FRAUD'S NO GAME

A Lloyds Bank report on how gamers can protect themselves from financial fraud

2021/2022

CITY UNIVERSITY OF LONDON EST 1894

ukie

LLOYDS BANK

Contents

Foreword

During the pandemic, many more people have used gaming platforms as a way to pass the time and to stay connected with other people. Gaming provides us with entertainment, a challenge, and a chance to interact with fellow players. So it's not surprising that millions turned to video games while so many restrictions were placed on other aspects of everyday life.

At the same time, we've seen how scammers are becoming increasingly sophisticated and are taking advantage of online social activity in new ways to target their victims. Over £2bn has been lost to fraud in the UK throughout 2021, with 80% of reported fraud cyber enabled.[1] Scammers are often organised criminals, and don't care who they defraud – and that includes gamers.

At Lloyds Bank, helping keep our customers' money safe is our priority and we're working behind the scenes 24/7 on our defences, investing more than £100million in state-of-the-art detection systems to stop the majority of attempted fraud. But it's also vital that we raise awareness of new and emerging threats, so that people are ready to protect themselves as that first line of defence.

Unfortunately, it was not surprising to me that the research underpinning this report found one in five (20%) game players have been - or know someone who has been - the victim of a gaming-related scam. Almost a third (32%) of players we surveyed told us that they are worried about fraud when playing on their computer, mobile or console, while just 8% have seen advice on how they can protect themselves from fraud.

That's why we've teamed up with The Association for UK Interactive Entertainment (UKIE) and cybersecurity experts at City, University of London, to further understand video game fraud and establish preventative advice for players of all ages to help combat fraud. We've come together to create the Game Players Code. This is a simple, six-step guide for players to follow to help prevent scammers from accessing their personal information and protect their money from fraudsters operating in the gaming space.

To help keep game players safe, we're encouraging people to learn about how to protect themselves from fraud, including in the gaming world, and urge players to join us on the frontline in the fight against fraud.

Philip Robinson
Retail Fraud Prevention Director, Lloyds Bank

Executive Summary

Video gaming is becoming an increasingly popular form of entertainment, with consumer spend on gaming-related items up 30% since 2019. Among children aged between 8-15 years old, 40% now spend their pocket money on gaming.[2] According to our study, more than three quarters (77%) of game players in the UK now spend more time playing video games than ever before, an average of 14 hours every week.

However, the increased popularity of gaming also comes with a hidden cost. While more of us enjoy the many benefits that gaming brings, there is an ever-present threat that is often overlooked: gaming fraud.

In this landmark report conducted with City, University of London, we seek to understand more about gamer behaviour in the UK and how this behaviour could make them more susceptible to being scammed. Whether it's obtaining personal details or hacking accounts linked to debit or credit cards, the report shows how criminals are tapping into the growing popularity of gaming to steal people's money.

Our study shows one in five (20%) players have fallen victim to a gaming-related scam or know someone that has. Yet, when it comes to players' knowledge about the different scammer tactics, almost one in three (29%) wouldn't know how to spot a scam. Meanwhile, just eight per cent of UK video game players can recall seeing any advice around how to protect themselves from fraud in video games.

Research also revealed that a fifth of players (20%) admit to sharing personal information - such as their age, birthday, or location – with other players that they haven't met in real life. One in six (15%) admit to playing regularly with others they do not know, while one in seven players (14%) would even consider transferring money to someone they had met online through a game but had never met in person.

These valuable insights have helped to inform a six-step Game Players Code using SHIELD, a guide designed to help people enjoy gaming safely.

Key findings

- Three in four **(77%)** play more now than ever before
- One in six **(15%)** play online with people they don't know
- A third **(32%)** of game players worry about fraud when they play online
- One in five **(20%)** know of someone who has been a victim or target of gaming fraud
- Two thirds **(66%)** of players have not seen any advice for how they can protect themselves from fraud when playing

CITY UNIVERSITY OF LONDON EST 1894

Professor Muttukrishnan Rajarajan, Director, Institute for Cyber Security and Professor of Security Engineering, City, University of London:

"Our study shines a light on how gaming is an emerging arena for fraudulent activity, and it is an important contribution in understanding how scammers are using gaming platforms to dupe their victims. Alongside this, it's becoming easier for fraudsters to harvest personal data through phishing and app collusion, while players not upgrading their devices or software regularly is providing a backdoor for fraudsters to exploit these vulnerabilities. With gaming interactions and the technological capability of fraudsters only set to advance, City, University of London is proud to be providing academic expertise on gaming-related cybersecurity issues and working with Lloyds Bank to help protect players."

ukie

Dr Jo Twist OBE, CEO of Ukie, said:

"We know that the vast majority of people have fun, positive experiences playing games online. But as with all walks of life and all parts of the digital world, there are some people out there who will try to take unfair advantage of safe spaces. The Game Players Code is a great way for players of all ages to think about how they can reduce their exposure to the small risk of financial fraud in games further and is a useful tool for fostering digital literacy across wider society"

The rise of gaming in the UK

Gaming became a natural pastime for many to turn to during the 2020 lockdowns. Playing games offers entertainment, a challenge, and a much-needed distraction at a difficult time, but also the opportunity to connect with people you can't see in-person.

With more than three-quarters (77%) of players saying they were spending more time playing games than ever before, and a fifth (19%) adding that playing was, for them, an alternative way to socialise, it's no surprise that the UK's gamer population grew by 63% in 2020.[3]

More than nine in 10 (92%) players aged 18-24 say they were gaming more during this time. On average, UK players now spend 14 hours a week playing video games, which rises to 17.3 hours amongst those aged between 13 and 17.

When it comes to the types of games people are playing, more than half (55%) of people enjoy the thrill of solving problems and puzzles, while a third (34%) are driven by the feeling of winning. Connecting with real-life friends (18%) and collaborating with others (18%) are also key reasons people love gaming in the UK.

Playing games is becoming ever-more socialised, with younger people embracing multi-player games as a new way to meet people. However, as in-game chats and multi-player games increase in popularity, so does the risk that personal information may end up in the wrong hands.

Key findings

of players aged 18-24 say they were gaming more during lockdown

of players say they were are spending more time playing games than ever before

of players enjoy the thrill of solving problems and puzzles

of players are driven by the feeling of winning

of players added that playing was, for them, an alternative way to socialise

The threat of gaming fraud

Fraudsters are often organised criminals on the lookout for new platforms and mechanisms to target victims. Following the shift in day-to-day interactions and spending from in-person to online platforms during the pandemic, they have become increasingly sophisticated in the ways they are obtaining personal information and duping people into making authorised push payments (APP) under false pretences.

According to UK Finance, £754 million was lost to fraud in 2020 in the UK – representing a 30% year-on-year rise, with much of the criminal activity taking place outside the traditional banking system.[4] At the same time, the number of scam attempts made every day is rising and is placing greater pressures on families. Recent research by Lloyds Bank reveals that 86% of parents are worried about a family member falling victim to fraud.[5]

With gaming console fraud, whereby scammers trick victims into buying consoles that they then never receive, amongst the most common types of purchase scams reported to Lloyds Bank[6], our study commissioned with City, University of London highlights how the gaming world is proving an attractive arena for scammers to operate in.

When it comes to the tactics scammers use to target their victims, phishing emails are found to be the most common (36%), whereby fraudsters send an email to players telling them they need to confirm their password and login information to obtain access to their accounts. In-game chats (32%), where fraudsters build relationships with players so they trust them with personal details, and malware installation (28%), where users are prompted to download a plug-in which installs malicious software onto their device, were other common scammer methods identified.

How fraudsters are targeting gamers:

The most common scammer tactics:

1. Phishing email or text
2. In-game chat functions
3. Malware installation
4. Impersonation of in-game support

Player under 21

"When you're playing games, you don't have a lot of time to think so you make quick decisions. If you're doing that in real life... you can end up making some wrong decisions. If my mum comes in to speak to me, I block her out because I'm focussing."

Player in their 20s

"I had assumed there'd been a rise in gaming fraud over the pandemic, but the amount of identity fraud is really worrying."

In terms of game players' knowledge about different scammer tactics, almost one in three (29%) wouldn't know how to spot a scam. People who mostly play puzzle-based video games (52%) are the least likely to know what to look out for, while simulation games (64%) and platform games (65%) were also amongst the lowest scores. Additionally, those playing on their mobile (56%) or tablet (57%) are less likely to be able to identify a scam than those who play on gaming consoles (67%) or a desktop PC (68%).

Exploring this further, Lloyds Bank and City, University of London ran focus groups to understand players' motivations and emotional drivers behind playing video games, and why these behaviours might make players more vulnerable to fraud. These groups included players aged under 21, players aged over 21 and the parents of players.

In the player-specific focus groups, it was found that the level of security checks made when making connections with people are reduced in-game compared to in-person, as the ability to verify the age, profile and true intentions of other players becomes more difficult. In addition, the excitement gaming brings can reduce players' inhibitions, making them less cautious about running security checks.

The study found that the level of trust players has towards strangers is higher, making them a higher risk of being susceptible to fraud.

The focus groups also highlighted how multi-player gaming creates a pressured environment, making players feel like they need to constantly perform at their best. It was found that the fast-paced nature and intensity of multi-player gaming can cause people to make rash decisions or block out their surroundings or other sources of information, which again could place them at higher risk of being duped by scammers.

When asked to consider the negative impacts of gaming, players highlighted the dangers of speaking with strangers – but didn't name fraud or scams. All bar one in the under-21 focus group had never heard of gaming fraud prior to the focus group – with the remaining participant saying they had heard of it but knew very little about it. Meanwhile, amongst the over-21 player focus group, not one respondent said they felt concerned by fraud, or that they were personally at risk.

Within the parent focus groups, they were aware that in-game conversations with strangers were taking place and recognised the benefit of gaming for socialisation. However, it was raised that multi-player gaming environments had led to instances where personal information such as name, age and address were shared with strangers.

Summary

From the ability to build relationships with strangers in-game to the time-pressured decisions involved in gameplay, the environment in which video games are played in is providing scammers with new ways in which they can steal people's money. The next section of the report looks at where the biggest vulnerabilities lie when it comes to the fraud risks people face when playing.

Parent, aged 65, of two players

"Tom played quite a bit with his schoolmates, but also games like World of Warcraft, where he was forming alliances with total strangers. One time, we had an odd experience which put him off playing with strangers altogether.

Tom received a postcard at our address from a stranger in America asking how he was, and why he hadn't been online playing World of Warcraft recently. We had no idea who this guy was or his agenda, and we weren't very happy with that at all. It was when he was younger, but it was a bit of a wake-up call as he had obviously given out his address to receive this unsolicited communication. We were unaware this was going on."

Identifying the gaming fraud risks

1 Leaking personal information

One of the most worrying fraud risks identified by the study was the willingness of players to share details with people they do not know when playing video games. In fact, one in five (20%) gaming Brits says they have disclosed personal information – such as their real name, birth date and location – with a player they have never met in real life. Nearly three in ten (29%) players say they trust their personal information with strangers they play with. Interestingly, female players (24%) are less trusting of other players than their male counterparts (35%).

The sharing of personal information increases the ability of fraudsters to access players' gaming accounts and, as a result, increases the risk of them being scammed out of money. In fact, players' top concern when it comes to gaming fraud is hackers being able to access their accounts. With almost one in four (23%) players having their bank details automatically saved either within gaming accounts or online browsers, those successful in hacking gaming accounts could use linked debit or credit cards to purchase items fraudulently.

2 Purchasing fake gaming add-ons

Add-ons such as in-game currencies, skins, new abilities, and level-ups are a big part of gaming culture and the focus groups highlighted how, for many video game players, these additional purchases are a must-have for enhancing their in-game experience. Our research shows that nearly half (45%) of players make additional purchases using real money, with the average player spending £141 on in-game items in the past year alone.

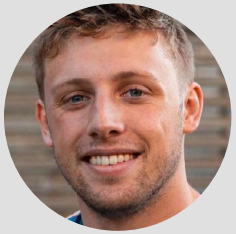
However, with spending on gaming add-ons on the rise, fraudsters are taking advantage and using in-game chat functions and phishing emails to trick their victims into making direct bank transfers for add-ons that they never receive.

Within the player focus groups, there were people who knew friends and family who had fallen for scams after making purchases from fraudulent websites to get the best players or equipment in the game. One in seven (14%) players told us that they would consider transferring money to someone they met online through a game yet had never met in person. This, combined with the social pressure players face to purchase gaming add-ons, is putting them at an increased risk of bank transfer fraud.

Player in their 20s:

"I got a notification through to my phone that there had been an unusual log-in to my gaming console account from Saudi Arabia, which clearly wasn't me. I then tried to load up my account and I realised that my email address had been changed and I had been locked out. I immediately contacted my console's customer support team, who were able to reverse the account back to me once I verified the console serial number.

"It turned out that the fraudster had managed to change the name, email, password and other account details, while also having the capacity to spend money on the debit card linked to my account. I didn't have two-factor authentication set up, which means they could have completely drained my bank account which is quite scary."



Harry Lewis, YouTuber and member of The Sidemen:

"I've been gaming for years now, and I've never seen any advice on how to stay safe from fraudsters. You can interact with so many different people from all corners of the world whilst playing, which is amazing, but does comes with risks. Often people are far too trusting of other players, and with scams on the rise, we need more education and advice about how to stay safe."

"When I was younger, I was scammed on FIFA by a duplication glitch and lost a lot of coins I'd worked hard to save. I was carried away and let my guard down to a stranger – this really brought home that I need to be protecting myself from scams. Fraud isn't something that's often talked about in our community, but that needs to change, so that we all know the tell-tale signs of a scam."

Identifying the gaming fraud risks

3 Downloading malware

Fraudsters are using coding to infect downloadable games or a plug-in for a game with viruses, otherwise known as malware. Installing malware can allow scammers to view the private messages of players, take remote control of devices and gain access to your passwords, address, or other personal details that increase your fraud risk.

Our study shows that, amongst those with experience of gaming fraud, malware installation is the third (28%) most common way in which the scammers were able to dupe their victims. Despite the risks, almost half (46%) of players make no security checks at all when downloading new games, with those under 18s almost half as likely to make security checks compared to those aged 18-34 (25% v 42%).

Amongst those that do take precautions, almost half (45%) use antivirus software to detect for malware while more than a third (37%) check the validity of gaming sellers before downloading new games.

Summary

Our study of gaming behaviour and player attitudes towards keeping themselves safe uncovers several areas where the risk of being defrauded, and therefore where the need for preventive advice, is heightened. The next section of this report details the actions that video gameplayers can undertake when playing to reduce these risks.

Player, London in their 20s:

"If you want the best pack or the best skin and someone comes to you with an amazing offer, it's understandable why you would fall for it."

Parent of gamer aged 18:

"My son has spent money in-game that he wasn't aware of or didn't mean to. It's when kids are in their early teens that they're most vulnerable with in-game spending, and that, for me, is where the education and information need to be there for both kids and parents. Scammers are very clever, so however on it you think you are, they'll find a way to catch you out."

Mum of twin players aged 14:

"Our kids have a lot of friends that live in different countries; some are friends they have met in-person and others are friends they have met online. But some have bigger funds, and therefore if you're not getting far enough into the game compared to your online friends, then they want to buy their way through. I'm often pressured by my kids to buy these level ups, but I think they should earn it."

Player aged over 21:

"The idea that 'I'm older and know better, so it's never going to happen to me' – actually makes you more vulnerable because you're less on the lookout for it."

How players can protect themselves

As part of its longstanding commitment to protecting customers' from fraud, Lloyds Bank has partnered with UKIE and City, University of London, to create a Game Players Code, an easy-to-remember six-point guide to help players identify financial scams and avoid falling victim to them.

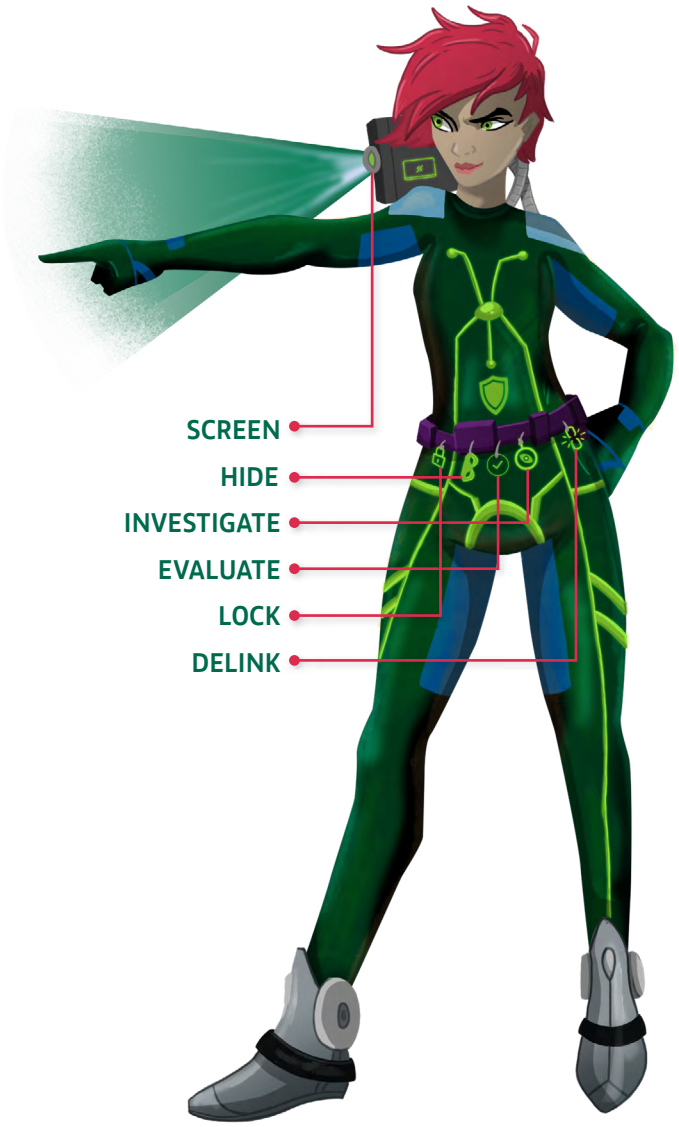
To help players remember what they need to do to protect themselves from financial fraud, Lloyds Bank is introducing the Guardian of the Game Players Code – a visual representation of the six-point guide of preventative advice.

As part of its Fraud's No Game campaign, Lloyds Bank has also teamed up with "W2S", aka Harry Lewis of the YouTube video game group The Sidemen, and gaming influencer Clare Siobhan to raise awareness about the risks of gaming-related scams and encourage their followers to SHIELD themselves against scammers.

The Game Players Code SHIELD, stands for:

- **SCREEN a**ny 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 https://sitechecker.pro/blacklist-checker/ and only making card payments which offer greater consumer protection.
- **EVALUATE** whether gaming-related downloads are being made from established trusted sources and whether they are safe by checking for malware via www.virustotal.com
- **LOCK** your gaming network by using password managers, 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.

GUARDIAN OF THE GAME PLAYERS CODE



How parents can keep their children safe

As a parent, keeping your children safe is the ultimate priority but it can be daunting when you don't know what you're up against. At Lloyds Bank, we take the concerns of parents seriously and stand by their side in keeping relatives safe from scams.

That's why, as part of our study, focus groups were conducted with parents of gamers to better understand their worries around gaming fraud, and to establish effective ways in which they can protect loved ones.

When it comes to all types of fraud, those aged 18 – 34 are almost three times more likely to fall for a scam than those aged 55+, it's important for parents to know that there are steps you can take to ensure that your child knows how to spot a scam and how they can reduce the risk of them falling victim when playing games on their computer, console or mobile device:

> *When it comes to all types of fraud, those aged 18 – 34 are almost three times more likely to fall for a scam than those aged 55+*

Kickstart a fraud conversation

Making young people aware to the threat of fraud is a crucial first step in getting them to change their behaviour so that they are protecting themselves from scammers. Choose a moment during your child's downtime, where you have their full attention, to understand their gaming habits, who they are speaking to when gaming and what about. This will provide an opportunity to talk about how changing their behaviour could reduce the risk of them falling victim to fraud.

Keep check of their gaming spending

Whether your child uses your debit or credit card for gaming-related purchases, or whether they use their own card details, it's important to check in on what they're spending to identify any unusual or risky transactions. It's important to remind them that if they are ever unsure about a purchase they are making, or if something sounds too good to be true, then they should speak to you for advice before parting with their money.

Remind them how they can SHIELD themselves from scams

To help you understand and communicate the ways in which your child can protect themselves, Lloyds Bank has partnered with UKIE – the UK's gaming industry body – to create the Game Players Code. Ask your child whether they know how to spot a scam, and search for Lloyds Banks's Game Players Code online for more information.

Gaming YouTuber Clare Siobhan, comments:

"It's not surprising that gaming has become so much more popular since the start of the pandemic, and it's really exciting that more people are joining our community. However, on the flipside of this growth, it's shocking to see how scams are becoming increasingly common amongst players, and fraudsters are taking the fun out of what should be creative, exciting and a way to connect with likeminded people."

"The work of Lloyds Bank and UKIE to raise awareness about the dangers of gaming is so important: when I share content about buying gaming add-ons and skins to enhance their gaming experience, viewers will often comment that they've been tricked by a fake website or accidentally downloaded malware. It's so important that we're teaching players, young and old, how to stay safe whilst gaming and how to spot the warning signs of a scam."

Summary

Working with industry partners and experts in the field, Lloyds Bank has undertaken a comprehensive study to uncover the fraud risks presented to players and, crucially, how they can take preventative steps to protect themselves from falling victim to a scam. In addition, it has underlined the importance of video game players and parents alike uniting to combat gaming-related scams, and joining Lloyds Bank on the frontline against fraud.

For more information about Lloyds Bank Fraud's No Game campaign, and how to protect yourself from fraud when playing video games, visit [link to be inserted] or search for Lloyds Bank Game Players Code online.

About the Research

The survey was conducted by Opinium Research between 13-20 August 2021. The study group included 2,002 UK players who play games online at least once per month. In addition, Lloyds Banks's PR agency Grayling conducted three online focus groups during August 2021 with players aged 13-20, players aged 21-45, and parents of players, in accordance with standard market research practices.

Contact

For further information please contact our Press Office team on lbgconsumer@grayling.com

References

[1] Action Fraud, www.data.actionfraud.police.uk/cms/wp-content/uploads/2021/07/2020-21-Annual-Assessment-Fraud-Crime-Trends.pdf

[2] Lloyds Banking Group, Pocket Money Index 2021. Survey conducted by OnLineBus and a sample of 1,000 GB children aged 8-15 were interviewed.

[3] www.opinium.com/gaming-in-the-time-of-covid-19-the-rise-of-covideogamers-and-how-to-retain-them

[4] UK Finance, September 2021

[5] Lloyds Bank, Frontline of fraud 2.0, June 2021

[6] Lloyds Bank, customer complaints about purchase scams between February 2020 and February 2021