

Lloyds Bank reveals "powerless" parents of online gaming children fear fraud "only a matter of time"

- Over a third (38%) of parents have never spoken to their children about staying safe from fraud while gaming online, with 25% lacking the knowledge on how to protect their child
- 36% of parents are worried they are leaving the family finances open to fraud as a result
- To support families, Lloyds Bank partners with gaming industry body Ukie, to give parents industry-approved guidance on the SHIELD Game Players Code to keep their children safe online.
- Television presenter Helen Skelton has joined forces with Lloyds Bank to encourage parents to learn about the risks of online gaming fraud and become SHIELD-qualified

London, 26 July 2022: With video gaming scams on the rise¹, Lloyds Bank is urging parents to learn how to spot the signs of online gaming fraud as new research reveals that half of parents are worried their children could fall victim to online gaming fraud. The rising potential for fraudsters to target children online has resulted in 30% of parents feeling fraud is inevitable, seeing it as "only a matter of time" until their child falls victim to online scammers.

Children are spending more time playing online games than ever before - over 5 million children aged between the ages of 3 and 15 are now regularly playing games online², up from approximately 4.6 million in 2019³. Fraudsters, always ready to take advantage of opportunities presented by new trends, are now increasingly targeting this rising demographic. With young people less experienced in recognising suspicious requests or activity and more likely to readily share information, many parents are seeing their own finances exposed as a result.

Research by Lloyds Bank found that over half (56%) of 6-10-year-olds now play video games between 6-20 hours each week. Ages 4-6 are the most common ages for children to start playing video games with parental permission, making this the critical time for parents to start having those important pre-gaming conversations with their children about the dangers of fraud.

While children are a common target for gaming fraudsters, the research revealed that over three quarters of parents polled (77%) allow their children to play video games without complete adult supervision. This means hundreds of thousands of children can potentially share personal details or important financial information online without their parents' knowledge.

A quarter (25%) of parents also said they do not use any security measures to protect their children. Over half (55%) of parents grant their children access to their own finances, with 36% admitting they worry about exposing the family bank account to potential fraud as a direct consequence of their child's gaming and their own lack of awareness and understanding.

¹ Lloyds Banking Group, Fraud's No Game 2021. Survey conducted by Opinium with a sample of 2,002 video players in the UK

² Ofcom, Online Nation 2021 Report

³ Ofcom, Children and Parents: Media Use and Attitudes 2019 Report



A lack of confidence on the issue is one reason why parents avoid the topic. Nearly a third of parents (31%) said they feel powerless to stop their children becoming victims of gaming fraud while a quarter (25%) attribute their silence to a lack of knowledge on how they can protect their children from gaming fraud. An additional 38% of parents said that they could not confidently explain what gaming fraud is.

Introducing the SHIELD code quiz

The research comes as Lloyds Bank partners with national gaming body Ukie, to offer parents the chance to get SHIELD Qualified through an informative interactive quiz which can be accessed at <u>www.askaboutgames.com/Lloyds-SHIELD-quiz</u>. The online test is based on the SHIELD code, developed by Lloyds Bank and Ukie. Successful completion enables parents to become SHIELD-qualified and come away with the confidence and guidance they need to start meaningful conversations with their children before they start gaming.

Spotting the signs of gaming scams

As gaming amongst youngsters rises, scammers are increasingly targeting the most vulnerable in order to defraud players, and their parents, of their money or identities. The research carried out by Lloyds Bank revealed the most common types of fraud and methods used by scammers:

Most common types of fraud		Most common methods used by scammers	
experienced by children		to contact children	
Identity Theft	67%	In-game chat functions	47%
Hacking	61%	Impersonation of in-game support	28%
Phishing	53%	Phone call	10%
Grooming	45%	Phishing email or text	7%
Purchase of fake goods	41%	Malware installation	7%

Television presenter Helen Skelton has joined forces with Lloyds Bank to raise awareness about the risks of gaming-related scams and getting parents to become SHIELD-qualified. She is encouraging parents to have conversations about gaming fraud with their children and set up parental controls on devices that can limit in-game chat or spend to reduce risks.

Helen Skelton comments: "For a lot of children gaming is playground currency, especially to kids with older siblings. Mine are no different to other kids and my eldest in particular is showing a growing interest in online games and activities. I am a self-confessed technophobe so, like a lot of parents I am nervous about the world beyond the screen I know nothing about. That's why it's important to me to try and put protections and safeguards in place so I know they can at times play safely online like their peers. I suspect many parents would welcome the chance to put an extra layer of protection in place for their families. Having taken the test and downloaded the SHIELD guidance myself, I now feel better placed to spot the warning signs of gaming fraud. This campaign by Lloyds Bank is really important to raise awareness of all the different ways in which fraudsters can make contact with children and I hope people find the resources on the Lloyds website useful."

Liz Ziegler, Retail Fraud & Financial Crime Director, Lloyds Bank comments: "Sadly, gaming fraudsters do not discriminate and all too often children can become victims of online gaming scams. We want to help bring parents into the world of online gaming to help them understand the types of fraud taking place within games and where the highest points of risks are. Parental awareness and education is the first step in helping to prevent gaming fraud amongst children. Our dedicated quiz will allow parents to test their knowledge on the issue and learn more about the risks before having those critical conversations with their children.



Parents should feel confident when educating their children on gaming fraud and the SHIELD protection is the first step to do just that."

Andy Robertson, Family Gaming Expert and Editor of Ask About Games, said: "Video games are an important way to maintain and extend playground friendships. They play a role in creating connectedness, reducing anxiety, and promoting relaxation. However, it's important parents are involved in this area of their life and encourage open conversations about online strangers and spending. Having conversations about fraudsters and setting up appropriate parental controls ensures that your child's gaming stays positive and healthy."

The Game Players Code

To help parents protect their children from financial fraud, Lloyds Bank with the support of Ukie launched its Game Players Code, providing a six-point guide encouraging players to:

- SCREEN any chats from strangers, as well as unexpected gifts and special edition or time-limited offers. Never transfer money to someone you haven't met in person.
- **HIDE** personal information from others at all times, concealing your personal details where possible to avoid them being leaked.
- INVESTIGATE any gaming-related purchases before handing over money, such as checking whether the website is blacklisted on <u>https://sitechecker.pro/blacklist-checker/</u> and only making card payments which offer greater consumer protections.
- EVALUATE whether gaming-related downloads are being made from established trusted sources and whether they are safe by checking for malware via <u>https://www.virustotal.com/</u>
- **LOCK** your gaming network by using <u>password managers</u>, two-factor authentication within platforms and anti-virus software.
- DELINK your bank details from gaming and online browser accounts. Having two-factor authentication set up on bank transactions and using prepaid cards will also help to keep your money protected.

Parents who are looking for further resources about gaming fraud and how to spot and avoid scams can also visit: https://www.lloydsbank.com/help-guidance/protecting-yourself-from-fraud.html or search for Lloyds Bank's Game Players Code online.

ENDS

Research methodology

All figures, unless otherwise stated, are from One Poll. Total sample size was 2,000 parents of 6-15 year olds in the UK whose child plays video games. Fieldwork was undertaken between 23rd-28th June 2022. The survey was carried out online.

About Lloyds Bank

For over 250 years, Lloyds Bank is proud to have served the people, businesses and communities of Britain.

Keeping customers' money safe is Lloyds Bank's priority and its fraud teams are working behind the scenes 24/7 with the bank investing over £100million in its defences, stopping the majority of attempted fraud.