Overconfident and over exposed: Are Children Safe Online?

Children are going online like never before. But just how safe are they? And who is helping protect them from cyber threats?

A Kaspersky Report
February 2023

Contents

Overview:

"Education is the most powerful weapon which you can use to change the world,"

Nelson Mandela

Keeping children safe online is at the top of the personal and political agenda for many in the western world. In the last 10 years, increasing access to the internet, has gone hand in hand with the ease of purchasing a connected device. As a result, children have become more and more at risk, not only from harmful content, but also from online fraudsters and scammers.

The EU's Digital Services Act aims to provide clearer and more standardised rules for digital content, whilst the UK Government is threatening senior executives of online companies with a minimum two-year prison sentence if they continue to ignore Ofcom regulations and fail to protect children from harmful content.

But despite the warnings, many parents across the world are still tempted to use screen time to buy a few minutes peace and quiet or to get the family through a long car journey. However, there are dangers; one minute your children could be watching Peppa Pig or the latest vlogger on YouTube Kids, and the next, they could be being told that the moon landing was faked, watch Lada Gaga twerking or far worse.

Equally alarming, it isn't just harmful content that is putting children at risk. The moment they step online, the threat of cybercrime is also present, from phishing attacks to ransomware.

Much of the public debate so far about the dangers of the digital world for children has concentrated on content. But young people also need to be educated and protected from online scams.

Children are extremely susceptible to online scams and very much at risk in a world rife with cyber-attacks

During the COVID-19 pandemic, schools around the world were forced online, creating an online presence for children whether they were ready for it or not. From video conference classroom sessions and individual pupil email addresses being created, to online YouTube tutorials, hundreds of thousands of children entered the online space. And while this undoubtably helped millions to keep up with their education, in the rush to take advantage of the benefits of online learning, did anyone really stop to educate children or their parents about the dangers of being online and how vulnerable they are, not only to all the damaging content, but also to the many scams out there waiting to exploit them?

Admittedly, Generation Z and Alpha are fairly tech savvy, and it would be remiss to imply otherwise. Having been exposed to the technological wonders that are now available to them from a young age, they are often more knowledgeable than their parents on how devices work, the content they can access and what is available to them online.

But are they aware of what a phishing attack is? Do they know if they have been a victim? Have they given away their own or a family member's personal information online? Can they spot the difference between a real email and a scam? Are they aware of how their data is used by legitimate companies?

Kaspersky is a global company with threat intelligence experts active in every region. The business has used this unique experience to undertake extensive research into how safe children are online and how much they understand about cyber threats such as phishing attacks.

The findings of our report exclusively reveal that nearly two in five children and young people surveyed who say they are knowledgeable[2] about online security, have in fact been victims of phishing scams. This not only highlights the gap of being able to work technology and the understanding of the threats with it, but also that children are extremely susceptible to online scams and very much at risk in a world rife with cyber-attacks.

The following report explores how vulnerable children are to cyber threats despite believing they are safe. It explores their attitudes to online security and finds that both parents and the education system need to play a more pivotal role in educating and protecting them. The findings reveal that when presented with real and fake emails, the majority are unsure about their authenticity, demonstrating that even if they feel confident online, there is still much to learn.

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.

In addition, 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 also asked about their cybersecurity knowledge, whether they too had been a victim of phishing and if they help their children or younger generations 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:

Children know they are being targeted by phishing scams on a regular basis yet are still giving their information away via social media or online games:

- Almost three in 10 (26%) children surveyed say they have been a victim of a phishing scam, with over a third (35%) reporting that they know that they have been targeted at least once a month or more.
- However, despite this, over half (55%[1]) of children surveyed admitted to using personal information such as their name and location on social media, with 54%[1] openly giving away information such as a first pet's name and their street name on social media quizzes.
- In fact, around two in five (39%) children surveyed who say they are knowledgeable[3] about online security have been a victim of a phishing scam, compared to only one in nine (11%) who say they are not knowledgeable[3] about online security.

The more knowledgeable children think they are about on security threats, the more likely they are to falling victim of an online scam:

- In fact, the ones who have already been a victim of a phishing scam are even more likely (79%[1]) to use personal information to help remember a password than those who haven't (47%[1]).
- Children surveyed also admitted that they would be more inclined to open a link from a WhatsApp message (30%) compared to only 11% who would be more inclined to open one in a text.
- Alarmingly, 83% of children surveyed who have been a victim of a phishing scam think they are now at risk of falling for another, compared to under 2 in 5 (39%) who have not been a victim of a phishing scam who said the same.

Although many young people know they are being targeted by phishing scams and admit that they are concerned, very little is being done by adults to teach children and young people how to stay safe online:

- Only two in five (42%) adults surveyed say they have helped their children or the younger generation to identify phishing scams.
- Some adults (27%) - who by their own admission are not knowledgeable3 about security threats - are trying to teach the younger generation about online safety and how to spot a phishing attack: a classic case of the blind leading the blind.
- Geographically 71% of adults surveyed in the UK, 67% in France and 53% in Germany admit to not helping children or the younger generation to identify phishing scams compared to 65% of adults in Greece and 51% in Portugal who have helped.
- And the phishing problems seem to be particularly acute in the UK, with 48% of children surveyed saying they have been targeted once a month or more, compared to just 36% of children in France, 32% in Italy, 30% in Greece and 22% in Spain.

> Only two in five (42%) adults surveyed say they have helped their children or the younger generation to identify phishing scams.

[1] 'Yes, more than once' and 'Yes, once' responses combined

[2] 'Very knowledgeable, I'm a pro' and 'Quite knowledgeable, I know more than most' responses combined

[3] 'Not very knowledgeable, I think I might be below average' and 'Not at all knowledgeable, I don't really understand it all' responses combined

The over confidence risk factor:

Children think they know more than adults, but over confidence is putting them at risk online.

The world has never been more connected than it is right now. It is estimated that 4.9 billion people are connected to the internet - that's 62% of the world's population. Of that, one in three is a child under the age of 18.

As a result, children's online safety couldn't be more important. Online learning, games and socialising means more and more children are turning to their devices to pass the time. Unlike previous generations, they know no different, brought up on tablets and smartphones, with instant access to endless information, content and conversation. The fact is, they live in a fast-paced connected world, which isn't slowing down.

As adults, we teach our children how to read and write, to cross the road. We tell them not to talk to strangers. But it appears that most of us are not teaching them how to stay safe online and avoid security threats such as phishing scams. Our research findings have found that 26% of children surveyed have been a victim of a phishing scam, with over a third (35%) saying that they had been targeted at least once a month if not more.

Even more alarming is that the children surveyed who believe they understand the risks of going online and are knowledgeable[2] about online security, are the ones most susceptible to scams. Around two in five (39%) children surveyed who say they are knowledgeable[2] about online security, have in fact been a victim of a phishing scam, which is much higher than the 11% who aren't knowledgeable[3], but who said they had also been a victim.

These findings point to an overconfidence in children when it comes to online security, and it is this confidence which is putting them at risk every time they go online.

Cybercrime is on the rise. Phishing attacks alone rose by 61% in the six months ending October 2022 and this shows no signs of stopping. Attacks and scams are only getting more sophisticated and with the introduction of AI platforms which are becoming more realistic and harder to spot, no matter how old you are.

Children surveyed in Germany are most likely to say they have ever been a victim of a phishing scam (54%), followed by children in the Netherlands (37%), UK (36%), Portugal (19%), Greece (17%), Italy (16%), France (14%), and finally Spain (13%) demonstrating that phishing attacks aren't just saved for adults and are a problem across Europe.

Phishing scams are so sophisticated that when shown a series of fake emails based on popular retailers, 72% of children identified at least one as being real.

Yet with just under three in five (55%) children surveyed say they are knowledgeable[2] about online security, how and why are they still falling for phishing scams?

26%
of children surveyed have been a victim of a phishing scam

How Generation Z are over sharing:

Despite children surveyed saying they are very knowledgeable about online security and that they understand exactly what a phishing scam is, the majority were unable to identify one or more phishing scams (72%), potentially putting themselves at risk every time they go online'. Most continue to willingly share information on social media, from the details they use to remember passwords to the games they play.

Over half (55%[1]) of children surveyed admitted to having included personal information on social media channels such as their name, date of birth and location. On top of this, 54%[1] also said they have answered social media quizzes which ask for details such as a pets first name, a street name or a favourite TV show.

What they don't realise is that these online 'games' are often scams for bad actors, who can then deconstruct their answers and use their social profile to form an online attack, such as account hacking or financial fraud.

Of course, anyone can be a victim regardless of the additional information that's put online. However, our data suggests that the more information you 'give away' to untrusted sources, the more likely you are to fall foul of an online security threat such as a phishing. The survey found that those children who have been a victim of a scam were more likely to have done the following, compared to those who have not been a victim:

- Use personal information to help them remember a password (79%[1] vs 47%[1])
- Include personal information on social media (79%[1] vs 46%[1])
- Engage in quizzes on social media (80%[1] vs 45%[1])

The findings clearly point to a growing problem of oversharing within Generation Z and Alpha. The more they share and trust, the more likely they are to fall victim to cybercrime.

> The more they share and trust, the more likely they are to fall victim to cybercrime.

Knowledge is power. But knowledge alone isn't always enough, and must be coupled with experience to be truly powerful.

It's no secret that today's children are digital natives, born into a technological world with no understanding of a world pre-connectivity. And it's fantastic to see that their knowledge of threats and online dangers is high, as well as their willingness to combat them. However, we must remember that children are exactly that – children. That being the case, their experiences and understanding of the world isn't yet fully formed, and as such, it's important to keep in mind that we must support their technological knowhow with the benefit of our experience and real-life wisdom. Because only then will they be well placed to overcome online dangers.

Having technical skills is necessary, but not sufficient. I may know the inner workings of the internal combustion engine, but it doesn't make me a safe driver. Online safety requires a technical knowledge combined with an understanding of human nature and the potential dangers that can stem from that, so it remains important that we continue to educate young people at school and at home about the world, real and cyber, so that they have the full tool kit to stay safe.

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

> Countries across Europe just aren't dedicating enough classroom time to online security.

'Knowledge' clearly isn't enough and more needs to be done to educate children on how to be safe online... but whose job is it?

Education is a basic human right and in most countries across the world, is guaranteed for all without discrimination. Alongside this, the education agenda keeps evolving and adapting to society's needs. For example, in early 2023, the UK Prime Minister, Rishi Sunak, announced plans for all school pupils to study maths in some form until the age of 18, in a bid to improve numeracy across the board.

Enhancements to education programmes are a good thing. But it is clear from our report that countries across Europe just aren't dedicating enough classroom time to online security. There simply aren't enough classes highlighting the dangers of different threats, or courses on how to stay safe in a virtual world. This means children are relying on their parents or guardians to teach them, but who is teaching the older generation about online safety?

Less than half (42%) of adults surveyed say that they have helped their children or the younger generation to identify phishing scams. Of the countries surveyed Greece are the most likely to say they have helped their children to identify phishing scams, with the UK being the least likely.

In fact, 40% of adults surveyed across Europe admitted that they weren't knowledgeable[3] when it comes to online security, with almost a fifth (19%) admitting that they too have been victims of a phishing scam.

The absence of online safety classes in schools and the lack of understanding or willingness of parents or adults to impart security wisdom on to the younger generation, is creating a perfect storm and reveals a huge online security education gap which must be addressed.

Quote from third party

Why we need cyber security education:

Children are the future: So, let's educate them on cyber security.

This research is clear: no matter your age, everyone is at risk of online scams and threats. A bad actor doesn't care how old you are or where you come from, to them everyone is fair game. The only way to put a stop to this is more and better education, giving people old and young the ability to spot and avoid the everyday scams.

Young people and children are no exception, and it's dangerous for them to think that just because they believe they are knowledgeable about online security, that they are not vulnerable to attack.

The internet has opened the world up to the younger generation and has presented them with a world of opportunities, but speed and adoption rates have been so fast that no one has stopped to look at how exposed we all are to the very real dangers that are out there. Dangers which are tripping up adults every day. It's simply unrealistic to expect that the generation brought up on tablets and smartphones would instinctively know what to avoid and what not to click.

Children are our future and more has to be done in schools and at home to teach them how to stay safe online. Even if they believe they have the knowledge and skills to protect themselves, they are still falling victim to even the simplest phishing attack. And the threats are only getting more sophisticated, as more of our information is only going online. We live in a data world now and whether you are 11 or 111, your digital footprint is expanding by the day, giving criminals more opportunities and more content to steal.

[4] Respondents from all countries surveyed, UK, France, Spain, Portugal, Greece, Netherlands, Italy and Germany

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