OPINION

‘Retailers that failed to invest in digital were suffering and the last few months has only speeded this up; many will fail to survive’

There has been phenomenal growth in ecommerce sales since lockdown started in the UK. Purchases have been forced online as a result of the lockdown measures and lifestyles of the past three months.

According to the *IMRG Capgemini Sales Index*, there was a 32 per cent year-on-year increase in May. There has been a huge rise in sales in the home and garden sector, up by 163 per cent year on year. Electricals, beer, wine and spirits, and beauty products too have all seen huge growth.

While many ecommerce categories have seen high spikes, this growth has not been realised across all sectors. Clothing sales have struggled. There is no point in buying a new outfit to sit at home.

Yet even in the apparel sector, there is some light at the end of the tunnel, with an uplift in sales from April to May. This has been largely in the health and fitness area, likely due to a relaxation of the lockdown rules.

The question I have is will ecommerce continue to maintain its share of the retail pie? There are two main changes that have taken place during lockdown which we need to take into consideration.

Firstly, consumers have been forced to purchase online; many shoppers that had never bought online before have had to make that leap. This has certainly been evident in the grocery sector. Many other sectors have also benefited from the forced change during the coronavirus crisis, electricals and home office equipment an obvious area.

Secondly, we have seen a fundamental shift in that many retailers and businesses have had to pivot their sales strategy. Ecommerce is the only sales channel they have had available, so those that have traditionally sold offline have had to change tack. The direct-to-consumer model has been implemented by large fast-moving consumer goods brands such as Heinz, with their first-ever UK online shop Heinz To Home; adidas too has been a high-profile example.

So, what next? The high street is again largely open for business, albeit under strict social-distancing rules.

For now, there is still a health risk and many people will continue to avoid the high street, purchasing online for some time. This will be especially true with commodity-type purchases, so ecommerce will continue to benefit. And consumer groups, such as the older generations, have had to familiarise themselves with buying online, so many will not revert to the weekly trip to the supermarket, assuming they can get a delivery slot.

Yet more than anything, COVID-19 has been a major accelerator of changes that were already happening. The high street has been under pressure for a number of years and the current situation has brought this into focus. Retailers that failed to invest in digital were suffering and the last few months has only speeded this up; many will fail to survive.

The importance of inventory, supply chain, delivery, a strong ecommerce website and the ability to be agile have all come into play. Businesses that are strong in these areas will thrive, whether pureplay or omnichannel. A strong product and ultimately a strong customer knowledge are fundamental. Today and for the future, owning the customer relationship is key and digital facilitates this.

Ecommerce will continue to increase its portion of the retail pie. It has been happening for years. The high street will evolve and new business models will be developed. Businesses that realise this will survive in the short term and thrive in the future. ●

Graeme Howe
Managing director
Ecommerce Expo
Director at IMRG

FRAUD

Lessons to learn from ecommerce fraud

As ecommerce continues to expand, with record growth figures already posted for 2020, so does the risk of fraud. Here are five lessons businesses can learn from recent cases of ecommerce fraud to keep themselves and their customers protected

Alex Wright

rzoze19/Shutterstock

1

Be open if you suffer a data breach

easyJet was targeted by hackers in one of the biggest ecommerce frauds committed on a British company. Records belonging to nine million of the budget airline’s customers were accessed in this highly sophisticated attack believed to have been perpetrated by Chinese hackers, which resulted in the credit and debit card details, including security codes, of 2,208 individuals being compromised.

The company, which has so far been tight lipped about exactly how the breach happened, has come under fire for being slow to respond. After becoming aware of the incident in January, the airline notified the Information Commissioner’s Office (ICO) and the National Cyber Security Centre, but didn’t start informing its customers until April, because it said it first had to establish the extent of the problem.

easyJet is the latest in a line of airlines to be targeted after British Airways and Air Canada were hacked in 2018. Customers have already reported cases of phishing and attempted social engineering stemming from the breach, while easyJet is also facing an £18-billion class action lawsuit brought by affected parties.

“The key message here is that once a data breach has occurred, you need to be as up-front as possible about the extent of what has happened,” says Jonathan Knudsen, senior security strategist at Synopsys.

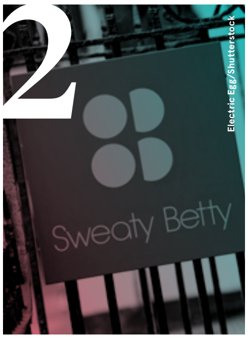
Monitor regularly for suspicious activity

Fashion retailer Sweaty Betty became the latest high-profile victim of the fastest growing ecommerce fraud: form-jacking. So-called Magecart hackers gained access to and injected malicious JavaScript programming code in the company’s website before exfiltrating customer details from the checkout page, using sophisticated web-based card skimmers to steal payment card information.

Names, billing, delivery and email addresses, telephone numbers and passwords were all taken from customers who entered their payment card details between November 19 and 27, 2019. After being captured by the skimmer, the information was sent to a remote server operated by the criminals to be sold on the dark web.

To Sweaty Betty’s credit, after being discovered, it quickly reported the incident to the ICO and disclosed the breach in an email to customers affected. It also enlisted specialist security consultants to help with the investigation into what went wrong.

Mimecast’s head of ecrime Carl Wearn says the lesson other companies should take from this is to regularly monitor webpages and the integrity of files in an effort to detect malicious code. “Without this constant monitoring, this form of attack can go undetected for long periods and can lead to the real-time theft of payment details, which can then be used online for fraudulent transactions,” he says.



2

Electric Egg/Shutterstock

Neil Setchfield/Alamy Stock Photo

Stay one step ahead of the hackers

As if being breached once wasn't bad enough, blender manufacturer NutriBullet was hacked three times in less than a month. In this elaborate ecommerce fraud, Magecart hackers first installed malware to steal credit card details on the company's website on February 20.

The skimmer was removed on March 1, after security experts identified the threat and took down the hackers' exfiltration domain, only for a second one to be inserted on a different part of the site on March 5. That too was soon detected and the new domain was removed. However, in a matter of days a third skimmer was implanted on March 10, again on another section of the site, and it too was discovered and taken down a week later.

NutriBullet carried out an investigation to determine how its JavaScript code was compromised and updated its security policies and credentials accordingly, adding multi-factor authentication as an extra layer of protection. But serious questions have to be raised about how the hackers were able to infiltrate the site again so easily after the initial attack.

"The message is clear: hackers are learning from past attacks to stay one step ahead, so it's up to the security community to do the same," says RiskIQ's head of threat research Yonathan Klijnsma.

IanC66/Shutterstock

You're never too big to get hacked

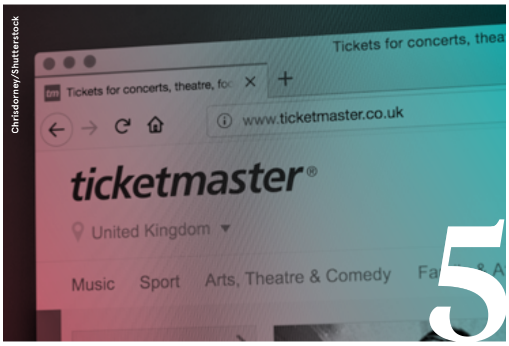
British Airways was hit with a record £183-million fine from the ICO after around 500,000 of its customers had their data harvested by hackers who breached its security systems. Users who booked flights through the airline's website and app were diverted to a fraudulent site where their personal details were siphoned off.

Around 380,000 transactions, including names, addresses, logins and payment card details, were accessed in this large-scale ecommerce fraud, which happened between August 21 and September 5, 2018. The problem was down to a vulnerability in the third-party Modernizr JavaScript installed on the website, which hadn't been updated since 2012.

BA notified all customers affected immediately and has agreed to compensate them for any losses. It has also fully co-operated with the ICO investigation and made improvements to its security. The airline announced its intention to appeal the penalty, which was the first to be made public under the General Data Protection Regulation.

"The lesson here is that if a big company like this can get hacked then anybody can get hacked," says Max Heinemeyer, director of threat hunting at Darktrace. "Now it's a matter of when, not if, you are going to be breached."

Make sure your third-party vendors are secure



Chrisdorney/Shutterstock

Up to 40,000 Ticketmaster customers had their personal information stolen after hackers gained access to it through malicious software inserted in a customer support product hosted by third-party provider Inbenta Technologies. The breach compromised data belonging to those who tried to buy tickets on its website between February and June 23, 2018 and may have included names, addresses, telephone numbers, email addresses, payment and login details.

Digital bank Monzo claimed to have spotted the signs of a breach on April 6 after around 50 of its customers reported fraudulent activity on their accounts and after investigating found many of those affected had used their cards on Ticketmaster's website. Monzo presented its findings from this sophisticated ecommerce fraud to Ticketmaster, but after looking into it, the event ticketing firm said it could find no evidence of a breach.

Ticketmaster informed the ICO and notified all customers affected, advising them to reset their passwords. However, a group of 650 people are suing the company for £5 million, claiming they have suffered "multiple fraudulent transactions" and "significant stress".

"One essential lesson organisations should take from such recent incidents is that our cybersecurity is only as good as our third-party vendors' security and compliance," says CyNation's chief technology officer and chief security officer Shadi Razak. ●