INDUSTRY REPORT

OpSec Barometer: Navigating the New Normal Online

Abstract

88% of consumers normally do at least 10% of their shopping online, with 37% of consumers now saying the frequency of their online grocery shopping increased during the peak of the coronavirus.

Over the last year, the use of online services for everything from shopping and banking, to educations and entertainment has increased. Already on an upwards trajectory, this trend has been accelerated by the COVID-19 pandemic. In its recent Consumer Barometer Report, OpSec Security surveyed 2,600 online consumers globally to understand how they are currently navigating the online landscape, the impact of cybercriminals, and how consumer behavior is being shaped by world events and previous online shopping experiences.

Respondents were asked questions regarding their habitual use of online services, such as the regularity of their online shopping, the threats they have come into contact with online, and how protected they feel by brands, as well as how their habits have had to change as a result of the pandemic. For example, 88% of consumers normally do at least 10% of their shopping online, with 37% of consumers now saying the frequency of their online grocery shopping increased during the peak of the coronavirus.

The results indicate that consumers feel brands are currently not doing enough to protect them online, with a growing number of people having fallen victim to credit card fraud and an increase in data breaches. The findings also highlighted the impact negative online experiences can have on brand perception. On this basis, and if they aren't already doing so, brands need to put the strategies and tools in place to safeguard consumers from online bad actors, protecting them from the myriad of threats, including phishing scams and the sale of counterfeit goods, and at the same time protect their brand reputation.

As the increased use of online services is likely to drive long-term changes in consumerism, being proactive and taking steps to mitigate the risks posed by cybercriminals will be fundamental in brands and businesses retaining consumer trust.

Introduction

2020 has been a year of unparalleled change and upheaval - for consumers and businesses alike. The impact of this global health crisis is far-reaching and as the world adapts to new ways of living, interacting, working, and shopping, brands are working harder than ever to maintain trust and loyalty.

This is especially true in e-commerce where, understandably, there has been a massive increase in the use of online shopping. Not only has consumer behavior changed, but the sharp rise in online activity has led to questions around security, piracy, and the ways in which brands are now perceived.

With this in mind, OpSec wanted to understand just how consumer behavior has changed in terms of shopping, consumption of pirated content, and purchase of counterfeit goods. The report also explores whether consumers have been affected by cybercrime, their perceptions of brands, and whether they believe the role of brands in keeping consumers safe has changed.

To gain this insight, OpSec's latest research focused on the experiences and perceptions of 2,600 online consumers globally, looking at their safety online, purchase of imitations, and attitudes towards authentication during the shopping process, as well as how consumer behavior has been impacted by the COVID-19 pandemic.

OpSec wanted to understand just how consumer behavior has changed in terms of shopping, consumption of pirated content, and purchase of counterfeit goods.

Independent research carried out by Vitreous World, commissioned by OpSec, surveyed consumers from the U.K., U.S., France, Germany, and Italy in July 2020.

Research Findings Overview

Pervasiveness of cyber attacks

- 40% have been the victim of an email scam or phishing
- 35% have experienced credit/debit card fraud
- 21% have been the victim of identity theft
- 30% have been impacted by data breaches

The research highlighted the pervasiveness of cyber attacks, with 40% of respondents having been the victim of an email scam or phishing, more than a third (35%) have experienced credit/debit card fraud and 21% have been the victim of identity theft. Meanwhile, data breaches have impacted 30% of respondents.

The report indicates growing desensitization among consumers when it comes to cyberattacks as 30% of data breach victims were unsurprised when it happened to them while half (48%) of those who haven't been the victim of a data breach believe they will be at some point in the future. Consumers are also being fooled by online counterfeiters, as indicated by more than a quarter (28%) of consumers having unintentionally bought a fake product. These trends beg the question 'are brands doing enough to protect consumers?', while also raising concerns around how much consumers are doing to protect themselves.

Among this year's key findings is the profound effect COVID-19 has had on consumer behavior. As expected, it has resulted in an increase in the frequency with which people have shopped online, as demonstrated by 37% of consumers, but what may not have been considered until now is how this might impact shopping long-term. Moving forward, 32% of consumers believe that they will somewhat increase the amount of online shopping they do as a result of the pandemic.

However, as consumers continue to look for ways to keep themselves entertained, piracy is on the rise, which a noticeably increased during lockdown. In fact, of those people that consume pirated content, such as movies, video games, and music, 29% said they did so more frequently during their country's "lockdown". If sustained over a longer period, this could have a significant impact on brands, cinema, and artists, among others.

As COVID-19 restrictions are likely to remain in place to some extent for the rest of the year, resulting in consumers continuing to conduct large parts of their lives online, they may be more susceptible to threats posed by online bad actors. The very fact that over half (51%) of consumers have noticed an increase in phishing activity during the pandemic is testament to that.

Consequently, brands and individuals must begin to work together to fight back against cybercriminals. Critical to this will be working with organizations such as OpSec to put the safeguards and solutions in place to protect their websites, data, and business, while also helping to spread awareness of online security among consumers.

The Threats Facing Consumers and What's Being Done to Tackle Them

1. Are brands doing enough to protect consumers online?

According to Statista, there are currently 4.5 billion active internet users worldwide[1], of this number external sources expect 2.05 billion to make an online purchase this year[2]. Unfortunately, cybercriminals are using the internet for more nefarious activities including committing online fraud, operating email phishing scams and stealing personal data. It is predicted by Cybersecurity Ventures that by 2021, cybercrime will cost the world $6 trillion annually[3]. It's this prevalence of cybercrime that presents a continuous risk for online consumers, many of which expect the organizations with whom they share their personal data or make purchases online with to safeguard that information. However, it is apparent that consumers are being let down in this regard and businesses must begin to turn the tide by implementing the strategies and tools needed to keep consumer data safe.

The threat of cyberattacks

According to OpSec's research, currently 88% of consumers normally do at least 10% of their shopping online. However, almost half (47%) of consumers have had concerns over using their credit card to make a purchase online, of which these concerns include hackers stealing their personal details (62%), scammers stealing their money (58%), and identity theft (57%).

For some, these worries stem from past experiences as 40% of respondents revealed they have been the victim of an email scam or phishing. Of this figure, more than one third (38%) of individuals had money stolen, but it was only returned in 58% of cases. The high number of those surveyed tallies with the fact that phishing attacks account for more than 80% of reported security incidents, as reported by CSO Online[4].

Worryingly, over half (51%) of consumers have also noticed an increase in phishing activity during the pandemic.

Overall, it seems that cybercrime could be on the rise across the board as more than one in five (21%) consumers have been the victim of identity theft, compared to 19% in 2019. Similarly, 35% of consumers have been the victim of credit/debit card fraud so far in 2020, rising from a third (33%) in 2019. Proactive monitoring of where their brand's vulnerabilities lie and using this information to educate employees and put protocols in place is just one of the approaches businesses can take to stop this figure from rising.

Worryingly, over half (51%) of consumers have also noticed an increase in phishing activity during the pandemic.

55% of consumers believe companies aren't doing enough to protect their data.

Consumers are becoming desensitized

As consumers interact with a growing number of websites and services online, 30% have experienced a data breach – an increase on 2019 when 28% of consumers experienced this type of attack. Of those who have had their data compromised, 46% have been contacted by brands about their data being breached two to five times, while 9% have been contacted more than five times. Meanwhile, almost half (48%) of those who haven't been the victim of a data breach worryingly believe they will be at some point in the future.

The frequency with which data breaches appear to be occurring is resulting in a degree of desensitization among consumers, as 30% of data breach victims were unsurprised when it happened to them. Although, that's not to say they aren't having a damaging impact on the businesses involved. 64% of victims lost trust in the company or brand that lost their data, with 28% of these consumers saying that this loss of trust means they won't shop with the business again. According to IBM, a data breach can cost an organization up to $3.92 million in terms of investigation expenses, damage control, repairs, lawsuits, and fines[5].

This sentiment is echoed by 55% of consumers who believe companies aren't doing enough to protect their data. Despite being the attitude of more than half of those surveyed, it is a marked reduction from 63% of consumers last year, suggesting some consumers may feel that some brands have begun to tackle this issue in the in the past 12 months. Working with brand protection partners and adopting the right strategies and tools is essential for this number to continue to reduce every year.

Sale of counterfeit goods

As well as the myriad of concerns relating to their personal data and the safety of making online purchases, consumers are also being caught out by counterfeit goods. In fact, OpSec discovered that 28% of consumers have unintentionally bought a product online that turned out to be fake - only a slight improvement on last year when 31% of consumers encountered this problem – but this could also reflect a change in purchasing habits due to COVID-19.

Looking at where these items are being purchased, 20% have unintentionally bought a fake product from a marketplace or online auction site. This coincides with a slight drop in people's confidence in using online marketplaces, with 55% of consumers saying they are confident using these platforms compared with 58% in 2019. Perhaps slightly more worryingly, 18% of consumers have unintentionally bought a fake product from a site that they believed was the brand's genuine page. This signals that some companies could still be doing more to ensure their brand is not being misused and their customers are being protected. Online monitoring services can ensure brand infringements are quickly identified to remove unauthorized use of the company's name and products associated to it.

As well as being detrimental to those brands affected, counterfeiting can have significant economic repercussions with a 2020 Federal Research Division report finding that counterfeiting and piracy costs U.S. businesses more than $200 billion a year and leads to the loss of more than 750,000 jobs.

Meanwhile, globally counterfeit goods are a $460 billion industry[7]. This indicates the vastness of the problem and why it should be a key consideration for brands operating both in the online sphere and offline.

Making purchases via social media

Over recent years, the way in which consumers interact with social media platforms has evolved, however, concerns remain regarding its use for e-commerce. More than half (56%) of consumers surveyed by OpSec are concerned about the quality of goods for sale on social media, while 55% have payment security concerns about buying goods via these channels.

Other worries about buying items from social media platforms include buying a fake (49%) and the safety of their personal details (48%). This suggests that consumers are wary of the legitimacy of items being sold via social media and don't feel fully protected by those sites.

Some of this distrust in social media may also come down to the other ways in which these platforms are being misused and exploited by online bad actors. Social media sites are now regularly used to share pirated content, with external sources finding that 2,637 pirate streams of the 2018 World Cup semi-finals were shared on social media sites, Facebook, YouTube, and Periscope[8]. This totaled almost 30 million views, while the final between France and Croatia received a staggering 60 million views via these illegal streams.

While pirating of live sports streams in these instances has a negative impact on broadcasters as they miss out on vital viewers and their subscription fees, there is also a wider impact on sports themselves. According to a third-party study, worldwide illegal streaming of the English Premier League delivers £1 million in uncaptured sponsorship media value per match[9]. With a total of 380 matches played each season, this is a staggering amount of money for these clubs to lose out on.

For consumers, accessing pirated content via streams advertised on social media isn't without its dangers as it is reported that internet users who visit content theft sites are 28 times more likely to get malware from those sites than from legitimate websites or content providers[10]. This demonstrates that even if users knowingly consume pirated media online, there are hidden risks that will leave them vulnerable.

Undoubtedly, social media can be a great tool for brands and broadcasters, allowing them to engage with influencers and consumers directly, while also doubling as an instant marketing platform. However, it is clear that these channels can also pose a significant threat. As a result, brands must continue to monitor social media sites for threats to find those who are sharing their content illegally or counterfeit versions of their products, for example. Understanding where these threats lie will help them shut them down quicker and mitigate the risk to their brand and customers.

2. Who's responsible for keeping consumers safe online?

Fighting the threat posed by cybercriminals is in the best interest of both consumers and brands. Yet, there isn't currently a consensus on who should be responsible for this. Staying safe online requires active participation from both parties, including vigilance from consumers. For online retailers and companies, the responsibility doesn't stop at taking measures to protect their brand and consumer data, there should also be an onus to educate customers about online security. The current state of play suggests that neither consumers nor businesses are taking the right level of precautions.

Shopping safely online

With so many threats facing consumers online, it brings up questions about who is ultimately responsible for protecting them and whether they are doing enough. Over half (51%) of consumers think brand owners should be responsible for keeping consumers safe from unintentionally buying fake products online. 47% of consumers think this responsibility should fall to watchdog organizations, followed by the government (40%) and social media platform owners (40%).

Just over a third (36%) of consumers think they should be responsible for keeping themselves safe. However, this requires some knowledge of how to determine what is and isn't safe or legitimate online, which brands and online protection organizations have a part to play in achieving.

Are consumers doing their due diligence?

When evaluating the safety of e-commerce sites, OpSec found that 54% of consumers make sure the site is a reputable brand name, while 46% check for the SSL certificate which presents as a green padlock in the URL bar. While it's positive that consumers are taking steps to keep themselves safe, the SSL certificate isn't always a good indication of the site's reputation. Despite this giving a website legitimacy in most cases, it's also possible for cybercriminals to sign up for a free 90-day SSL certificate for their websites, which they can then simply renew every 90 days. This is demonstrated by the fact that over half of the phishing sites OpSec has detected year-to-date have used an SSL certificate to "fake" legitimacy.

Other evaluation measures consumers take include reading customer reviews (46%), investigating the brand on social media (23%) and looking at Companies House (15%). Concerningly, 10% don't do any form of evaluation into websites they might make a purchase from.

Consumers also don't appear to be doing enough to report those selling counterfeit products with only 29% of consumers saying they contacted the seller after receiving a fake product. Just 7% of consumers contacted the police whereas 11% did nothing.

Ultimately, keeping safe online is a team effort with vigilance needed from consumers, while brands need to do their bit to protect customers, which extends to educating them about online safety.

When evaluating the safety of e-commerce sites, 54% of consumers make sure the site is a reputable brand name while 46% check for the SSL certificate.
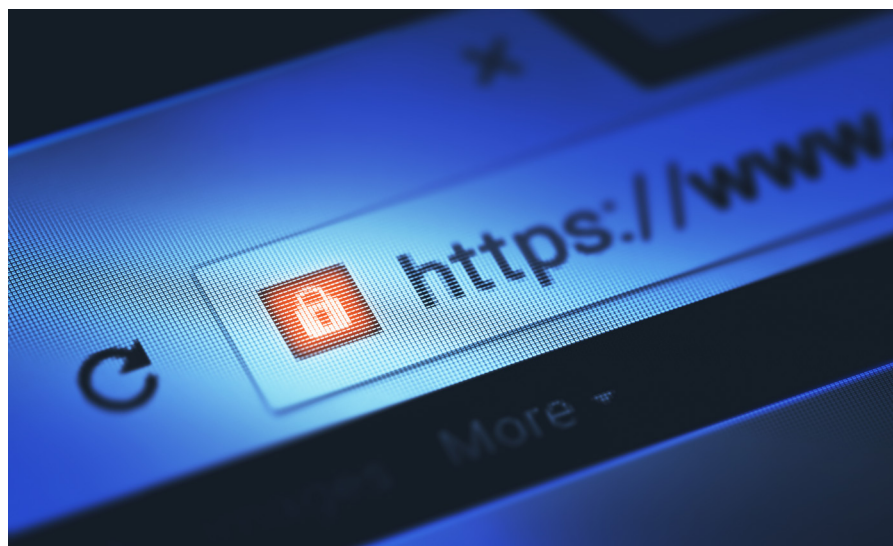
24% of consumers are knowingly accessing pirated content – with 25% watching or consuming this on a daily basis.

By increasing awareness of how to shop safely online and use online services, brands can help to limit the number of people duped by fake products or caught out by phishing scams, for example. This is key to helping everyone enjoy the multitude of benefits that the online world can bring.

Active participation in online misuse

While there is a high proportion of fake goods being purchased unintentionally, there are still some consumers actively seeking out counterfeit goods with 16% of consumers having intentionally bought a fake product online this year, which is an increase from 12% last year. For 44% of respondents, the main reason for buying a fake was the price, with 18% saying they could never afford the real thing. Almost a quarter (24%) of individuals were influenced by the fact the fake looked like the real thing. This highlights the importance of brands gaining an awareness and understanding of how their brand is being misused online to shut down instances of it being used by counterfeiters.

As well as buying counterfeit goods, a growing number of people are also knowingly accessing pirated content with almost a quarter (24%) of consumers confessing to doing so. When asked about how often they watch or consume pirated media, a quarter (25%) said daily, followed by 22% who do so several times a week, and 19% who engage with pirate content on a weekly basis. Currently, 80% of piracy is attributable to streaming compared with just a few years ago, when BitTorrent downloads on their own accounted for nearly 40%, as stated in a report from The GIPC[11].

The damaging effect of piracy has been evident over the last decade as the number of cinema trips have dwindled and record sales lower than ever. In fact, the RIAA stated that the US music industry alone saw revenue drop from $14.6 billion in 1999 to $9.8 billion in 2018[12], perhaps unsurprising given that 45% of those who consume pirate content illegally access music. As well as promoting content, those in the creative industries, whether they are brands or industry bodies, need to also educate audiences on the repercussions that piracy can have.

Consumer trust

Due diligence when purchasing items or sharing data is extremely important, particularly as many consumers don't trust brands and websites to do it for them. This can be seen in consumer attitudes towards social media sites with 38% of consumers saying they don't trust them to keep their data safe, while 32% don't trust using the platforms for shopping. Twenty-seven per cent of consumers are more likely to trust a product promoted by social media influencers.

While there is some mistrust in social media sites, a quarter (25%) of consumers think that links to products that are advertised in posts on social platforms mean that the content is legitimate. This suggests that more needs to be done to educate consumers about how to determine whether content shared on social media is trustworthy or if bad actors are using these sites to disseminate illegal content.

Confidence in shopping via different online methods has begun to wane with 53% of consumers saying they are confident making purchases via smartphone apps, down from 60% in 2019. Similarly, fewer consumers are confident making purchases via links in social media posts - changing from 29% in 2019 to 26% in 2020. This could indicate a growing awareness among consumers about the potential dangers of online shopping if they don't remain vigilant.

How COVID-19 has impacted the online landscape

The majority of brands seemed to maintain high levels of customer service during the pandemic with 61% of consumers stating that they had positive online experiences.

The COVID-19 pandemic has profoundly affected society's use of the internet and online services. With bricks-and-mortar stores, banks and entertainment complexes closed for extended periods around the globe as countries entered a state of lockdown, the online world played a more crucial role than ever before. While an external report found that online travel agencies saw bookings plummet by 90% in April , online grocery shops struggled to cope with increased demand - with a year-over-year growth of 103% in online grocery shopping in May in the UK alone, as reported by Reuters[14].

3. The consumer experience during COVID-19

Shoppers move online

Undoubtedly, the COVID-19 pandemic has had a profound impact on all aspects of society and has forced a shift to the online world for everything from shopping and banking, to schooling and working. During this period, and discovered through OpSec's findings, 37% of consumers said that the frequency of their online grocery shopping increased, of which 14% said it increased significantly.

Moving forward, the ongoing pandemic is likely to have a lasting impact on shopping habits, with 32% of consumers believing that they will somewhat increase the amount of online shopping they do as a result. However, while the COVID-19 virus remains a threat and affects the usual operations of bricks-and-mortar stores, this increased use of online shopping could potentially make consumers more susceptible to online threats.

Online customer service

The majority of brands seem to have maintained high levels of customer service during the pandemic with 61% of consumers sharing that they had a positive online shopping experience. For a quarter (25%) of consumers trust in online shopping increased during the pandemic. Just 11% of people had a disappointing online shopping experience during the pandemic, which was mainly down to items being out of stock (42%). This was a common occurrence particularly at the beginning of the pandemic when third-parties revealed that demand for toilet roll spiked by 845%[15].

## 4. Staying entertained online

Piracy in the pandemic

Piracy is a huge problem that continues to grow. According to the US Chamber of Commerce, it costs the US economy $30 billion a year and results in up to 560,000 job losses[16]. As COVID-19 required a significant amount of the world's population to stay at home, many turned to pirated content to keep them entertained. OpSec's survey revealed that almost a quarter (24%) of people consume pirated content with 29% of these individuals increasing the frequency with which they pirated during their country's lockdown.

Exploring the types of content pirated, movies (49%) were revealed to be the most popular, followed by music (45%), TV shows (36%) and video games (34%). Over a quarter (26%) of consumers pirate live sports, however, with the results of COVID-19 cancelling the vast majority of live sporting events for several months, the return of this content could result in increased piracy.

> With research from The GIPC finding that pirated TV shows receive 230 billion views every year worldwide and with the vast majority coming from outside the US but 126 billion of these views were of content produced in the US, it seems that the regional release of content is a key driver of piracy[17].

Yet, according to the research with 25% of consumers believing that links to content that are advertised in posts on social media platforms mean that the content is legitimate, it could be that some consumers are unaware they are accessing pirated content. By doing more to educate consumers on issues such as piracy, they can be more alert to pirated content and determine themselves if content is legitimate, whether that's by simply checking an official brand page for content as opposed to links found in a search engine or on social media. For broadcasters and streaming providers, this also means working with third-parties to shut down pirates as quickly as possible and to direct viewers to legitimate sources of their content.
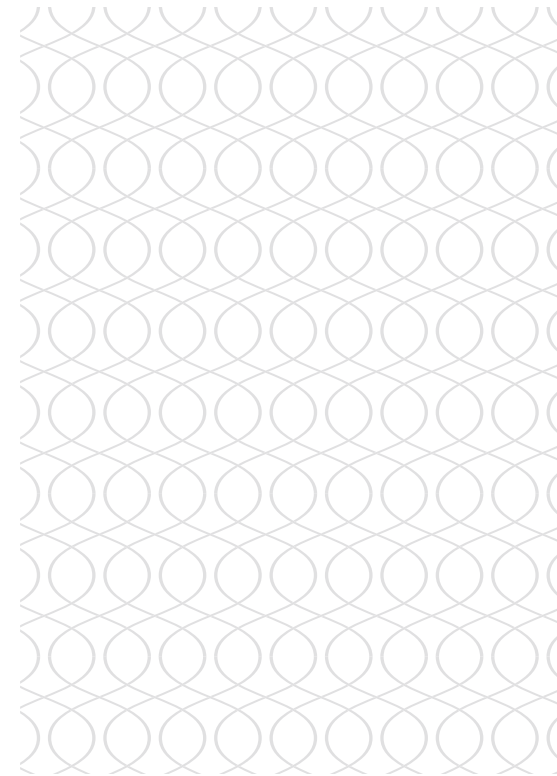
Conclusion

Where does this leave consumers?

COVID-19 has had a major impact on consumers' use of online services, and this has coincided with higher levels of online fraud. The pandemic could have a lasting effect on consumer behavior with 32% of consumers believing that they will somewhat increase their online shopping as a result, but with this, there is the potential that they will also be more susceptible to cybercriminals.

Despite best efforts, the research has demonstrated that consumers are still falling foul of online bad actors, whether in terms of having their identity or data stolen to being sold counterfeit items. While it's clear that some consumers could do more to check the legitimacy of the websites they are using to make purchases, much of the responsibility for keeping consumers safe online falls to the brands themselves.

Brands need to be front and center when it comes to protecting consumers from fraud and data breaches, particularly as 55% of consumers currently don't believe companies are doing enough to protect their data. The impact of failing to protect consumers can be extremely damaging for a brand, not only impacting their reputation but also consumer trust and their willingness to make future purchases.

As the fight against cybercriminals intensifies in a post-COVID-19 landscape, brands must implement the right strategies and develop relationships with law enforcement agencies and brand protection experts to proactively tackle the threats they are facing and safeguard consumers.

OpSec Security's Top Tips for Brand Owners

This report highlights the impact of cybercrime, counterfeiting and brand abuse in today's online landscape and how this has been impacted by the COVID-19 pandemic.

With consumers and organizations significantly affected, brand protection has never been more important. What should brand owners consider?

- Take a consumer-centric approach to brand protection by adopting comprehensive, cross-channel solutions to proactively monitor for threats in order to stop them in their tracks and limit damage to your customers and your brand. After all, prevention is better than a cure.

- Use smart technology to strengthen your online defense strategy with innovative search capabilities and proprietary techniques to mimic what consumers would find online when searching for your brand to identify and shut down illegitimate operations. Brand reputation has a significant impact on whether a consumer makes a purchase, so safeguarding that reputation in this way is vital.

- Preserve brand equity and customer trust by implementing powerful phishing prevention tools, detection technology, and comprehensive mitigation strategies, to protect you and your valued customers from phishing attacks.

1. www.statista.com/statistics/617136/digital-population-worldwide

2. www.oberlo.com/statistics/how-many-people-shop-online

3. https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016

4. www.csoonline.com/article/3153707/top-cybersecurity-facts-figures-and-statistics.html

5. https://newsroom.ibm.com/2019-07-23-IBM-Study-Shows-Data-Breach-Costs-on-the-Rise-Financial-Impact-Felt-for-Years

6. www.uspto.gov/sites/default/files/documents/USPTO-Counterfeit.pdf

7. www.adweek.com/brand-marketing/counterfeit-goods-are-a-460-billion-industry-and-most-are-bought-and-sold-online/#:~:text=Consumers%20spend%20%24460%20billion%20on%20counterfeit%20goods%20every%20year

8. www.forbes.com/sites/nelsongranados/2018/07/18/world-cup-live-streaming-piracy-thrived-on-social-media-platforms/#6d9b8cad259a

9. https://gumgum.com/newsroom/press-releases/study-shows-illegal-streaming-of-english-premier-league-worth-1m-in-uncaptured-sponsorship-media-value-per-match

10. www.fact-uk.org.uk/files/2017/09/Cracking-Down-on-Digital-Piracy-Report-Sept-2017.pdf

11. www.ibc.org/trends/digital-piracy-costs-us-economy-30bn-annually/4037.article#:~:text=Piracy%20results%20in%20up%20to%20560%2C000%20industry%20job%20losses&text=Online%20piracy%20costs%20the%20US,the%20US%20Chamber%20of%20Commerce

12. https://www.riaa.com/u-s-sales-database

13. https://www.globenewswire.com/news-release/2020/05/29/2040716/0/en/COVID-19-Impact-on-e-Commerce-Online-Payments-Worldwide-2020-Online-Shopper-Penetration-Increases-During-the-Pandemic.html

14. https://www.reuters.com/article/us-health-coronavirus-britain-supermarke/online-uk-grocery-spending-hits-record-in-lockdown-shopping-spree-idUSKBN2330RP

15. https://www.businessinsider.com/why-toilet-paper-demand-spiked-845-how-companies-kept-up-2020-5?r=US&IR=T

16. https://www.ibc.org/trends/digital-piracy-costs-us-economy-30bn-annually/4037.article#:~:text=Piracy%20results%20in%20up%20to%20560%2C000%20industry%20job%20losses&text=Online%20piracy%20costs%20the%20US,the%20US%20Chamber%20of%20Commerce

17. https://www.ibc.org/trends/digital-piracy-costs-us-economy-30bn-annually/4037.article#:~:text=Piracy%20results%20in%20up%20to%20560%2C000%20industry%20job%20losses&text=Online%20piracy%20costs%20the%20US,the%20US%20Chamber%20of%20Commerce

About OpSec

OpSec is a market leader in brand, transaction cards, and government protection and provides a comprehensive suite of end-to-end solutions, including advanced physical security technologies, supply chain track and trace services, and online and e-commerce monitoring and analysis. We can help you find the right solution for your brand or agency, your budget and your protection goals.

OPSEC WORLDWIDE OFFICES

The Americas	Europe	Asia
Boston, MA, USA	London, GBR	Kowloon, HKG
Lancaster, PA, USA	Leicester, GBR	Shanghai, CHN
San Francisco, CA, USA	Washington, GBR	Beijing, CHN
Meridian, ID, UDA	Munich, DEU	Tokyo, JPN
Santo Domingo, DOM	Santa Venera, MLT	
	Vilnius, LTU	