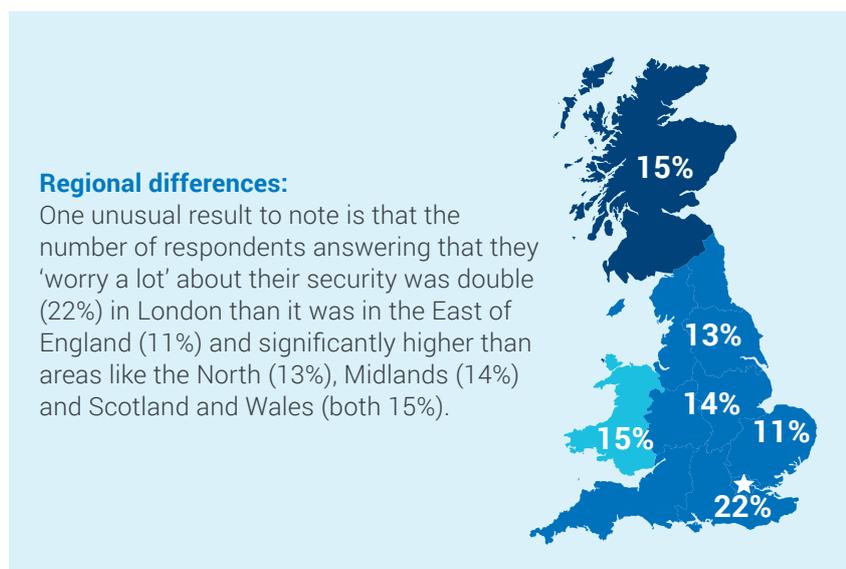
Trust in a Digital Society

The first and perhaps most important data point that the survey revealed was that **70% of people feel some level of worry about their data when using online services.**

How concerned are you about the security of your data when using digital services on the internet?

	Total	18-24	25-34	35-44	45-54	55+
I worry a lot.	16%	10%	11%	18%	21%	16%
	159	12	16	35	31	66
I worry a little.	54%	36%	55%	53%	54%	59%
	550	40	81	101	81	247
I don't worry much.	23%	33%	25%	22%	17%	21%
	229	37	37	42	25	88
I don't worry at all.	5%	10%	5%	4%	6%	3%
	47	12	7	8	8	12
Don't know / no answer.	3%	11%	5%	3%	3%	1%

The differences between men and women were negligible, with men reporting slightly higher confidence in general. Interestingly, when it came to education, respondents with post-graduate education and respondents with no formal education both reported higher than average levels of distrust. This could be explained by people with some level of education overestimating their own understanding (a phenomenon known as the Dunning-Krueger effect), while people with low levels of educational achievement correctly estimate their knowledge and people with high achievement also correctly understand that the issue is extremely complex.



What is more telling is the number of **people who have been affected by identity theft, data loss and fraud:**

Have you ever been a victim of data loss, identity theft or fraud online?

	Total	18-24	25-34	35-44	45-54	55+
Yes, and it was very damaging to me.	4%	1%	3%	4%	5%	4%
Yes, and it caused me little harm.	11%	6%	12%	15%	13%	9%
Yes, but it caused no harm.	13%	16%	18%	10%	15%	11%
I am not sure if I have been a victim or not.	16%	15%	19%	14%	20%	14%
Don't know / no answer.	3%	11%	5%	3%	3%	1%
No.	52%	50%	41%	49%	45%	59%
Don't know / no answer.	5%	12%	6%	7%	3%	2%



We find that over a quarter of people (28%) have been the victim of some kind of digital crime and an equal number (27%) don't know. We also saw a significant difference between London and the rest of the country, with only 45% of Londoners reporting that they haven't been the victim of cybercrime – though oddly Scotland reported the same figure. We also saw that respondents with STEM (science, technology, engineering and maths) educations reported less incidences of cybercrime than people with no higher education or higher education in humanities subjects.

Trust and Knowledge

One of our key findings is that a significant number of people don't know what information is collected about them online, even when every website will give them information on how cookies are used and therefore what information is being collected. Of course, social media sites and search engines have much more sophisticated and quite opaque data gathering operations, so it is quite likely that these are the sites that people are referring to when they say that they don't understand what is being done with their information.

Media stories over the last few years are also likely to play a part. The Cambridge Analytica scandal exposed how sophisticated non-state and para-state actors have become when it comes to using social media data, and highly-targeted fake news and disinformation remains a problem.

As with so much in digital security, the sheer amount of information that a person would have to sift through to have an adequate understanding of their own data footprint creates a vacuum that can be filled with misinformation and just-so stories (like the popular urban legend that social media sites are listening through your phone for you to mention brands and products, which they will then market to you).



Many people don't know what information is collected about them online.



How to fix the digital knowledge gap

Although we have seen that people are generally very positive about digital technology, we also see that they are often quite worried about their safety on these services.

Although the specifics of how each service works are complex and always changing, the ways in which they gather data and what it is generally being used for is generally quite standard. We can all see that if you search for 'camping equipment' or 'hair dye' it will soon start turning up in targeted advertisements. Beyond that, if companies are using data in specific ways, then they need to be upfront about it in ways that are clear to users.

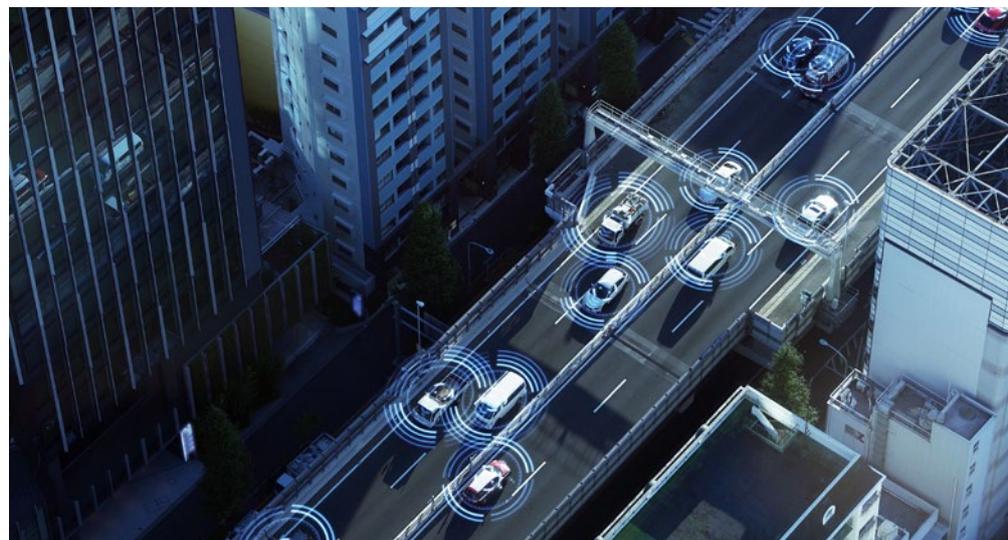
Trust in Automotive

In the last decades, vehicles have gone from having no connectivity technology beyond the radio and, in some rare cases, a mobile phone, to being data and telecommunication hubs with multiple ways to connect to the outside world for everything from emergency assistance to entertainment.



Today, cars can communicate bidirectionally with other systems outside the vehicle.

The first connected car was Cadillac's 1996 DeVille, which had simple cellular connectivity to allow drivers to access roadside assistance. Today even a budget vehicle can have dozens of systems, giving bad actors many ways into a system and creating an attack surface that can potentially be riddled with vulnerabilities. Despite connected vehicles being almost thirty years old, most drivers see their vehicles as being something that 'just works' instead of a complex collection of digital components that needs to be continually updated in the same way as a laptop or phone.



Attitudes towards connected cars

When it comes to digital technology in motor vehicles, we see a similar story emerge to the story of people's attitudes to digital technology overall: **they are enthusiastic about the benefits but wary of security risks, likely because of a lack of knowledge.**

Navigation / traffic news



Theft protection



Driver assistance



Parking assistance



Automatically paying at toll booths



Entertainment systems (music, videos, etc.)



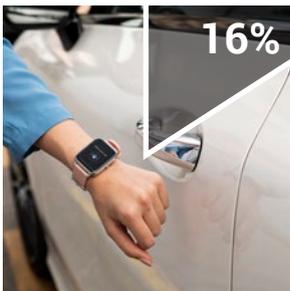
Predictive maintenance



Financial advantages based on user behaviour (i.e., insurance discount)



Connection to other devices



Other



None



Don't know / no answer



The most important stat in the chart above is that only 16% of respondents believe that there are no advantages to connected vehicles. As with other questions, this answer was most prominent among the youngest and oldest demographics: 18-24 year olds likely because they are less likely to drive than other demographics (only 35% of 17-20 year olds have a driving license); the 55+ group because they will have spent much of their driving life in 'analog' vehicles. Oddly, we also saw a significant spike in skepticism towards connected vehicles amongst Welsh respondents – 23% versus the average of 16%.



Only
16% believe
that there are
no advantages to
connected
vehicles.



When asked what they most worried about when it comes to connected vehicle security, the most common answer was additional costs for subscriptions to use digital services – with optional extras like the self-driving packages in Tesla vehicles costing as much as £6,800 this might seem like a valid concern. Coming in close behind with 43% of respondents reporting it as a concern was that of criminal attacks on vehicles, such as theft of payment data or even vehicle hijacking. Both are ‘black swan’ events that happen rarely, if ever, in the real world, but just as more people are worried about shark attacks than slipping in the shower, worries about them are powerful drivers of behavior. Only a tiny fraction of respondents believed that there would be no downsides to using connected vehicles – not a single person in the 18-24 demographic gave this answer.

There was a much higher rate of ‘don’t know’ answers to this question than others. Perhaps this simply reflects people who don’t drive and therefore have no opinion on the subject, but it may be that a large number of people still do not see their vehicle as a digital device, and this may be something that the automotive industry needs to change.

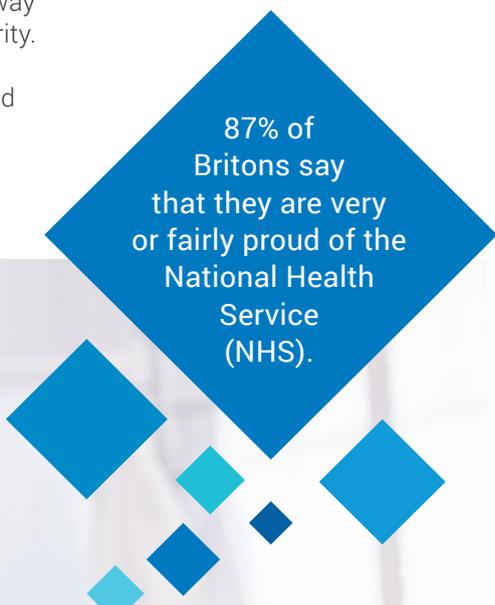
Trust in Healthcare

Since it is sometimes literally a matter of life and death, and since medical records are highly sensitive and personal, digital security in the healthcare sector is extremely important.

The COVID-19 Pandemic forced much of the UK's healthcare into digital spaces: instead of visiting their General Practitioner patients would contact them by email, video chat or phone. This caused some push-back in the press, although our survey shows that the majority of people across all demographics actually prefer accessing healthcare services digitally.

Although privatization is increasing, the UK's National Health Service is extremely popular. 87% of Britons say that they are very or fairly proud of the National Health Service (NHS) according to a YouGov survey¹, and although high levels of public satisfaction have slipped slightly during the pandemic², it remains high. This goodwill seems to have transferred to the NHS's digital services in the form of a high level of trust in the security of these services.

It is also important to note that while high-profile data leaks and hacks seem to be happening every day, the NHS has not been subject to any known breaches. Partly, this may be because there is not much in the way of a financial reason for doing so, but hopefully it is due to strong security. As with any service, consistent safety builds trust, and barring a major, well-publicized event we can expect healthcare to continue to be trusted even when the public is generally quite skeptical of digital services.



87% of Britons say that they are very or fairly proud of the National Health Service (NHS).



1 <https://yougov.co.uk/topics/politics/articles-reports/2018/07/04/nhs-british-institution-brits-are-second-most-prou>
2 <https://www.kingsfund.org.uk/publications/public-perceptions-nhs-2020>

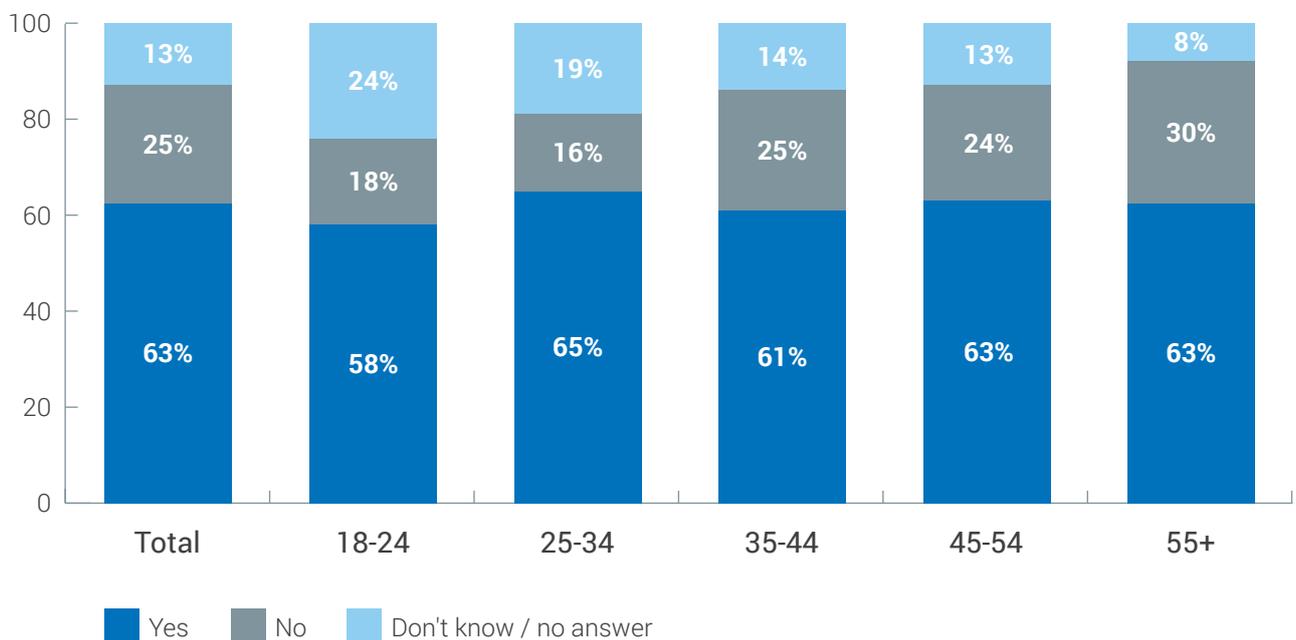
Trust in Digital Healthcare, by the Numbers

After nearly two years of almost-exclusive digital service for non-emergency healthcare and for many respondents a lifetime of increasing digitalization in healthcare, we have found that UK residents are on the whole very positive about continuing to use digital services.

63% of respondents said that given the choice they would use digital services to access healthcare when possible

Although this preference was strongest amongst the 25-34 demographic, results were remarkably uniform across all demographics and regions. As with other categories, the 18-24 cohort expressed the least outright positivity about digital healthcare, with 58% saying that they would use it, though this wasn't the result of actual negativity. In fact, it was consistent with a trend that was consistent across all age groups:

Given the choice, would you use digital services to access healthcare when possible?



As the chart shows, as respondents aged they became more polarized in their opinion on digital healthcare, with the number of 'don't know' answers diminishing over time and being replaced with outright nos. Does this mean that today's young people will start to distrust digital healthcare more as they age? Not necessarily: providing that the NHS's systems remain safe they should get used to it and the 'don't knows' will convert to yeses instead of nos.

What's up with Wales?

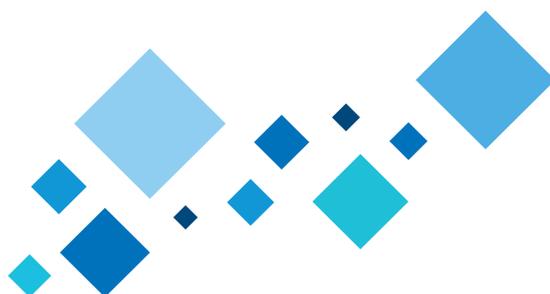
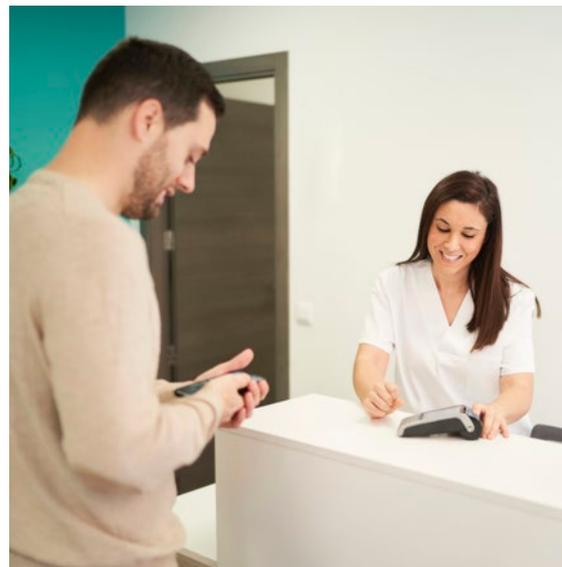
One seeming anomaly in the results is Wales – Welsh respondents reported far less enthusiasm for using digital healthcare services (45% answered that they would not use them if given the choice), that they didn't use digital healthcare services (34% gave this answer, as opposed to ~17% in other regions) and that there were no advantages to using digital healthcare (22% vs ~9% in other regions). This is likely down to the fact that many NHS digital services are not available in Wales, and the survey results show that with only a short amount of time using them that trust will substantially increase.

Why do people like digital healthcare?

The most common answer to this question is convenience. Digital 'appointments' don't require travel, don't require patients to take much time out of their day and can be 'booked' at any time. Digital prescriptions are similarly popular, especially in older demographics.

The number of people who outright reject digital healthcare is very low – 9% overall and 14% of the 55+ demographic. As before, this negative response grew as 'don't know' answers shrank, but as before there is every reason to believe that younger demographics won't become more distrustful as they age.

The main reason for disliking digital healthcare was the lack of human interaction, followed closely by the potential for security breaches. Although the former is inherent to the concept of digital healthcare, the latter concern can be addressed by communicating the security measures that the NHS takes and keeping patients secure with the latest technology.



Healthcare and Cybersecurity

Despite its importance, the systems for logging into NHS websites are fairly similar to those used for eCommerce sites: a username, password and usually a form of two-factor identification such as a PIN sent to a user's mobile.

46% of respondents consider the information that they send to their healthcare provider to be secure

As mentioned, there has yet to be a major breach in NHS cybersecurity, so there should be no reason to consider it insecure except for a general unease with digital technology. That feeling seemed to be quite powerful: despite the level of trust in the NHS and enthusiasm for digital services, trust in the security of those digital services never peaked above 50% across the age ranges surveyed.

Again, the youngest respondents reported the highest level of uncertainty (28%) versus the oldest (15%), with outright negative answers rising as respondents aged.

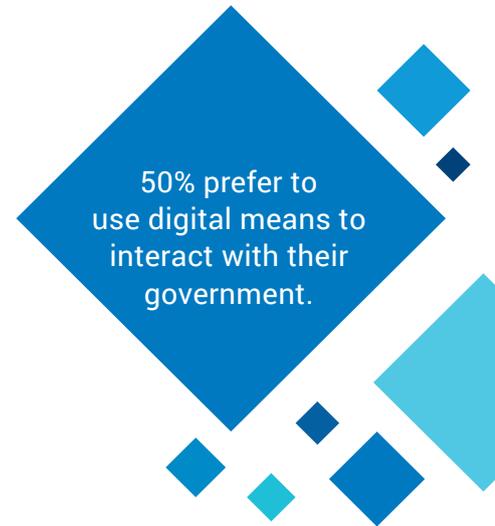
People still trust the NHS more than private healthcare providers

Although there is a perhaps unwarranted lack of trust in the NHS's cybersecurity, respondents were much less comfortable with sharing healthcare information digitally with companies outside of the NHS. Only one fifth (20%) of people across all demographics answered that they would allow their information to be shared with third parties, and as with other answers this reticence increased with age, with the 'no' answer going from 48% for 18–24-year-olds to 71% in the 55+ demographic.

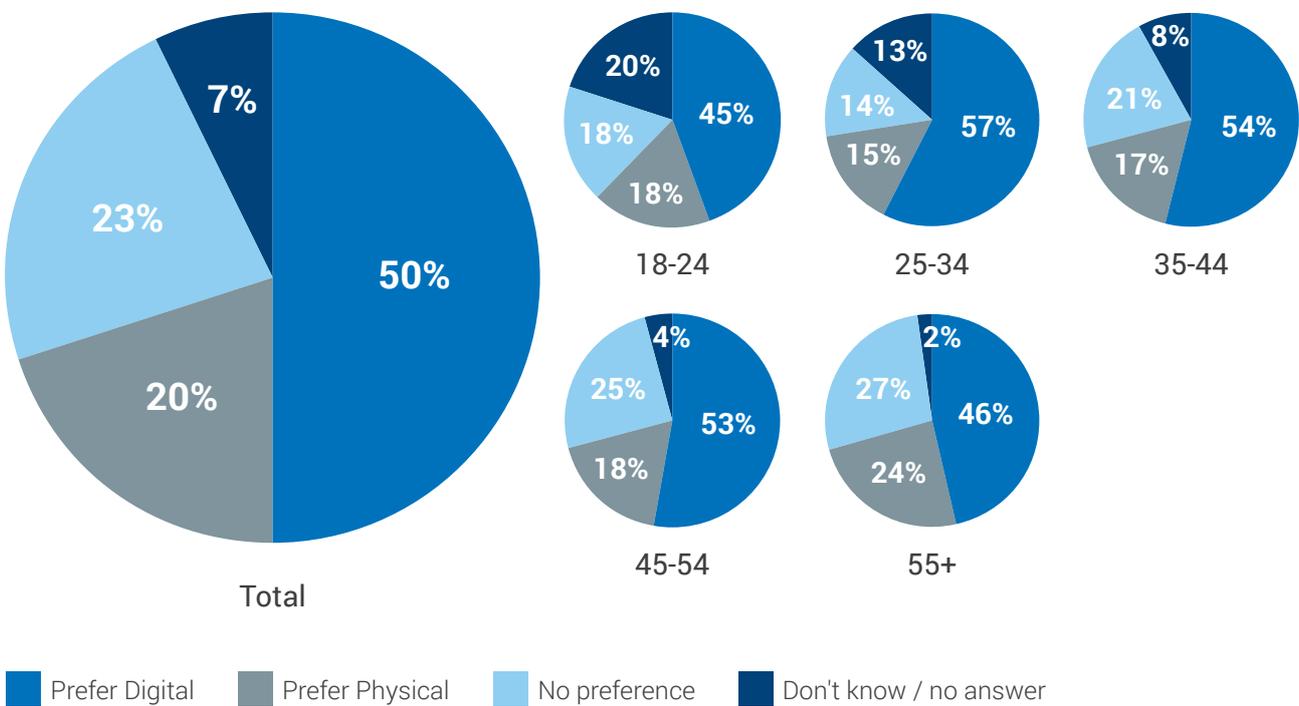
Trust in the Public Sector

Alongside healthcare, a person's interactions with their government are extremely important to keep secure. Governments hold information on a person's finances, criminal history, health, immigration status and a wealth of data that bad actors could use for identity theft.

However, much like the NHS, the UK government has not been subject to any major security breaches, and we can assume that the data given to them when filing taxes or applying for Universal Credit is extremely secure. This fact does not stop a significant number of people from worrying about their security: around a third of respondents (32%) say that it is not secure and another third (31%) don't know. These answers hold steady across age groups, regions and educational achievement.

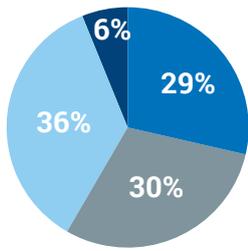


Most people like interacting with their government digitally

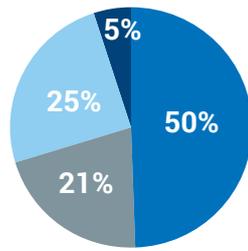


The survey results show that 50% of respondents prefer to use digital means to interact with their government and a further 23% have no preference. Considering how many government services have digitalized over the past decades, in practice this will mean that 73% of people will be perfectly happy using digital services.

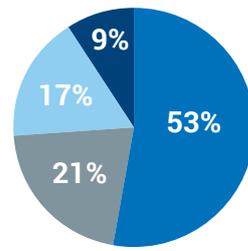
As can be expected, preference for physical interactions with the government increases with age, but this increase isn't huge: 18% for 18–24-year-olds compared to 24% for 55+ year olds, a difference of only 6%. As before, certainty also increased with age, with 'don't know' answers dropping from 20% to 2% from the youngest to oldest demographics. There was also a significant difference in answers when education is factored in: only 29% of the small cohort that answered that they had no formal education wanted to use digital services to interact with their government, compared to 62% for people with post-graduate STEM training.



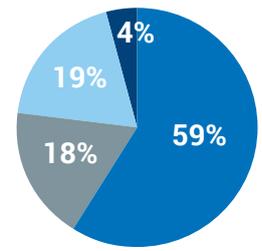
None



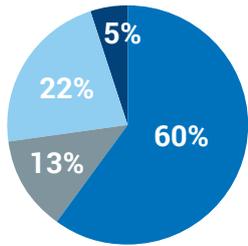
GCSEs/A-levels or equivalent



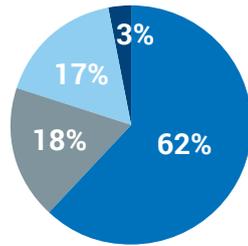
University degree in a humanities subject



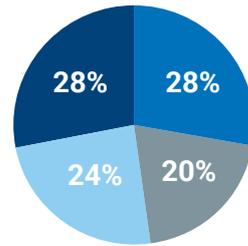
University degree in a STEM or vocational subject



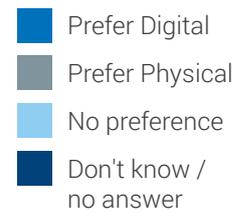
Post-graduate degree in a humanities subject



Post-graduate degree in a STEM or vocational subject



Other



Despite the NHS being literally a part of the UK's government, 13% more people overall prefer to use digital healthcare services than digital methods of interacting with the public sector. This is despite the fact that there is a clear reason for many people to prefer in-person healthcare – it's far easier for GPs to notice health problems in person than other email. This largely reflects the fact that many interactions with the NHS are positive, in which they receive free healthcare, and interactions with the public sector are largely negative – paying taxes for instance. There is also the broader question of whether people trust 'the government' versus whether they trust the NHS.



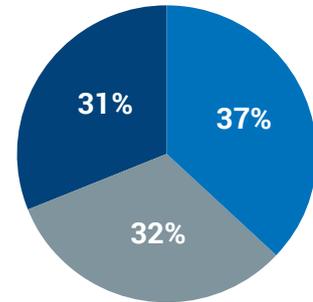
Security in the Public Sector

The most common objection to using digital services to interact with the UK government is the potential for security breaches – 61% overall. This worry increased substantially as respondents aged, from 43% in the 18-24 demographic to 68% for the 55+ demographic. As with similar worries about data leaks from the NHS, this is despite a total lack of major leaks of data from the UK government and a lack of financial motive for anyone to attempt the very difficult feat of accessing information from the HMRC or DWP.

However, it is important to stress that these worries are only potential downsides to digitalization, and that many people either believe that their data is safe or have no opinion either way. Unlike other sectors, there was not a major difference between UK regions, although Wales did exhibit a lower level of trust than other parts of the UK, possibly due to the relative lack of digital services there.

Although this lack of trust might be concerning, a significantly smaller number of people trust companies outside of the UK government to take other government functions digitally. Only 20% of people would trust a private company with their data – having their tax return sent to a contractor to be processed for example. Privatization is a fraught issue in the UK, and the figures show that most people are as opposed to privatization of government functions as they are to the NHS.

Do you feel that the information held about you by the UK governments is secure against third parties?



- Yes
- No
- Don't know / no answer

People are hesitant to use digital services to interact with the UK government because of potential security breaches.



Trust in other countries

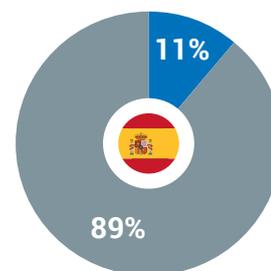
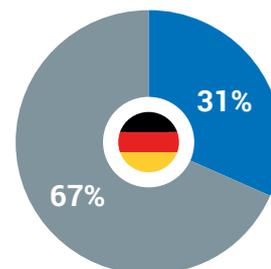
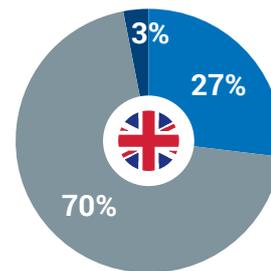
As a company with a global reach, UTIMACO was able to carry out similar surveys in Germany and Spain. Since both of these countries have different systems for healthcare and government services, we couldn't carry out an 'apples to apples' comparison of trust, but what we could do revealed some very important insights.

The UK is more trusting than other countries

The first and most notable result was that the UK showed significantly greater trust in digital technology than Spain and roughly equal trust to Germany. Although all countries gave similar answers when reporting whether they had been a victim of cybercrime, Spanish respondents were 20% more likely to report worrying about digital safety, with 89% of respondents saying that they were concerned about the security of their data. The UK's respondents were also significantly more likely to report that they were knowledgeable enough to make informed decisions about their digital security and slightly more likely to report that they have not been a victim of digital crime – though they were more likely to say that they didn't know what information was being gathered about them online or what the data collected by a connected vehicle is used for.

Why is this the case? One explanation could be the cultural proximity and lack of language barrier between the UK and the USA. Although innovations in technology happen across the world, there is still a general perception that the locus of digital technology is in Silicon Valley. This means that countries that can easily absorb US news and culture are going to come to resemble it, and the enthusiastic and yet paradoxically paranoid attitude is certainly reminiscent of the technology news coming from the US, where major companies can promise that they are creating the future one day and will be exposed for harvesting data the next.

Another factor could be historic experience, as both Spain and Germany have been dictatorships within living memory, so they are likely to be skeptical of the kind of mass-surveillance technology that makes those regimes possible. The self-reported lack of knowledge may be a function of this proximity, in which having access to more first-hand information about digital technology simply shows how much there is still to know.



Trust in digital services is very homogeneous in Europe.

Digital trust is surprisingly uniform across Europe

However, the similarities far outweighed the differences. Despite significantly more skepticism in Spain, most results clustered closely together, and Germany and the UK gave nearly identical answers to many questions. It would seem that digital culture is fairly uniform, and that many countries are experiencing the same rapid digitalization, with the attendant worries about safety.

Conclusion

At the core of the answers was a central problem for any organization that provides digital services to the general public: people want to use digital technology but they are worried about the security implications.

How can we solve this problem?

Firstly, telling people that they are simply overreacting to cybersecurity threats is not going to be an effective approach. Not only is it likely to be rejected, but there are also legitimate reasons to worry about security when using digital services. We have seen during last years 'summer of ransomware' that professional, organized and innovative criminal groups are perfectly capable of carrying out attacks on major institutions, including the US State Department. Just because a major data breach hasn't affected a large car manufacturer, the NHS or the UK government yet, doesn't mean that it can't happen. We should be encouraging people to take security seriously.

Our recommendations are twofold:

1 Arm people with the information that they need to make effective decisions about their security. This involves dispelling long-standing myths about 'hackers' and showing people that even the biggest security breaches are caused by re-used passwords, misconfigured security settings or simply answering the wrong email. An awareness of what social engineering is and how it works would go a long way to showing the public that the threats they face are more likely to come from clicking a link than the services they use being compromised.

This also means being upfront about the data collection that your company performs and the security that you use to keep customers safe. We have seen how agreeing to tracking cookies when visiting a new website has become the standard in a short time, though many people consider them a nuisance, and it may be that this system can be further refined to explain what is being tracked and what an organization is doing to keep its customers safe.

2 Building up digital defenses so that these kinds of major breaches don't occur. All this education will be for naught if a large-scale and well-publicized data loss occurs, or if car owners start their vehicle one morning to find a demand for bitcoin to start their engine. This means doing the difficult but necessary work of creating and maintaining security systems that can stand up to evolving threats.

UTIMACO has been at the heart of many companies and governments digital security for decades, and is vital in creating the 'root of trust' that assures the public that they are safe online. Our cybersecurity solutions underpin the cryptographic security in many of the world's most demanding security environments, so if your organization is trying to develop a security solution that can stand up to 21st century threats then we are an ideal partner.



About UTIMACO

UTIMACO is a global platform provider of trusted Cybersecurity and Compliance solutions and services with headquarters in Aachen (Germany) and Campbell, CA (USA).

UTIMACO develops on-premises and cloud-based hardware security modules, solutions for key management, data protection and identity management as well as data intelligence solutions for regulated critical infrastructures and Public Warning Systems. UTIMACO is one of the world's leading manufacturers in its key market segments.

500+ employees around the globe create innovative solutions and services to protect data, identities and communication networks with responsibility for global customers and citizens. Customers and partners in many different industries value the reliability and long-term investment security of UTIMACO's high-security products and solutions.

Find out more on utimaco.com



Headquarters Aachen, Germany



Headquarters Campbell, USA



Contact us



EMEA

UTIMACO Management GmbH

📍 Germanusstrasse 4
52080 Aachen,
Germany

☎ +49 241 1696 200

✉ info@utimaco.com

Americas

UTIMACO Inc.

📍 900 E Hamilton Ave., Suite 400
Campbell, CA 95008,
USA

☎ +1 844 UTIMACO

✉ info@utimaco.com

For more information about UTIMACO® products, please visit:

utimaco.com

© UTIMACO Management GmbH 06/22

UTIMACO® is a trademark of UTIMACO GmbH. All other named trademarks are trademarks of the particular copyright holder. All rights reserved. Specifications are subject to change without notice.

Creating Trust in
the Digital Society

utimaco®