

Scalpers are using bots to exploit your customers

Customer satisfaction, trust and loyalty is front of mind for nearly every company in the world. What if there was a threat that could destroy that, simply by purchasing your products faster than anyone else and selling it for higher prices?

That is exactly what scalpers are doing and they are using highly sophisticated, often undetectable, bots to do it. The pandemic has impacted the supply of many products and pushed consumers to become increasingly comfortable purchasing online. This has created a huge market for scalpers who have now built up the scale and resources to operate like multi-national companies.

In this paper, we explore where this challenge has been faced before and the potential implications on your business and for your customers. We also talk about where we think the scalpers will go next and investigate what you can do to protect your business now and in the future.

This is not a new challenge



What is a scalper?

Scalpers are people (and these days commonly groups of people) who buy products that are often difficult to get and sell them at much higher prices.



References to scalpers date back to the 1800s

Scalpers have been capitalising on in-demand items to achieve large profits for a long time. **It is not a new business**, with references to such activities even dating back to the 1800s where rail tickets were sold in America on secondary markets. Since the turn of the 21st century, scalpers' capabilities have increased thanks to a helping hand: bots...

Along came the bots

Bots are automated pieces of software, that allow users to complete online activities at a much higher speed than humans. Bots were originally used to automate certain tasks and improve the speed, ease and accuracy that any human could achieve. However, just like any technology, bots have been misused and repurposed for a more malicious intent.

Scalpers used bots to strengthen their abilities to make a profit. Bots increased their speed of purchase, widened their scope to multiple industries and extended their reach to a global scale.

The most common type of bot is the All-in-One (AIO) bot. AIO bots work by scanning multiple pages on different sites, hundreds of times per second. The most advanced bots are able to bypass most security measures and purchase at scale.



Scalping was most prevalent in the ticketing industry

In recent history scalping has been most **prevalent in the ticketing industry**, with the biggest music concerts and major sporting events being two of the main victims. Vast amounts of the best tickets were bought by scalpers and then resold to dedicated fans willing to pay over the odds to get their hands on a ticket. Scalpers exploited fans in this way for a number of decades.

Bots sweeping up and causing instant sell outs

While online ticket sales gave fans greater accessibility to events, it also gave scalpers armed with bots greater opportunities. Throughout the 2000s and 2010s, we saw **sold-out events all over the world fall victim** to bots. Broadway musicals, concerts and boxing fights to name a few. Minutes after the primary sale, boxing tickets were available on secondary sites for absurdly inflated prices. A \$10,000 seat was listed at over \$140,000.





Governments were forced to step in to the ticketing industry

With many high-profile cases and the issue only growing, **governments were compelled to step in**. The Better Online Ticket Sales Act (BOTS Act) was signed in the US in 2016 to protect fans from ticket scalping, and similarly in 2018 the UK government outlawed online ticket scalping. New legislation banned ticket scalpers from using automated software to buy more tickets for events than they were allowed. Laws also demanded more information from sellers on secondary ticket sites to further protect consumers from rip-off prices.

Scalpers turned their attention to other industries

Despite legislation against online ticket scalping, product **scalping remained legal** in other industries (and still is). The scalping of limited-edition trainers became widespread, with consumer hype and celebrity endorsement driving the demand that scalpers thrive on. Some consumers (now collectors) see trainers like art. As well as trainers, scalpers have targeted some of the most wanted gadgets and Black Friday deals. The growing **reliance on e-Commerce** has a big part to play in driving this problem in the retail industry. An emphasis on consumer hype and limited stock to drive sales has further fuelled the issue.



And then came the global Coronavirus pandemic

Growing e-commerce trends had already created a hunting ground for bots and then the world was hit by the global Coronavirus pandemic in 2020. The impact that the pandemic had on consumer trends and supply chains further exacerbated the problem of scalpers utilising bots. **Consumers were forced to shop online** more than ever, and many businesses had to shift focus to e-commerce models to remain afloat. The increase in online activity presented huge opportunities for scalpers, compounded by **limited supply of certain in demand products**. Items targeted include home gym equipment, graphics cards and even swimming pools.



The most notable victim throughout the pandemic was games consoles, with businesses and consumers fighting a global battle. Bad press has not only impacted businesses selling the consoles but caused significant damage to the brands themselves. Sites have refused to sell the products because of the risks and challenges their site would face. In December 2020, MPs in the UK tabled a motion to prevent the re-sale of games consoles and computer components above retail price. Although it is in discussion it will take time to materialise as legislation, so expect the challenge to persist and grow.

E-commerce trends suggest that the pandemic shifted the way people shop and how businesses sell for the long-term. While it is hard to predict what is next, the recent trends have demonstrated that this is no longer just an issue for products of limited supply. One thing for certain is that **scalpers are broadening their target sphere**.

You are facing groups with unprecedented resources and scale

Scalpers using bots have been posing problems for a while so why are we talking about it now? What has changed? The answer lies in who you are up against. It is no longer individuals, but groups and forums who are operating like actual companies – with resources to match. It has transformed from a side-job and hobby, to a full-time job for many. The pandemic in 2020 compounded this problem but whilst the pandemic will end, the threat of scalpers and their bots is here to stay.



Scalpers are now operating in globally connected groups

Past

Individuals in isolation:



For many scalpers this is now a full-time job and they often operate in small teams of experts. However, one challenge on a more substantial scale comes in the form of “cook groups”. Cook groups are large communities of individuals and teams from across the globe who connect online, pool their resources together and form a single, significant force in the market.

Clusters of scalpers:



It’s not just the scale of their resources that makes these groups powerful (more of that in a moment) but it’s their collective nature too. These are communities of people sharing knowledge to circumvent controls. This means your security teams are fighting against thousands of minds working together to break controls. Once one person finds a way to circumvent a control, they all have. It’s this collective force and sharing of knowledge and skills that is perhaps their big asset.

Networks connecting globally:



On top of running communities, bot developers also sell their bots to others, which only increases the challenge exponentially. After many people found themselves with more time and limited income, the pandemic in 2020 compounded this rise in casual bot users around the world and those joining cook groups. With the ability to recover their money quickly, consumers are purchasing bots as the only way to obtain the items they want. As the saying goes, if you can’t beat them...

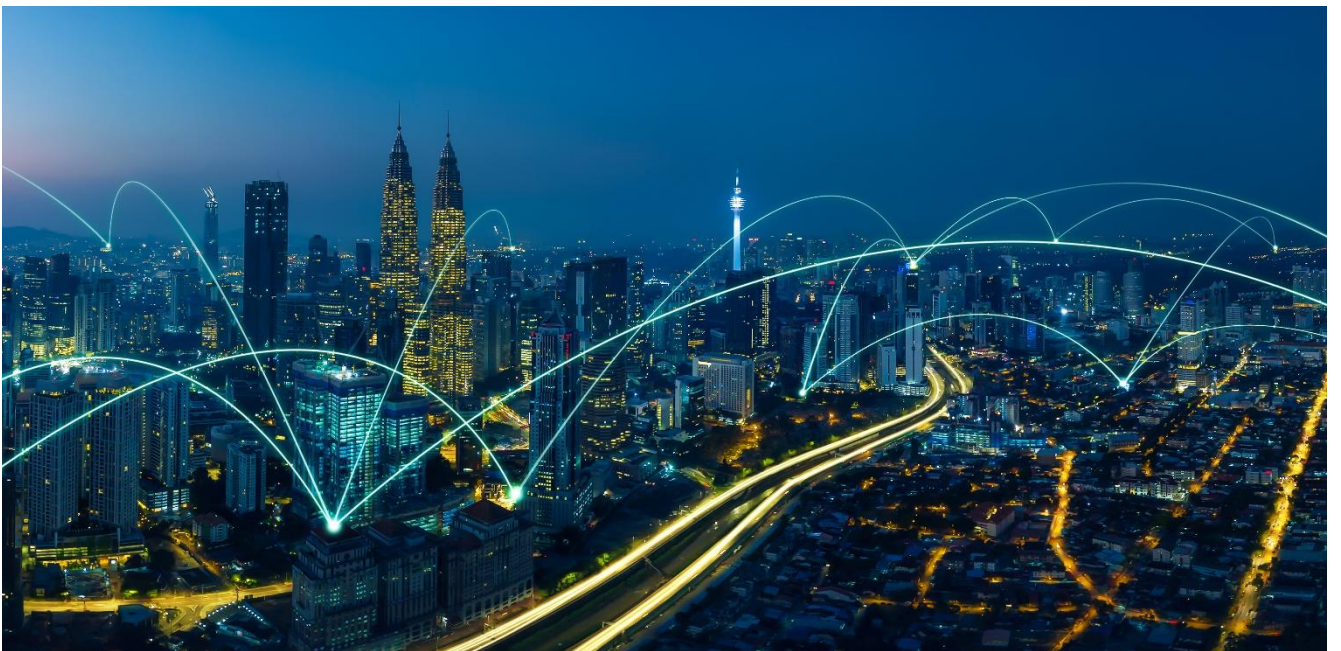
Present



These globally connected groups have the resources of multi-national companies

Groups of scalpers around the world are operating at unparalleled scale and have unprecedented resources at their disposal. In January 2021, a UK-based scalper claimed to have secured two thousand game consoles. This represents an investment of about £1million, with profits likely to double that.

These groups have turned into commercial businesses. They employ individuals, have marketing plans, use PR strategies and receive significant investment. Individuals can join cook groups and receive advice on what products to target, which bots to use, how to create their own bots, and more. There are hundreds of such groups that can be joined, and ironically even subscriptions to these groups can sell out quite quickly!



Why should you care?

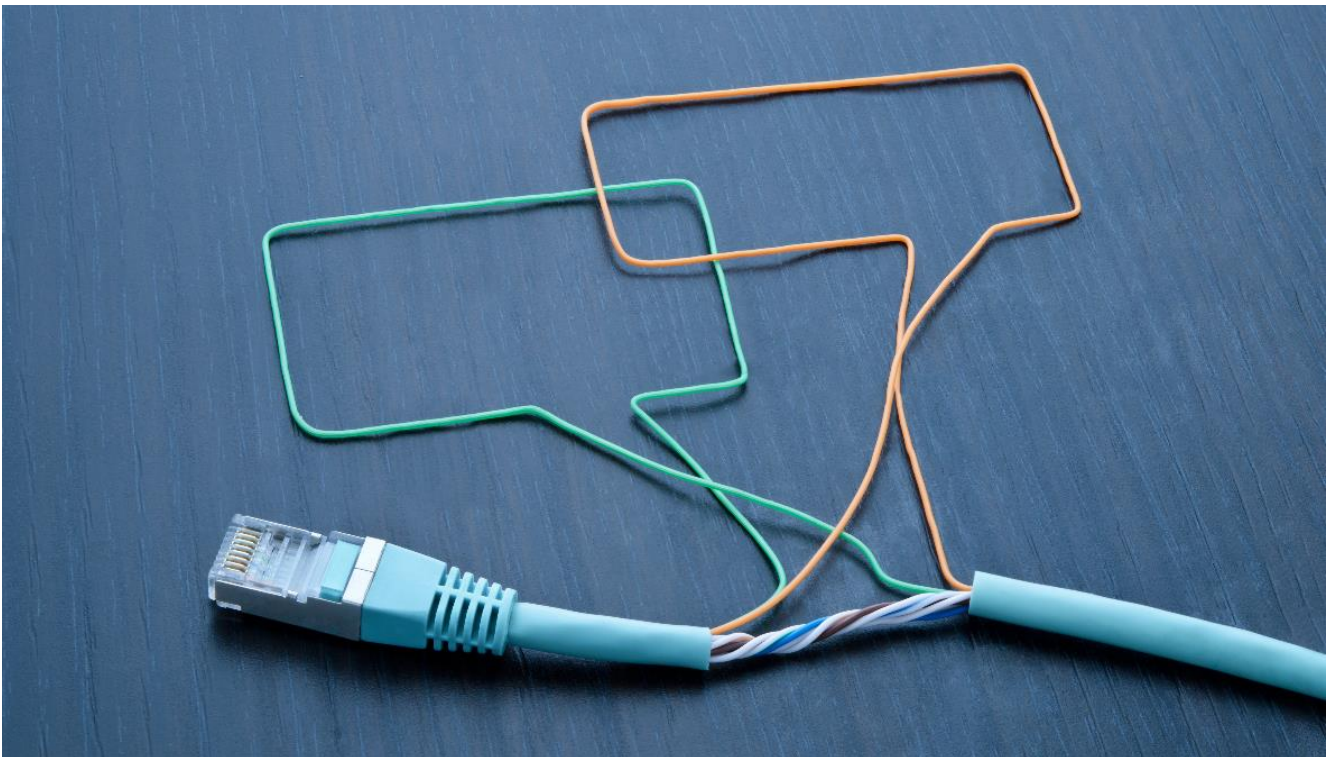
In a world where competition is rife and choices for consumers are endless, as a business it is more important than ever to put your customers first. A loyal, happy customer is critical for success, so ensuring there is a focus on customer trust is key. Scalpers and their bots pose a significant threat to this customer-centric drive. The potential impact on businesses must not be underestimated: brand reputation, future supply and entire business models can all be damaged.

Quotes from genuine customers impacted by scalping and bots

“Overall, I feel like it would be easier to get one of Willy Wonka’s golden tickets.¹”

“This is a launch disaster....Scalpers can keep them.³”

“The bot scalpers have got them all again. At this point, not worth trying anymore.²”



¹ <https://www.businessinsider.com/playstation-5-launch-day-us-europe-flooded-by-reseller-bots-2020-11?r=US&IR=T>

² <https://comicbook.com/gaming/news/ps5-restock-order-buy-game-carnage/#3>

³ <https://www.bloomberg.com/news/articles/2020-12-16/playstation-5-scalpers-use-bots-to-hunt-down-scarce-consoles>

The impact on B2C organisations can vary compared to B2B organisations:


The impacts on Business-to-Consumer (B2C) organisations




As a B2C company, ensuring you give customers the best experience, retain their loyalty and build their trust is key to sustainable success. Scalpers are disrupting this and leave customers with 3 options: they do not purchase the product they want, they overpay scalpers, or they turn to alternatives in the shape of your competitors. Either way, customers will be left unhappy as a result of their experiences. Scalpers might be the root cause of this anger, but it's B2C companies where it is often directed.

 Long-term reputational damage

The struggles customers face when trying to purchase their most-wanted products can inflict long-term reputational damage to a B2C company. As the problem grows so does the media coverage around such events, which has the potential to cause significant brand damage. Customers will start to go to competitors (or to the scalpers) – ultimately losing you profit and future sales.

 A threat to your third party relationships

While ensuring customers return to purchase certain items B2C companies must also ensure they are able to stock those products in the first place. As a B2C, implementing measures to protect against bots will not just protect your business but will protect your supply. If you cannot demonstrate this to manufacturers they might allocate their stock elsewhere, among your competitors.

 Damage to your wider portfolio of products and other customers

A damaged customer experience can have knock-on effects to your wider portfolio and customer base. As bots are deployed in their masses, sites will crash and customers will be physically cut off from the rest of your products. Recent examples have seen companies having to set up and run a separate site dedicated to a certain product just to protect the rest of their portfolio.

 Increased risk of fraudulent activity

Providing the endpoint sale makes B2C companies susceptible to fraud. Bots have multiple cards at their disposal to help bypass controls, increase opportunities and gain from even greater profits. They often use fraudulent credit cards, and the liability of accepting a fraudulent transaction would lie with the B2C themselves. In a digital world where financial crime is already rife, scalpers only had to the problem.

The impacts on Business-to-Business (B2B) organisations



While focussing on individual customers helps to drive successful B2Cs, B2B companies must also employ similar approaches. In this case your customers are other businesses, but trust and loyalty is of equal importance. Not only this, but because B2Bs are often manufacturers of certain products, brand reputation is another crucial success factor. As a B2B company the potential impacts are often out of your control – it's the B2C's e-commerce platform where bots will look to target.



Long-term reputational damage

Long-term damage on brand reputation can have multiple implications. Customers might start to purchase alternative products, leading to a loss of profits and market share. And not only would brand damage put customers off purchasing products targeted by scalpers, but they might also stop buying other products amongst your wider portfolio, damaging long-term sales and profits. A strong brand and customer trust are built over many years but could be shattered instantly thanks to scalper and bots.



Future supply becomes hard to forecast and plan

Groups of scalpers operate internationally and they will often buy where supply is high and sell where demand outstrips supply. With scalpers reselling large amounts of products (and effectively becoming the B2C), businesses lose visibility of key trends relating to demand which makes it almost impossible to understand where future demand will come from. Where do we need to focus efforts? What does future supply look like? These are some questions that suddenly become a lot harder to answer.



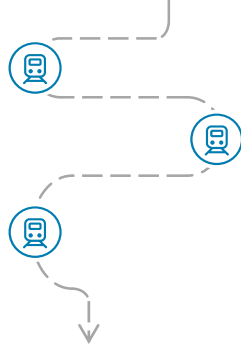
A loss of third party relationships

As a B2B company, the end customer is not the only party you need to be concerned about. As the bots challenge grows and problems mount, B2Cs might be reluctant to stock certain products. In early 2021 we saw some B2C organisations refusing to sell a certain tech product on their platform because of the impact the traffic would have on their site. If this becomes a common problem for B2B companies, it could present a real challenge in ensuring their products reach the end consumer.

Could your industry be next?

With the impact being widespread and causing long-lasting damage, appropriate measures will need to be put in place. Although recent examples have been most prevalent in the Retail industry, it isn't just limited to this industry.

As trends show, scalpers leveraging bots is a constantly evolving industry itself and **their target sphere has no bounds**. So, what industry could be next? What will be the next product targeted? In the next section we explore some of the areas which could well be impacted in the near future. And it's not as obvious as you might think.



What is the next target?

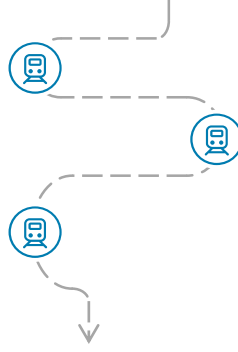
While it's impossible to predict the next unprecedented event one thing clear is the growing scope and challenge posed by scalpers and bots. As scalpers' capabilities and resources grow, they see and capitalise on the next opportunity.

While technological advances have given consumers greater accessibility to the goods they want, it also adds fuel to the fire. Industries around the world are becoming increasingly reliant on e-commerce, making them more susceptible to bots. It's not just a reliance on e-commerce from businesses but consumers too. Consumers are now more used to buying online and a wider audience are much more comfortable doing so, the way people shop has shifted for the long term.



The next big tech drop?

As the reliance on e-commerce grows, for consumers and businesses alike, it's becoming more and more feasible that any consumer product sold online could fall victim to bots. The latest big technology drop always attracts a lot of attention with consumers eagerly awaiting release dates. This is often one factor instrumental in drawing in groups of scalpers. With game consoles already impacted, could we see smartphones next to be targeted? The next generation of smartphones continues to evolve at speed, and when the next cutting-edge device lands there is always a long queue waiting to be the first people to own that device. Whether one with new-found processing capabilities, the latest AI or internet generation integrated, or perhaps a foldable phone. The buying behaviour of these customers and their demand for the latest device could create another ideal target for scalpers to utilise bots.



Collectible items

Industries for all generations could suffer. **Collectible toys** can send children crazy and in turn compel parents to purchase certain items at all costs. As it becomes easier and easier for these groups of consumers to purchase these collectibles online, it could become another lucrative avenue for scalpers to deploy their bots. This issue would become particularly prevalent at times like Christmas where demand for children's toys is very high.

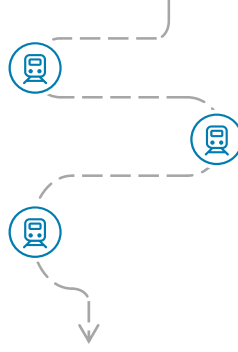
While collectible toys for children could be next, another rewarding target for scalpers could be collectible "toys" for older generations: **cars and watches**. Although much lower in terms of numbers manufactured, scalpers could employ the same techniques to snap up a very sought after but rare edition car or limited-edition watch. With high net worth individuals willing to part with boundless amounts of cash, scalpers could realise large profits in this industry.

Luxury goods

Methods used by bots to target the high net worth individuals could also be extended and further applied to other luxury goods – one in particular being high-end fashion. **Handbags, clothing and jewellery**.

We see production numbers for some of these products in the single digits, with each item retailed at 6+ figure fees. If scalpers utilising bots are capable of sweeping up and owning every item released, they would find themselves in a very powerful and an extremely lucrative position.





Commodities

But as scalpers widen their scope and their bots become increasingly more capable, we might even see the impact spread to less obvious, less consumer-focussed products. Commodities could present scalpers with an alternative but just as rewarding industry. **Gold and silver** are just two examples where when individuals (or groups) build large stockpiles of a certain commodity, they can find themselves in a very commanding position. And when we flip our attention from consumer products to commodity goods, we start to see the wider impact that could be had. Take **crude oil** for example, if this was to be successfully targeted by scalpers then not only will there be ramifications for businesses and manufacturers, but for wider society too. This could start to have an impact on everyday life and suddenly seems a whole different problem.

While some of these examples might seem implausible, this is the very trait of an unprecedented event. They are unparalleled, and never experienced before. But understanding the magnitude of the challenge and deploying appropriate measures to protect against scalpers and their next move is the only way to ensure these events remain implausible...

What can you do to protect yourself?

For many industries scalpers present a relatively new threat. Businesses quickly learn there is no silver bullet. A **multi-layered defence** is needed, however it's not just as simple as implementing a set of controls.

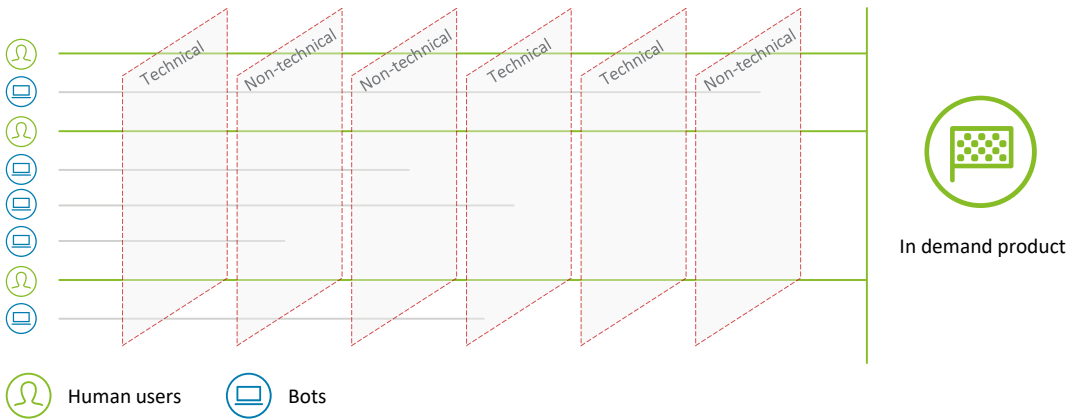
- Controls must be **specific** – apply them with context and cater for the threat profile you are protecting against
- **Continue to adapt** your approach. Scalpers have the resources and hunger to adapt and change their approach, so your measures must evolve even quicker to ensure you are always one step ahead.



What can I do as a B2C?

Scalpers target the endpoint sale via a B2C's e-commerce platform, it is at this point where most measures can be deployed to stop the bots. A multi-layered defence of technical and non-technical controls will protect your customer base and future profits and also demonstrate to others you are deploying appropriate measures.

Multi-layered defence of technical and non-technical controls



Non-technical controls Non-technical controls can deter scalpers and reduce their power. Setting purchase limits and validating proven human users can be effective measures. Verifying who your real customers are gives you confidence you are selling to proven human users. This can be useful information when implementing a host of non-technical controls.

Technical controls A combination of technical controls will significantly bolster your defence. As with all controls, it is important that they are contextual and specifically target the bots. Using CAPTCHA tests, configuring Web Application Firewalls (WAFs), implementing specialised detection and monitoring tools can all help to detect and eliminate bots. Understand the type of boots you are up against and use the most relevant controls.



What can I do as a B2B?

A big challenge for B2B organisations is the lack of control on the endpoint sale and e-commerce platforms where consumers are buying their products. Measures to gain greater control and fight the challenge with others can be effective and significantly reduce the impact felt.

- Gain greater control on third parties** Ensure contracts oblige retailers to take effective steps in mitigating bots. This then gives you a basis to assure and validate that third parties are indeed taking appropriate steps to protect your products from scalpers on their sites.
- Monitor the situation** Monitoring activity and conversations on social media gives you insight to measure the impact of controls implemented by you and retailers. It can also detect potential brand damage and a loss of reputation across the global social media sphere.
- Team up and share knowledge** Scalpers' collective force is what makes today's threat so challenging. Play them at their own game. Team up with others, co-innovate together and share knowledge. Sharing data on scalpers and embellishing your knowledge with intel from other organisations will give the ability to prevent bots faster and more effectively.



How can Deloitte help?



Breadth of capabilities

We understand the scale of the challenge. From security to fraud, we have the understanding and capabilities to address this multi-faceted challenge and enable your multi-layered defence.



Depth of experience

This is a new threat to most industries. However, with experience in anti-fraud, cyber security controls, third party reviews and monitoring services, we have implemented controls to fight similar challenges.



Passion to safeguard businesses and consumers

Our purpose at Deloitte is to make an impact. A large part of this is safeguarding businesses and the wider society too. We share an interest to help protect both parties in this fight.



Knowledge sharing

We can be a reliable partner to co-innovate with you and facilitate sharing of information. We are in a position where we can embellish your knowledge from intel across the market and other areas to better equip you.

Contact us

If you are interested in this topic and would like to have a conversation with our team, please don't hesitate to reach out:



Susan Sharawi
Cyber Risk TMT Lead
ssharawi@deloitte.co.uk



Nick Seeber
Risk Advisory Media & Entertainment Lead
nseeber@deloitte.co.uk



Hasan Muchhala
Cyber Risk SME & Author
hmuchhala@deloitte.co.uk





This publication has been written in general terms and we recommend that you obtain professional advice before acting or refraining from action on any of the contents of this publication. Deloitte LLP accepts no liability for any loss occasioned to any person acting or refraining from action as a result of any material in this publication.

Deloitte LLP is a limited liability partnership registered in England and Wales with registered number OC303675 and its registered office at 1 New Street Square, London EC4A 3HQ, United Kingdom.

Deloitte LLP is the United Kingdom affiliate of Deloitte NSE LLP, a member firm of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"). DTTL and each of its member firms are legally separate and independent entities. DTTL and Deloitte NSE LLP do not provide services to clients. [Please click here to learn more about our global network of member firms.](#)

© 2021 Deloitte LLP. All rights reserved.