mailock

The Consumer Knowledge Gap: An Analysis of Email Security

CYBER ESSENTIALS CERTIFIED PLUS

British Assessment Bureau UKAS MANAGEMENT SYSTEMS 0289 ISO 27001 INFORMATION SECURITY MANAGEMENT

Crown Commercial Service *Supplier*

Beyond Encryption

Personal data is an essential part of our digital identities. Transacting with businesses online requires us to share our personal data to prove ‘we are who we say we are’. However, with cyber threats rising, protecting our data is becoming increasingly challenging. Frequent and high-profile data breaches suggest that not enough is being done to make sure our data is exchanged securely.

Email, in particular, has become a major concern. Despite email being unsecured in nature, it is used for transactional and interpersonal communications on a global scale. One would assume that this would lead to a great awareness of email’s risks. Yet, email is continually reported as the leading cause of data breaches. The evidence shows that an alarming number of individuals and businesses share personal data via email, including highly sensitive information such as passport and bank details.

Are people unaware of the dangers? Or are they simply ignoring the risks? This report sheds light on the current state of consumer email security practices to help businesses understand how to enable communication that protects their customers’ data. The results demonstrate that there is still much work to be done in terms of educating consumers about email security and the importance of protecting their data.

As a society, we need to ensure that we are doing everything we can to protect our personal information. It's not just the responsibility of consumers to keep their personal data safe, but also the responsibility of businesses to provide secure methods of communication for customers to interact with them. Only by working together can we ensure that data is kept secure from risk.

Paul Holland
CEO and Founder of Beyond Encryption

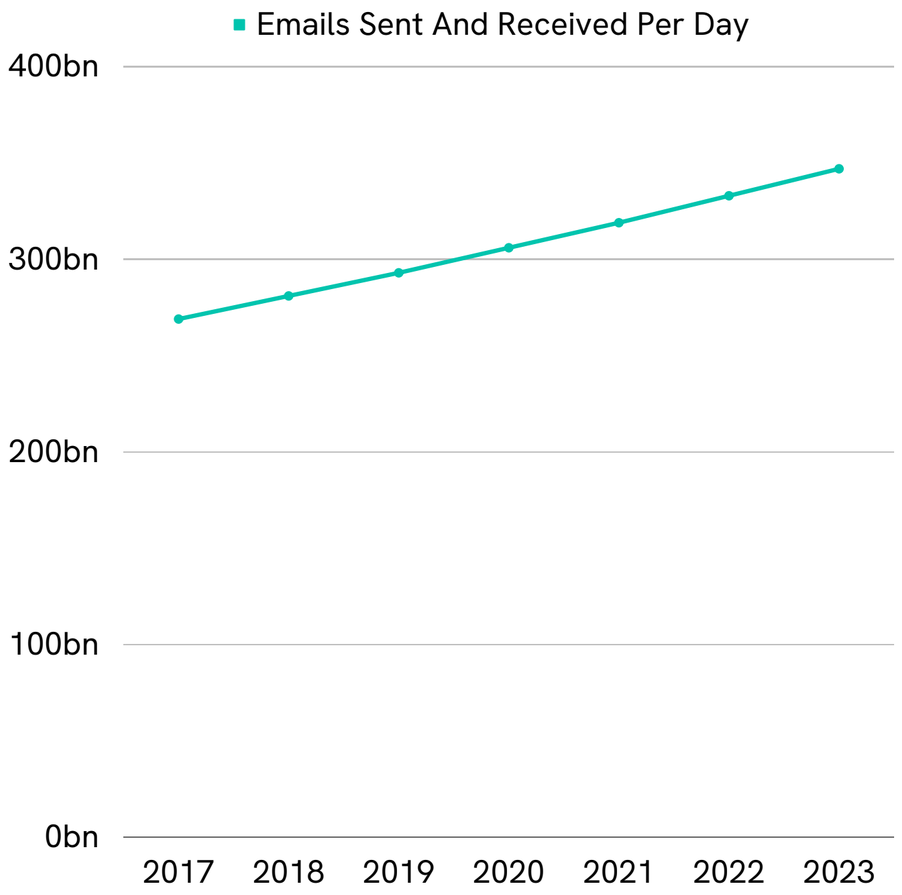
Contents

Introduction

In the past few years, there has been a significant shift towards digital services, which has brought about a rapid evolution in business communications. As organisations increasingly rely on digital communication tools to exchange information with their customers, partners, and employees, they face a number of challenges, including heightened cyber risk.

Cybercriminals have taken advantage of this surge in online communications, with phishing scams, malware attacks, and other malicious activities rising. Cybersecurity has become essential for both businesses and individuals to protect their data and take responsibility for their online identity.

With an estimated 347bn messages sent and received each day, email is the most common online communication tool used for personal and professional purposes. However, while it is a convenient way to send and receive messages, it is inherently unsecured. Are consumers aware of how easily their emails could be intercepted? Are they doing what they should be to stay protected?



Source: Statista

Overview

This report presents the key findings of a survey conducted to explore UK consumers' knowledge and behaviour towards email security threats. The research reveals insights into consumer awareness of email security threats, communication preferences, and sustainability concerns. The effect that generational and other demographic divides have had on the findings is considered.

The results show a significant disconnect between an individual's email security awareness and the reality of their actions. Some individuals lack a basic level of email security awareness but believe themselves to be educated on the dangers. Nearly ¾ of UK adults believe they are knowledgeable of the risks they face when using email but do not take necessary precautions to protect their data. This risk is exacerbated by businesses, with 73% of consumers having been asked by a professional services provider to share personal data over email.

Methodology

Beyond Encryption partnered with 3Gem Media Group, who surveyed 2,000 UK adults between the 17th-20th February 2023. Quotas were applied to age, gender & region, to ensure the sample was representative of all UK adults, aged 18+ years old.

Key Findings

More than

1/2

of consumers have shared personal data over email.

3/4

of UK adults feel that they are knowledgeable about cybersecurity threats.

73%

of consumers have been asked by a professional services provider to share personal data over email.

1/4

UK adults have accidentally shared personal data via email with the wrong recipient.

7 in 10

UK adults feel that businesses should **decrease** their postal communications to reduce their carbon footprint.

27%

of respondents said that they feel email is protected and secure.

Perception vs. reality

Personal data (otherwise commonly referred to as personally identifiable information) is data that, when used alone or with other relevant information, can identify an individual. It is vital that personal data is safeguarded to protect peoples' identities from fraud and theft. But are consumers aware of the threats against their data? And are they taking the proper precautions to keep their data safe?

Our research reveals that there is a significant disconnect between an individual's perceived cybersecurity awareness and the reality of their actions. Nearly ¾ of UK adults (73%) feel that they are knowledgeable about the cybersecurity threats they may face online, such as phishing scams, malware, and password attacks. When questioned further, results show that 6 out of 10 UK adults (65%) feel very or quite confident that they can identify a phishing scam.

However, less than half (45%) of respondents feel that they have an understanding of the term 'end-to-end encryption' and 13% have never heard the term before. With encryption being one of the key methods in which businesses and consumers can protect sensitive information when transmitted online, this reduced understanding is concerning.

3/4

of UK adults feel that they are knowledgeable about the cybersecurity threats they may face online

85%

of consumers believe they take care to protect their personal data from online threats.

ARE CONSUMERS PROTECTING THEIR PERSONAL DATA?

Perception vs. reality

When putting cybersecurity knowledge into practice, the majority of respondents (85%) believe that they take care to protect their personal data from cybersecurity threats when online. Yet, when drilling down into the common methods by which individuals can protect themselves, the responses show a firm disparity between how consumers feel and the actions they are taking.

Nearly a quarter of UK adults change their most commonly used online passwords at least once a month, despite NCSC guidance stating that frequent password changes leave individuals open to increased risk. This is because users who change their password frequently will often choose a ‘weaker’ one that is memorable.

Only a third of participants update the antivirus software on their devices at least once a month, with 13% sharing that they don’t use antivirus software at all.

ARE CONSUMERS PROTECTING THEIR PERSONAL DATA?

The problem with email

Email was never created to be secure, and any information transmitted within this channel is at risk of being intercepted or accessed by third parties, placing individuals and their identities at risk. Are consumers aware of the dangers, and are they comfortable using email to share their personal data?

According to survey results, over a quarter (27%) of respondents say they feel email is protected and secure (73% are aware it is unprotected). Yet, over half of consumers share personally identifiable information via email, with 55% of these having done so within the past 3 months.

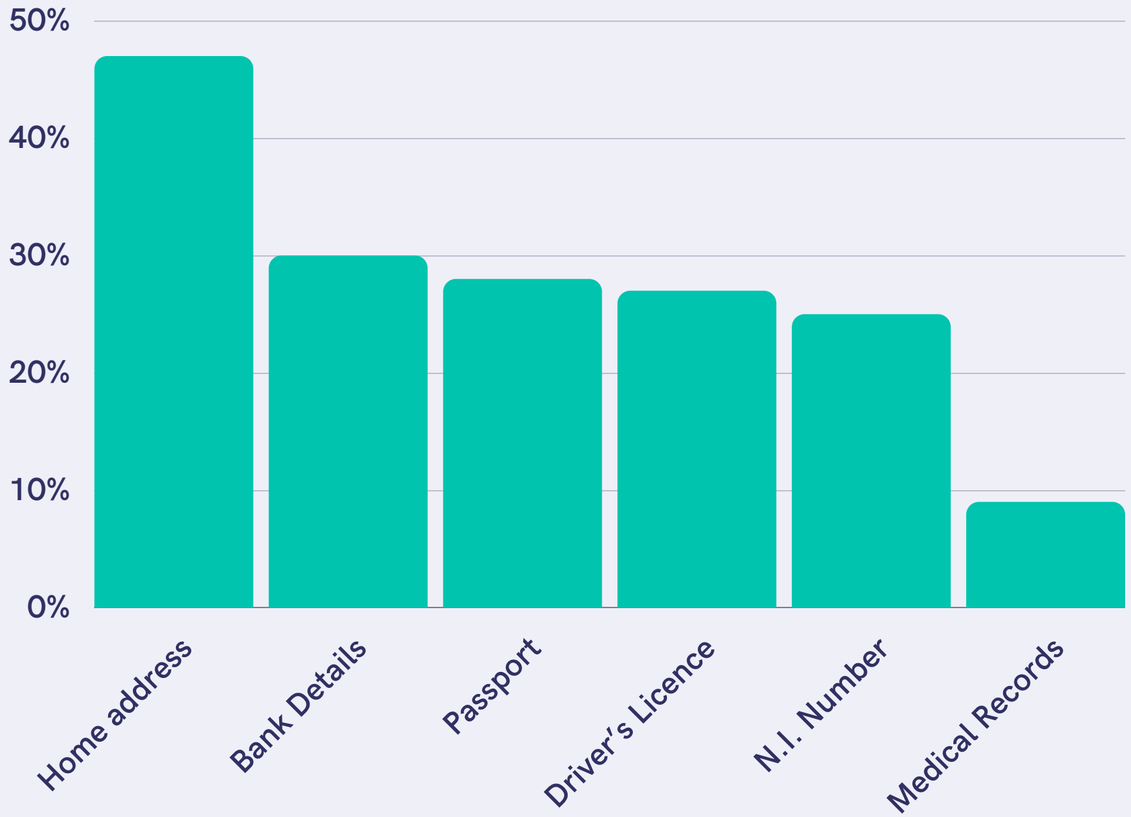
This highlights that consumers are willing to send sensitive data over email even when they know it might not be secure. This might be due to the widespread nature of email and the convenience it offers, as well as the majority of businesses still utilising it for their customer communications.

The problem with email

Amongst those who have knowingly shared personal data via email, almost half (47%) sent their full home address, three-in-ten shared bank details, and at least a quarter sent their passport, driver's licence, or National Insurance Number.

If threat actors were to intercept this type of data sent via email, they could conduct a range of malicious activities, including identity theft and financial fraud. The impact of these on a consumer or business can be significant and long-lasting.

A quarter (24%) of UK adults said they have accidentally shared personal data with the wrong recipient, with the majority (16%) occurring in the past 3 months. Of course, this number is likely to be higher when we consider that many people may be unaware of their mistakes.

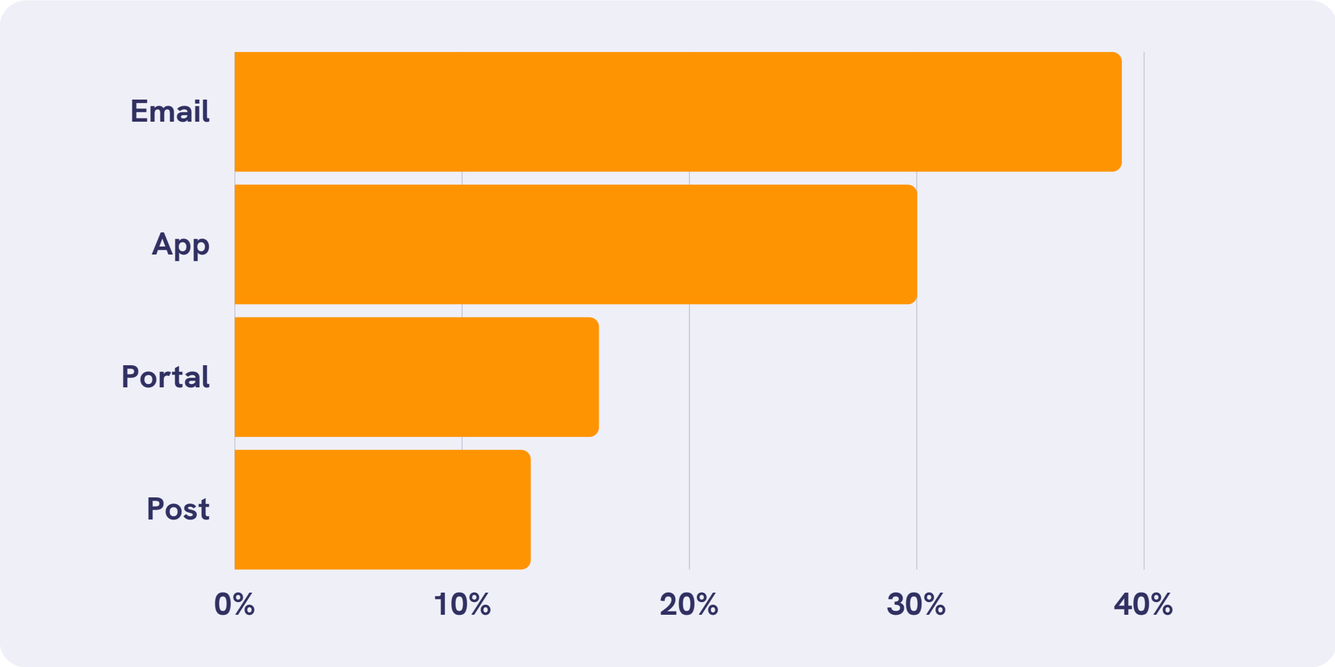


Customer preference

Since the pandemic, businesses and consumers have increasingly relied on digital communications, with customer choice being key to achieving high levels of engagement and retention. But what communication channel do consumers prefer when interacting with businesses?

Email is the most popular choice, with four in ten (39%) surveyed stating it is their preferred method of communication with a business that they have an existing relationship with. This falls ahead of a company's own mobile device app, with 3 out of 10 consumers preferring to use this method. Only 16% of consumers prefer an online portal and 13% prefer post.

Other preferred communication methods that were mentioned by respondents include phone calls, SMS messages, and face-to-face interaction.



Sustainability

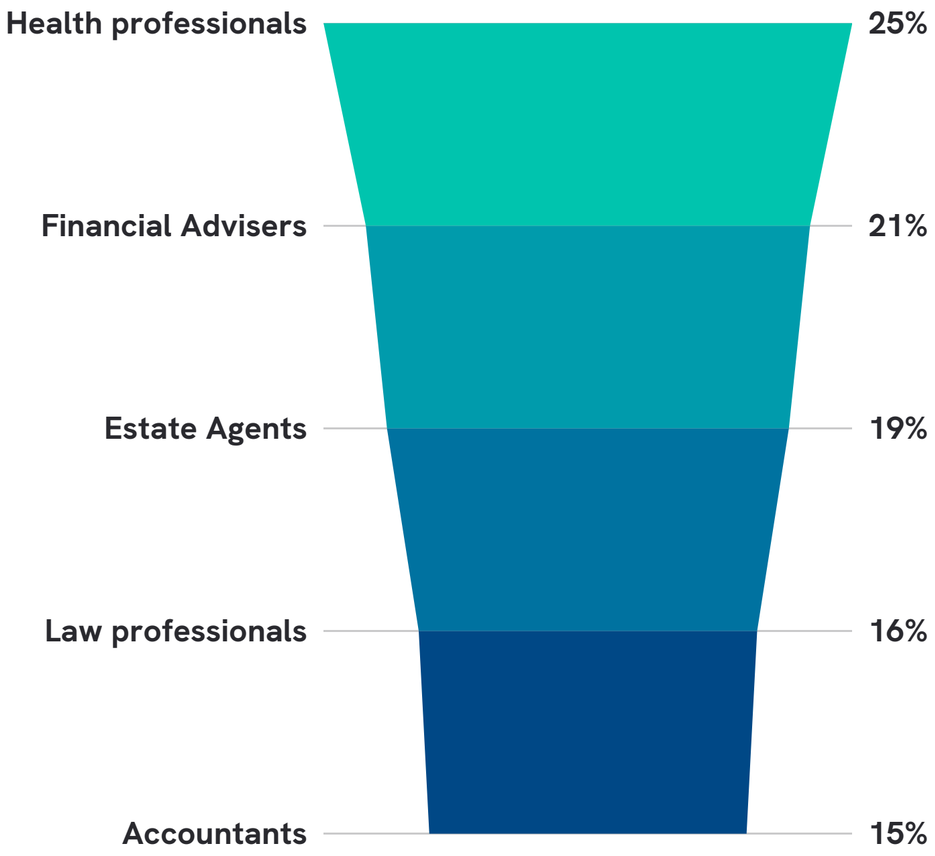
Considering that only 13% of consumers prefer to receive communications from a business by post, that the current volume is still so high is, perhaps, surprising. Data suggests that Royal Mail delivered just under eight billion letters last year alone.

Postal communications have a significant carbon footprint, with a large amount of resources required to manufacture, process, and transport letters and packages. It is estimated that every tonne of post generates around 3 tonnes of CO2e. This comes at a monetary cost to businesses' bottom lines.

Seven in ten (69%) UK adults feel that businesses should reduce their postal communications to reduce their carbon footprint, with a third (32%) strongly agreeing with this sentiment and only 8% disagreeing.

7 in10

UK adults feel that businesses should decrease their postal communications to reduce their carbon footprint.



With cyber-attacks on the rise, it’s vital that industry guidelines are upheld by businesses when it comes to customer safety. Businesses that encourage their customers to send sensitive information unsecured are not just putting their data at risk, they could be subject to fines and reputational damage.

HOW ARE ORGANISATIONS COMMUNICATING WITH CONSUMERS?

Business interactions

Guidance from the ICO (Information Commissioner’s Office) and other regulatory bodies state that businesses are legally required to secure and encrypt sensitive data. Email is the channel of choice for consumers, yet companies are still failing to implement the appropriate protections to ensure that email is secure and their customers are protected from risk.

Which businesses are requesting personal data over email?
Results show that almost three-quarters (73%) of consumers have been asked by a professional services provider to share personal data over email.

Amongst respondents who have shared personal data via email, a quarter (25%) have been asked to do so by health professionals, a fifth by financial advisers (21%) or estate agents (19%), and one in six by legal professionals (16%) or accountants (15%).

Other answers from respondents included:

- Banks
- Insurance company
- Council
- Employer
- Government
- Holiday booking organisation/ hotel
- Recruitment agencies

DEMOGRAPHIC DIFFERENCES

Generation

The research explored the effect that generational divides may have on consumers' approaches to cybersecurity, email usage, and communication preferences.

Cyber awareness and actions:
Survey responses reveal that baby boomers are the least confident when it comes to cybersecurity knowledge and actions, with only 66% being confident in their ability to protect themselves from cybersecurity threats, compared to the population average of 73%.

Additionally, 15% of baby boomers either wouldn't feel confident or do not know how to spot a phishing scam, and six in ten have little understanding of end-to-end encryption. Despite this, baby boomers are more diligent when it comes to cybersecurity measures than other generations, being the most likely to update their anti-virus each month.

In comparison, we find that Gen Z displays the most casual attitude to cybersecurity, with 14% never having updated their passwords and 18% not having antivirus software on their devices.

66%

of baby boomers are confident in their ability to protect themselves online

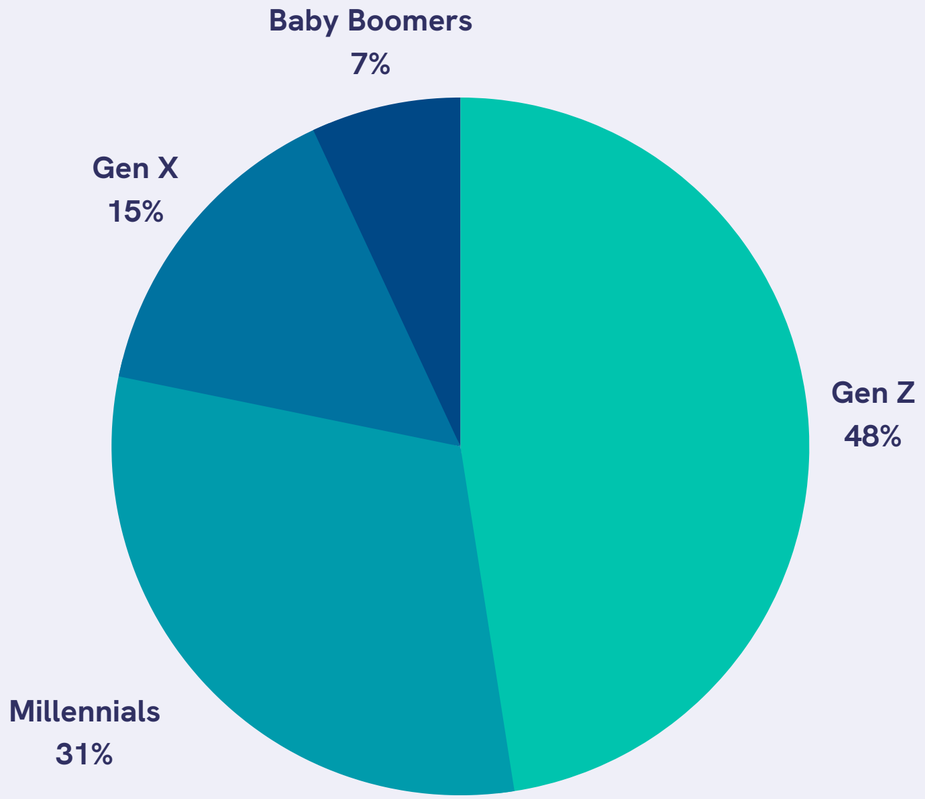
Generation

Email and personal data:
When it comes to digital comms, baby boomers were most sceptical of the security they provide, with 4 out of 10 believing that email, WhatsApp, SMS, and Facebook Messenger are not secure. On the other end of the spectrum, Gen Z is the most trusting of digital communication channels, with only 17% saying the aforementioned messaging platforms are not secure.

Looking at email specifically, baby boomers are the least likely to send personal data over email, with over 60% saying they have never done so (compared to the overall average of 47%). Additionally, less than 10% have mistakenly sent personal data to the wrong person.

In comparison, over 30% of Gen Z have shared personal data over email in the last four weeks alone, followed by millennials (21%) and Gen X (11%). Gen Z is also seven times more likely than Baby Boomers to have accidentally emailed personal data to the wrong person, and twice as likely compared to the population average.

Have you ever accidentally shared personal data over email with the wrong recipient?



DEMOGRAPHIC DIFFERENCES

Generation

Choice of comms:
In terms of communication preference, email ranked highest for each generation of respondents. However, Gen X and Gen Z differ in their likelihood to use each method:

- Gen X is the most likely of all generations to want to use an organisation's app, with 35% stating it as their platform of choice.
- Gen Z is the most likely to want to use online portals or receive postal comms, with 15% stating it as their chosen platform.

Baby boomers are the least concerned with sustainability, with only 61% agreeing that businesses should decrease their postal communications to reduce their carbon footprints. This compares with 73% for Gen Z and millennials and 72% for Gen X.

Location

Which region has the best cybersecurity practices?
Breaking down the data by geographic area, the region with the highest confidence in its cybersecurity knowledge and abilities was Wales. Responses from Welsh participants revealed that:

- 89% feel they protect their personal data from cyber security threats.
- 78% feel they are knowledgeable about cyber threats.
- 73% feel confident about identifying a phishing scam.

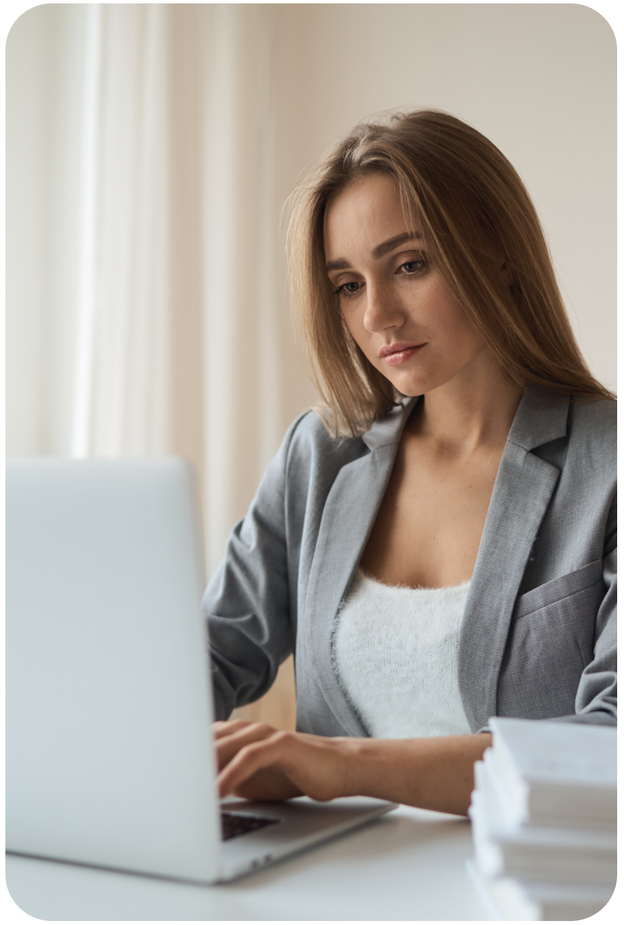
We see that Welsh participants are also the most sceptical of the security of digital comms, with 37% saying that WhatsApp, email, SMS, and Facebook Messenger are not secure or protected. This aligns with their actions, with nearly 60% having never sent personal data over email. Of the 41% that have done so, nine out of ten say that they have never sent it to the wrong recipient.

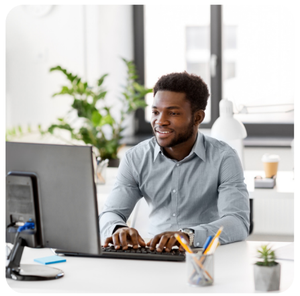
Location

Which regions have the most misaligned perception of cybersecurity?
When we consider the regions with the highest confidence in their cybersecurity awareness and the lowest level of action, the top contenders are the West Midlands and Northern Ireland.

Northern Ireland presents as one of the most knowledgeable regions when it comes to understanding encryption (62%) and the cybersecurity threats they may encounter online (78%). However, this understanding does not extend to individuals' efforts in protecting their digital assets. Results from Northern Ireland participants show that they update their anti-virus the least per year, as well as being one of the most likely regions to not use an anti-virus at all.

Respondents from the West Midlands are some of the most confident when it comes to their understanding of encryption, as well as their abilities to identify a phishing scam. However, this understanding of email risk and security is not necessarily being acted upon, as the West Midlands is the second most likely region to send personal data over email (60% compared to an average of 53%) and to accidentally send personal data to the wrong recipient (32% compared to an average of 24%).





4 in10

adults in London have sent their passport and full home address over email.

DEMOGRAPHIC DIFFERENCES

Location

Which region has the worst cybersecurity practices?
London showed the worst results comparatively in terms of the security of its personal data. Those living in London are the most likely to send sensitive data over email, with 67% of participants saying they had done this compared to an overall average of 53%.

London respondents were also most likely to send an email containing personal data to the wrong recipient, with 43% of respondents confirming they had done this, and at least 2/10 having done so in the last month. In terms of what type of personal data they are sending, 4/10 people in London have sent their passports and full home address over email, and 3/10 have sent their bank details.

Yet, London respondents were most keen on being communicated with by email (42%) and are the highest supporters of a reduction in postal comms (74%).

DEMOGRAPHIC DIFFERENCES

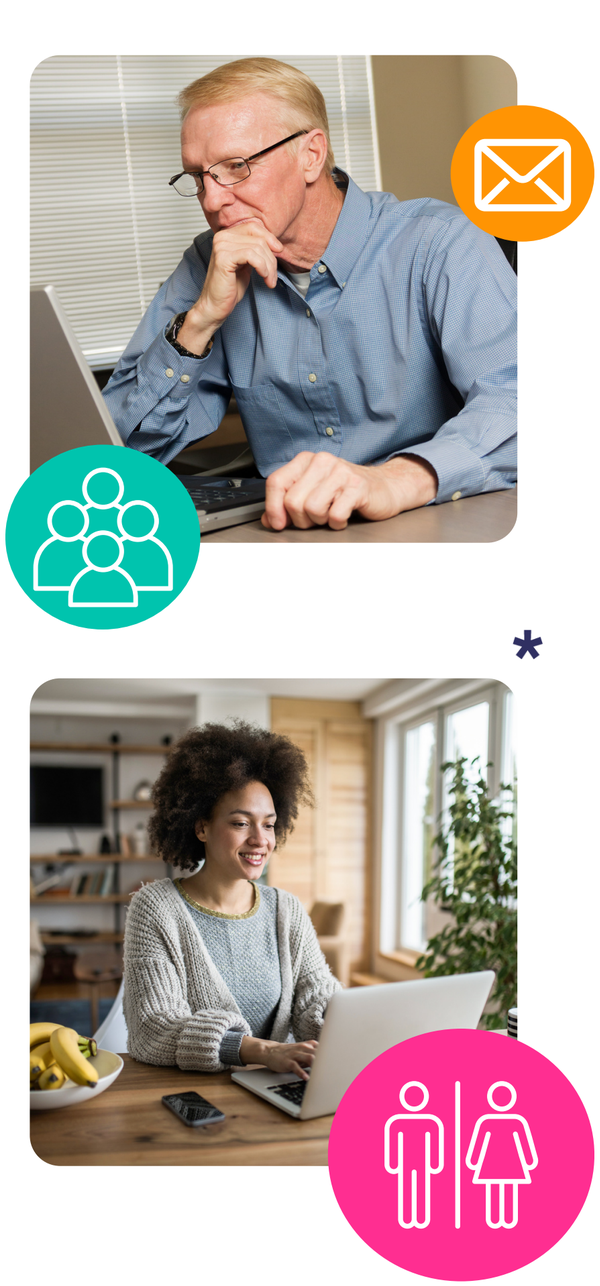
Gender

When comparing the gender of our respondents and their answers, we can see a clear split in cybersecurity awareness levels. The data shows that:

- More men than women believe they are knowledgeable about cybersecurity threats (76% compared to 70%).
- More men than women feel confident identifying a phishing scam (69% compared to 61%).
- More men than women are knowledgeable about encryption (55% compared to 36%).

However, while men appear to be more well-versed in the technical aspects of cybersecurity, they appear to have worse email habits. 58% of men have sent personal data over email - an increase of 10% compared to 48% of women – and double the percentage of men than women have sent personal data accidentally to the wrong person (32% compared to 16%).

Women are also more distrusting of digital comms, with 36% saying that none of the communication options provided are secure compared to 22% of men, and only 24% of women saying email is secure compared to 29% of men.



Conclusion

The increasing frequency by which services are moving to digital can make it difficult to find the right balance between security and efficiency for businesses looking to engage their customers – especially as there are such drastically different preferences and behaviours between demographics.

Taking the steps to understand consumer attitudes towards cybersecurity and desired communication methods for particular segments will be crucial in meeting customer demand. It is also critical for facilitating the security needed to protect personal data.

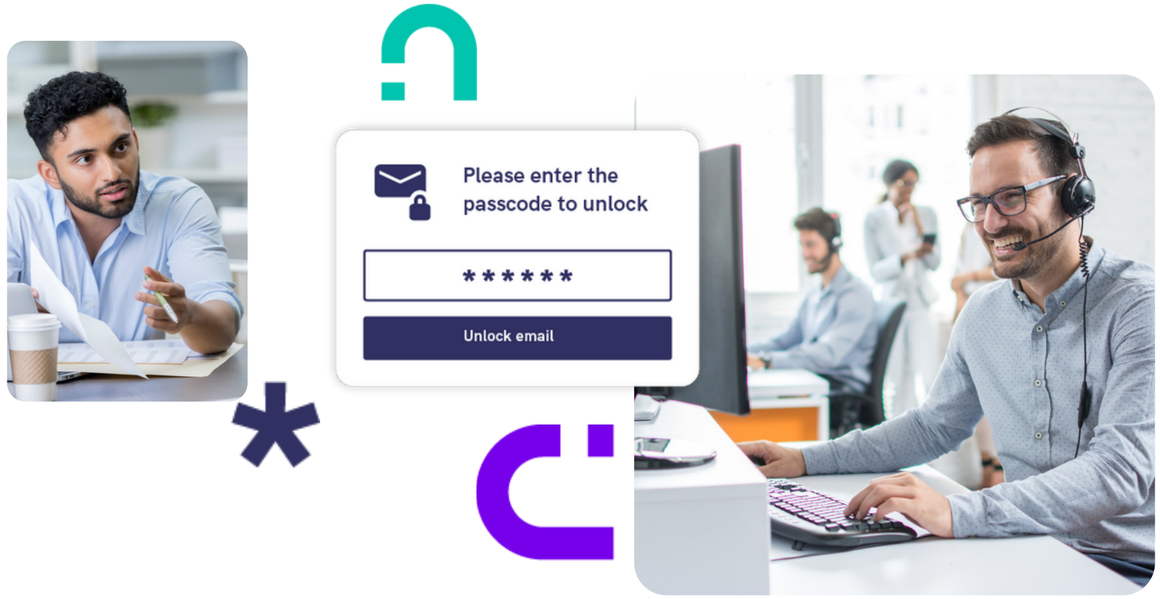
With the results revealing that consumers still send personal data over email, despite knowing it is unsafe to do so, we must question why this is the case. Firstly, as four in ten (39%) respondents stated that email is their preferred method of communication, we can deduce that consumers are choosing the convenience of email regardless of the risk to their personal data. We can also see that 73% of consumers have been asked by a professional services provider to share personal data over email, showing that businesses may be facilitating this preference for email communications but are disregarding the safety of their customers' data.

Going forward, businesses must offer their customers a choice of communication channels in which to interact with them, and each method must be secure. For the majority of consumers who prefer email, this means implementing a secure email solution, utilising encryption and authentication to protect the transmission of sensitive information.

Organisations that manage to balance consumer preference with security will be the ones who thrive in the new digital era.

About Beyond Encryption

Beyond Encryption is the platform of choice for secure digital communications. We give organisations the freedom to exchange digital information confidently, cost-effectively, and with full compliance, supporting them on their digital transformation journey. We've built the world's most secure encrypted communications network to protect and connect personal data using Mailock secure email.



About Mailock

Mailock is our versatile secure email solution, enabling organisations to send customer communication securely via email. Mailock protects sensitive data through end-to-end encryption and multi-factor authentication, helping you remain compliant, reduce costs, and improve operational efficiencies - not to mention achieving a positive environmental impact through the reduction of print, pack, and post.

CONTACT US

beyondencryption.com
marketing@beyondencryption.com
Beyond Encryption, Gloster Court, Whittle Avenue, Fareham, PO15 5SH

Beyond Encryption