Ignorance is Bliss:

Most adults are leaving themselves open to cybercrime, despite knowing the dangers.

Kaspersky research asks WHY?

Generation X and Millennials are putting themselves at risk online, and failing to accept that their actions have consequences when it comes to cyber security.

A Kaspersky Report
April 2023

Contents

Overview:

We can reveal that most adults are their own worst enemy, leaving themselves wide open to taking risks online in the belief that it's simply someone else's problem.

Complacency is the enemy of progress when it comes to the risks adults are unwittingly taking online. According to the findings from our latest survey, most people, regardless of age, gender, or social status, are currently taking a 'this won't happen to me' or 'what's the worst that can happen?' approach to cyber threats.

We can reveal that most adults are their own worst enemy, leaving themselves wide open to taking risks online in the belief that it's simply someone else's problem. In fact, while most respondents to our survey (aged 16-55+) believe they are knowledgeable about online security (76%), only 21% have taken action to block phishing scams after they had been a victim of them.

Millennials, a generation that has grown up in a rapidly changing digital world, are seemingly amongst the most vulnerable to cyber-attacks. They thrive on technology, engage with it regularly, and consequently are very confident about the risks involved.

Too confident by half, it seems.

But it's exactly this confidence and lack of caution which is leaving adults overexposed to the risks. Why are they not doing more to protect themselves online? How can we change behaviours and attitudes towards online safety to ensure that the cyber criminals can't win?

The following report explores adult behaviour, attitudes, and approach to online safety, revealing that, when it comes to cybersecurity, adults still simply don't realise that their actions have consequences. Kaspersky is a global company with threat intelligence experts active in every region. The business has used its unique experience to undertake extensive research into how safe adults are online and their general understanding of a range of cyber threats including phishing attacks.

6,382 online surveys with children

aged 11-15 were conducted by Censuswide across 8 countries

6,655 online surveys with adults

were conducted by Censuswide across the same 8 countries

Methodology:

A total of 6,382 online surveys with children aged 11-15 were conducted by Censuswide across 8 countries in 2023 between 03.01.23 – 10.02.23 in the UK (1,003), France (1,001), Spain (1,000), Portugal (507), Greece, Netherlands (501), Germany (1,002) and Italy (1,013). Respondents were asked about their cybersecurity knowledge, whether they had been targeted by a phishing scam, if an adult had ever helped them to spot a potential phishing scam and if they could tell the difference between a fake and a real email.

An additional 6,655 online surveys with adults were conducted by Censuswide across the same 8 countries in 2023 between 03.01.23 – 10.02.23 in the UK (1,001), France (1,000), Spain (1,000), Portugal (503), Greece (650), Netherlands (501), Germany (1,000) and Italy (1,000). Respondents were asked about their cybersecurity knowledge, whether they had been a victim of phishing and if they help their children or younger generations to identify potential phishing scams. Censuswide abides by and employs members of the Market Research Society, which is based on the ESOMAR principles.

What we found:

All adults over the age of 16 understand what a phishing scam is, and the more they are targeted, the savvier they believe themselves to be...

- Over three-quarters of all adults say they know what a phishing scam is.
- Adults who admit to being a victim of phishing scams are more likely than those who haven't to say they are an expert when it comes to online security (17% vs 6%).
- The majority (88%) of millennial adults (aged 35-44) are the most likely to know what a phishing scam is, with 3 in 5 (60%) saying that they are knowledgeable about online security. Millennials in the UK are the most likely (70%) to say that they know about online safety.

> Only 1 in 10 (10%) people surveyed in the UK claim to have 'taken action' after suffering a phishing attack,.

Despite claiming to understand the risks of phishing, adults of all ages are still failing for them...

- Over a fifth (22%) of all adults surveyed who claim to be knowledgeable about online security have, in fact, been a victim of a phishing scam.
- A quarter (25%) of all adults aged between 25-35 admit they have been a victim of phishing scams, compared to just 1 in 8 (12%) aged 45-54 who said the same.
- Only 1 in 10 (10%) people surveyed in the UK claim to have 'taken action' after suffering a phishing attack, compared to 25% in Greece who said the same.

Despite knowing the risks, adults are putting themselves at risk because they are still sharing personal information online...

- Nearly three-quarters (74%) of adults include personal information such as their name and location on their social media channels.
- A further 69% have given away information such as their pets first name, their mother's maiden name and their street name on social media quizzes.
- Alarmingly, 69% of all adults are still using personal information, such as favourite football team and first pets name to help them remember their passwords.

Online actions have consequences

Adults admit to knowing that they are being attacked by cyber criminals, but still aren't taking any steps to protect themselves.

The Internet is pretty much indispensable now to most people; screen time is up and so too is the security risk. Generation X and Millennial adults have grown up around technology, so it would be reasonable to expect them to have a deep understanding of the threats involved and a desire to protect themselves and others against them.

phishing attacks alone rose by **61%**

But this is only partly true.

According to our research, 80% of millennial adults aged 35-44 say they know what a phishing scam is, compared with only 60% of Generation X adults aged 16-24. A further three in five (60%) of all adults claim to be knowledgeable about online security. This reveals that most adults today believe they are either cyber security savvy, or do, at the very least, have a broad understanding of online security and the risks it can protect them from.

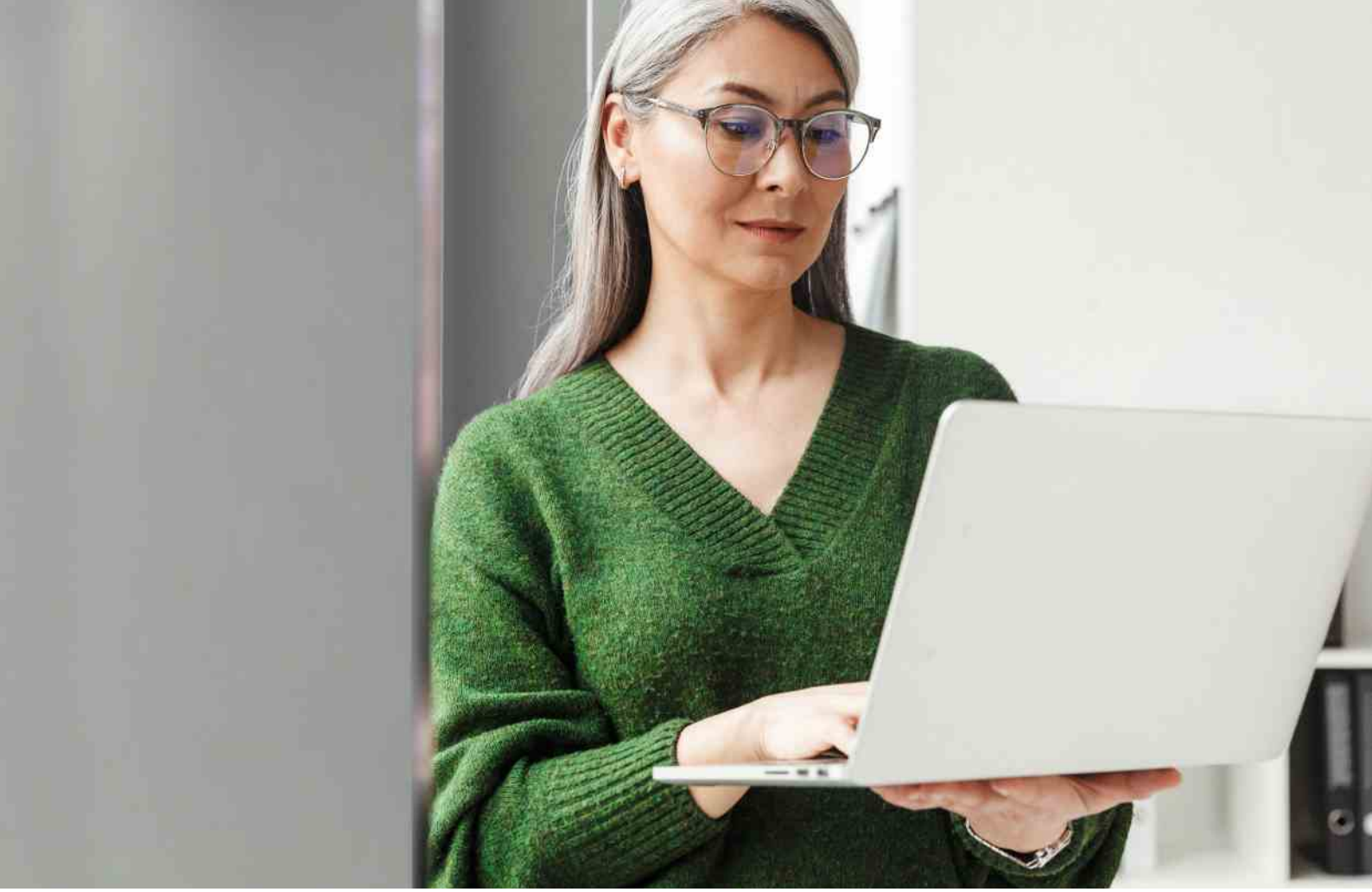
Our research reveals that despite this knowledge, over a fifth (22%) have still been a victim of a phishing scam, with a quarter (25%) of 25–35-year-olds admitting to being a victim. Of course, this could be down to bad luck, a simple mistake or even the fact that attacks are getting harder to spot – which of course they are.

However, only a fifth (21%) of people aged 25-35 who have been a targeted by a phishing scam took any sort of action to try and stop it happening again. This number dropped even lower among the 45-54 age group (15%). This level of complacency suggests either a lack of understanding about how to reduce the risks, that adults aren't as knowledgably as they think or an even more alarming attitude that cybercrime simply isn't enough of a threat to act on.

The reality is that the threat is very real.

Our first report in this series [LINK] highlighted that phishing attacks alone rose by 61% in the six months ending October 2022. It's showing no signs of stopping with the added sophistication of scams which has been brought about by generative AI chatbots, and the ability for a non-native language criminal to easily construct an almost perfect digital imitation of another human being.

Fail to act now, and you will regret it sooner rather than later.



Share, phish, repeat

> If you share your public information online, it's there forever and you have no control over who, sees it, uses it and how.

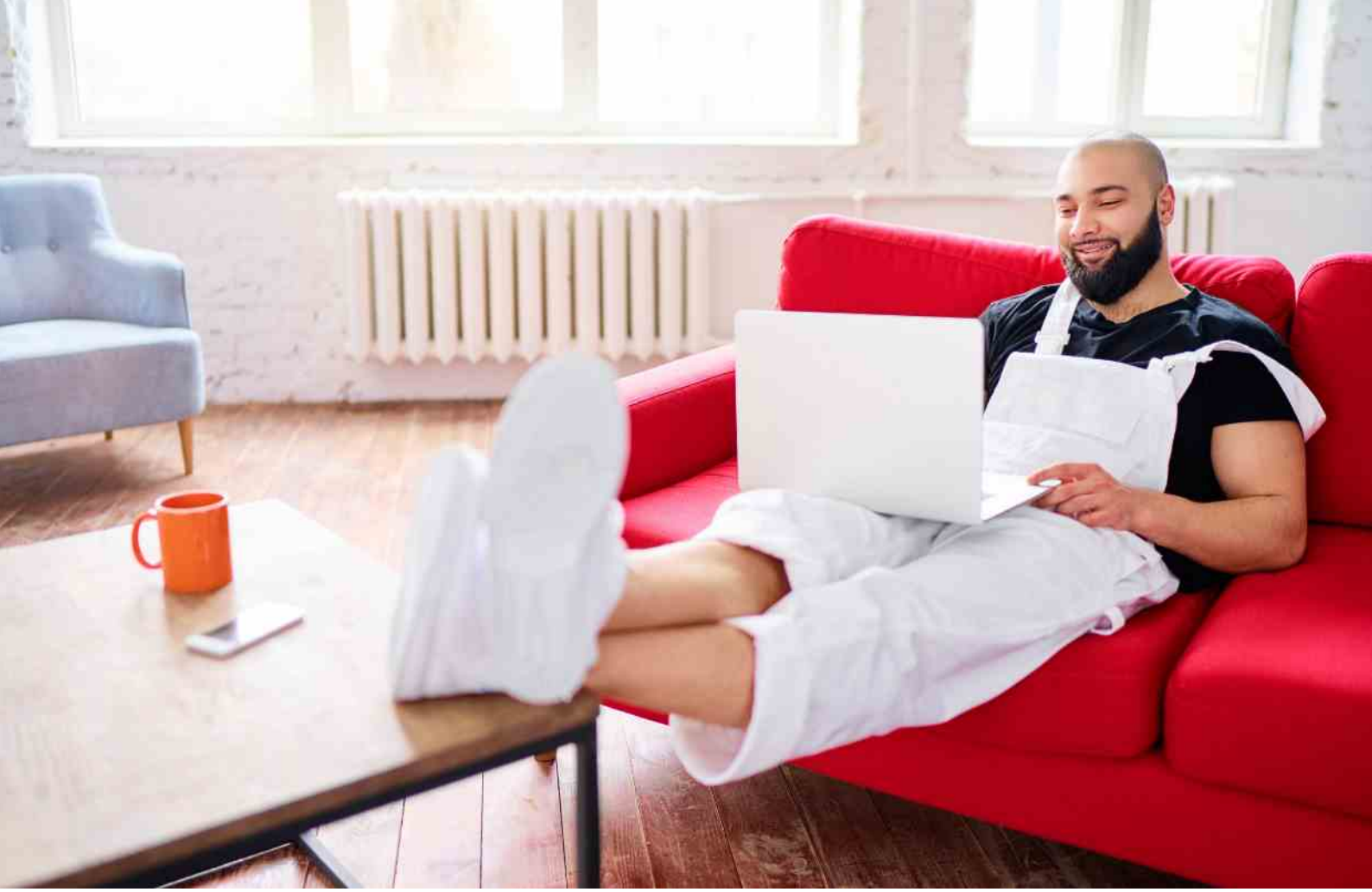
Adults claim to understand the dangers of cyber threats, but rather than protect themselves, they are sharing more online than ever before.

The threats are evident, the risks are known and understood and, in some cases, (58%) adults are aware that they are being targeted by phishing scams at least once a month. Yet, paradoxically, they are still likely to share basic information and content online.

The survey revealed that 74% of adults who have been a victim of phishing scams say they would still share personal information on social media, use the same personal information as passwords (69%), and participate in online quizzes about their first pet or their mother's maiden name (69%).

It's clearly not a lack of awareness that's causing the problem, but rather an attitude of complacency and not appreciating the value of the information they are freely putting out into the world. Our findings highlight an urgent need for adults to understand that their online actions have consequences and that their digital identities are just as important as their birth certificate or passport.

The reality is if you share your public information online, it's there forever and you have no control over who, sees it, uses it and how.



The price of over sharing

> Most adults simply don't understand the value of the data that they are giving away for free.

Everything has a price, but the value of some items might be less obvious than others.

As we know, nothing in life is free, and if it is, there is usually a catch. It is often said that if you are not paying for the product, you are the product – meaning that if a platform or app is free to use, then it's very possible they make their money from your data. While it's straightforward to put a price on a house, a car, or an item of clothing, it is less easy to put a value on your data, but never the less, it is valuable!

Our research shows that most adults simply don't understand the value of the data that they are giving away for free. Just as they wouldn't leave the front door wide open when going away on holiday for risk of being burgled, they need to take pre-emptive action when they know cyber criminals are targeting them with phishing scams.

So, how much is your data worth to a cybercriminal?

Kaspersky threat experts analysed 10 international darknet forums and marketplaces to understand the 'street price' of personal information, and the results were alarming.

Among the most popular and highly sought after items were PayPal account details trading for up to £420 a time. A selfie with documents such as driving license or passport can be sold for up to £50 each; a name and date of birth £8; and subscription service passwords, such as Netflix, £7.

How much are cybercriminals paying for your information?

Credit card details	£5 - £17
Driver's license scan	£4 - £21
Passport scan	£5 - £12
Subscription services passwords	40p - £7
Full name, date of birth, email, mobile	40p - £8
Selfie with document details – driving license or passport	£33 - £50
Medical records	83p - £25
Online bank account	1-10% of value
PayPal account	£42 - £420

This demonstrates that not only does everything have a price, but that this kind of information is extremely valuable to criminals.

At first glance, these may not appear to be huge sums, but this kind of data can be used to take control of subscription services, drain bank accounts, or be used for other large-scale purchases. Yes, in some cases money lost in this way may be refunded by banks or vendors, but there's no guarantee and being careless about safety online could lead you to be being seriously out of pocket.

Between 2021 and 2022, cybercrime in the UK alone totalled over £3 billion – a figure that demonstrates the scale and impact of these actions on individuals, businesses, and the wider economy. The National Fraud Intelligence Bureau (NFIB) tracked losses resulting from cybercrime incidents and found that cybercrime cost £3.1 billion from April 2021 to April 2022, representing a significant increase over previous years.

> This demonstrates that not only does everything have a price, but that this kind of information is extremely valuable to criminals.

Cybercrime costs people hundreds, if not thousands, of pounds every year. What's more concerning is that adults are not only admitting to knowing about cyber threats such as phishing, but many of them have also been victims of it. This somewhat cavalier attitude towards cybersecurity is only making the problem worse and, perhaps most concerningly, setting a bad example for the next generation.

"We need to take action to protect ourselves online and do it right now. It's like knowing about the dangers of the road, but still crossing without looking. It's time for adults of any age to take responsibility for our own online safety and adopt good cybersecurity practices to protect ourselves and our families both now and in the future.

David Emm
Principal Security Researcher Global Research and Analysis Team, Kaspersky

Knowledge isn't enough. Attitudes must change if we are to stop cybercrime...

The results are clear: all adults have the knowledge to tackle the perils of cybercrime, but lack the desire and attitude to effectively fight against it. There is a need for greater awareness and more education around online security across the board to make adults sit up and take notice.

The next generations are looking to their parents, family members, and teachers to show them the way. If they are to be protected, adults today must show them that it's important to realise that actions have consequences, that data is valuable and that we all need to be careful when disclosing information about ourselves online. Adults must demonstrate that if they see a threat, they act.

It's not enough to simply put your heads in the sand and hope for the best. So, let's not be the 'so what' generation, but rather the 'let's stop this' generation and together we can reduce cybercrime and keep the internet a safer place for everyone, both today and tomorrow.

For more information on how children and adults can protect themselves online against cybersecurity threats get in touch with the **Kaspersky team here.**

Kaspersky
Kaspersky Lab, 1st Floor
2 Kingdom Street
London, W2 6BD, UK
www.kaspersky.co.uk

kaspersky