MarkMonitor
Protecting brands in the digital world

Clarivate Analytics

REPORT

MarkMonitor® Online Barometer

Fraud and Cybercrime Survey 2016

Overview

The MarkMonitor Online Fraud Barometer reports findings from a global consumer survey that analyses the prevalence of cybercrime across various online channels and how consumers respond to it. It also provides insightful information about the impact of fraud and cybercrime on brands in both financial terms and brand reputation.

Table of Contents

Executive Summary

Cybercrime, cyberattacks and online fraud are growing in scale, sophistication and frequency, affecting not just businesses, but also consumers. The types of organisations and industries targeted have changed — while historically it was financial and banking institutions that were most often attacked, or multi-national companies, no market or size of company is now immune. According to recent IBM research[1], the healthcare industry is most at risk from cyber attackers, followed by manufacturing, financial services, government and transportation.

The motives for these attacks vary — from stealing intellectual property and customer data to siphoning off funds, or disrupting systems, websites and operations in order to make a ransom demand. What doesn't change is the fact that these attacks have major impact on both brands and customers. From an organisational point of view, cyberattacks, regardless of what they are — distributed denial of service (DDoS), data breach or malware events — can lead to lost revenue, missed business opportunities, breakdown of customer trust and damage to reputation. For the customer, personal details and data could be stolen, they could lose money as a result, become victims of identity theft, and ultimately lose trust in that company.

Cyber fraud is often the purpose and result of an online attack against a company but can also be perpetrated against consumers directly. Globally, cybercrime is forecast to increase to $2 trillion by 2019[2]. As a result, online security is a growth industry with research suggesting it will grow at a rate of 8.3 percent until 2021[3]. But this increase in spending is not necessarily protecting customers as online attackers are still able to compromise brands and defraud consumers by stealing their credentials. In many cases breaches are taking place outside of the firewall of an organisation, away from their online security measures.

As a result, the problem remains pervasive and there is a definite need for organisations to invest in both online security measures, as well as a wider-reaching online brand protection strategy that incorporates fraud protection and customer education.

Mitigating these risks and protecting customers is made even more difficult as cybercriminals make more use of the Deep Web — the vast majority (around 96 percent) of the Internet

comprising unindexed content, such as webmail pages, company intranets and pages behind paywalls[4]. The Deep Web includes the Dark Web — websites with hidden IP addresses that allow criminals to act anonymously. More than that, the Dark Web provides a marketplace where criminals can sell stolen company and personal data and even co-ordinate attacks.

In order to better understand the perception, attitudes and experiences of consumers regarding online fraud and security, MarkMonitor® commissioned Opinium, a leading market research agency, to conduct a global survey. This report details the findings of the research. With a sample size of 3,457 adults 18 years and older, the online research was carried out in the UK, USA, Denmark, France, Germany, Italy, The Netherlands, Spain and Sweden between 26 August and 05 September 2016.

[1] Morgan, Steve. "Top 5 Industries At Risk Of Cyber-Attacks," Forbes, May 2016. http://www.forbes.com/sites/stevemorgan/2016/05/13/list-of-the-5-most-cyber-attacked-industries/
[2] Morgan, Steve. "Cyber Crime Costs Projected To Reach $2 Trillion by 2019," Forbes, January 2016. http://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/
[3] "Cyber Security Market to Grow at CAGR 8.3 percent Till 2021 Says TechSci Research Report," PR News Wire, August 2016. http://www.prnewswire.com/news-releases/cyber-security-market-to-grow-at-cagr-83-till-2021-says-techsci-research-report-590704471.html
[4] Egan, Matt. "What is the Dark Web? How to access the Dark Web. What's the difference between the Dark Web and the Deep Web?," PC Advisor, April 2016. http://www.pcadvisor.co.uk/how-to/internet/what-is-dark-web-how-access-dark-web-deep-joc-beautfiulpeople-3593569/

20%

Of the sample that fell victim to cybercrime, 20 percent lost more than £1,000.

Key Findings

1. Cybercrime is prevalent across today's online environment

> 45 percent of those surveyed said they had been a victim of cybercrime, with one in six losing money. Globally, 20 percent of victims lost more than $1,298

Out of the sample of 3,457 respondents, 45 percent said they had been a victim of a cybercrime. The most cited example of fraud was receiving false requests to reset a password for social media logins. This was experienced by 20 percent of the subsample.

Of the sample that fell victim to cybercrime, 20 percent lost more than £1,000. Looking specifically at the UK and USA, the overall average of money lost totalled £1,627 and $1,840, respectively.

In terms of industries in which the crimes occurred, 30 percent of incidents originated in the banking and finance sectors — historically the source of the majority of attacks — followed by online services, including paying household bills, social media, and consumer goods.

The result of experiencing this fraud included fear of using online services in the future, which was the most identified consequence, as well as damage to technology, dissatisfaction with the brand involved, loss of funds and identity theft.

However, the results also showed respondents were aware of, and used, a number of precautions when transacting online. Overwhelmingly respondents said they only entered their details on the websites of familiar brands, checked for https or the padlock symbol in the browser address bar, and used different passwords for different sites.

2. There is widespread awareness of cybercrime and cyber fraud

> 87 percent of respondents were aware of different types of tactics used by cybercriminals

A reassuring finding in the research was that consumers exhibited a high awareness of the tactics and methods used by cybercriminals to get personal details or steal money. However, 45 percent still fell victim to cybercriminals, which perhaps points towards the increase in sophistication of scams and tactics being used. The research also found that almost two-thirds of victims did not report the crime.

Overall, 87 percent of respondents were aware of cybercrime — with consumers most aware of emails impersonating known brands with lookalike website registrations, while awareness of fraudulent business emails sent with the intention of getting users to reveal personal information or credentials received a lower awareness rating.

Despite this widespread awareness, when consumers were asked about the Dark Web, 37 percent said they didn't know what it was used for. Among the ones that did know what it was, they displayed varying degrees of understanding of how it actually worked.

3. Damage extends beyond the bottom line

> 78 percent of consumers say cyberattacks on companies affect their perceptions of those brands

With the number of high profile cyberattacks and data breaches that have taken place in the last few years, respondents were asked how their perceptions of the brands involved were affected. Overwhelmingly, almost 80 percent said their views had been affected with 29 percent stating they had a negative perception of that brand and a further 49 percent saying perceptions were somewhat affected.

Participants were also asked about what other consequences they

believed could follow a successful cyberattack, and damage to a brand's reputation was the most cited example. This was followed by decreased brand trust, taking additional care in future engagement with the brand, and ceasing to engage with the brand.

4. Customers expect brands to protect them from cybercrime

> 74 percent said brands should have a fraud protection policy in place to protect consumers and expect the brand to educate them more thoroughly on the dangers of online fraud

The research also revealed that consumers believe they should be protected from fraud by the brands they interact with. Three-quarters of respondents said that brands should have a fraud protection policy to safeguard them, while 63 percent of consumers also said that brands should educate customers in online fraud, implement stronger logins and passwords (54 percent), and have a compensation process when things do go wrong (49 percent).

5. Consumers trust banking apps and online shopping sites to protect their data

> Mobile banking apps rated 54 percent in terms of trustworthiness versus 14 percent for social media advertising

When asked to rank various channels according to whether consumers believed they could keep private data and money safe, respondents overwhelmingly rated established methods — online banking apps and online shopping websites — higher than new entrants to the market. Social channels and social media advertising, for example, scored lowest on the trustworthiness scale.

Setting the scene: online behaviour, cybercrime and consumer experience

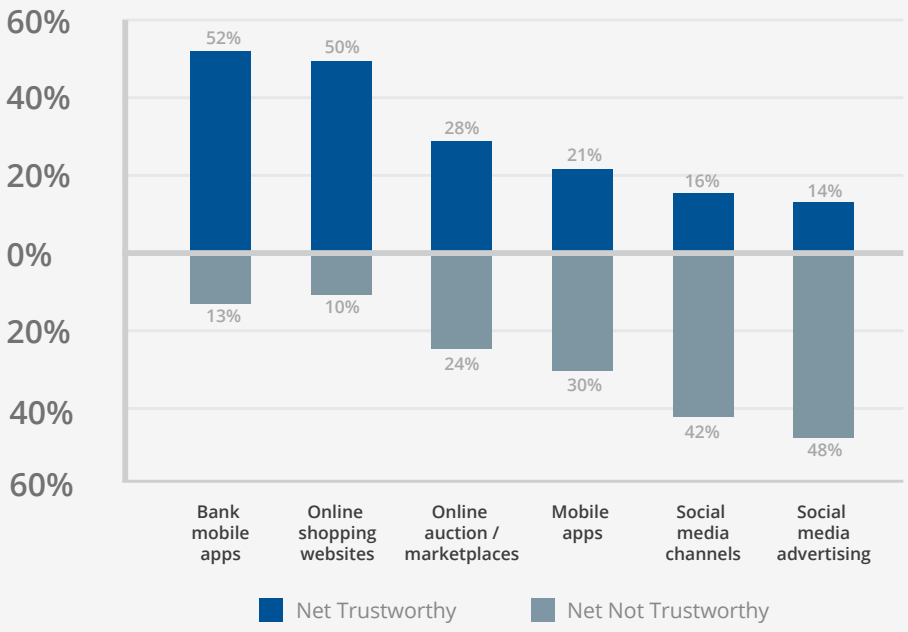
The incidents of cybercrime, fraud and cyberattacks haven't increased in isolation. Instead, as the Internet has grown in scope and scale, more consumers and businesses are using it in myriad ways — from day-to-day tasks, such as emails, to actual operations such as e-commerce. In the same vein, cybercriminals are capitalising on the opportunities presented by more brands having an online presence and more consumers using the Internet to transact.

The research shows how consumers interacted with companies online and how confident they were in doing so, as well as their experiences of online fraud.

Online channels, services and apps

Respondents were asked to rank various channels and apps on a scale of 1 (least trustworthy) to 5 (most trustworthy). The research found that they are most confident when it comes to using mobile banking apps — in terms of trusting the brands to protect their data and private details. This was highest in the USA and Denmark (58 percent) and the Netherlands (55 percent) and lowest in Germany (21 percent) and Italy (20 percent).

Trustworthiness of different channels at protecting money, data and personal details



[5] Number of digital banking users in the United States from 2013 to 2018 (in millions). Statista, 2013-2018. http://www.statista.com/statistics/333972/number-of-digital-banking-users-usa/
[6] Online banking penetration in selected European markets in 2015. Statista, 2015. https://www.statista.com/statistics/222286/online-banking-penetration-in-leading-european-countries/
[7] Facts on Online Shopping. Statista, 2015. https://www.statista.com/topics/871/online-shopping/
[8] Zaroban, Stefany. "U.S. e-commerce grows 14.6 percent in 2015," Internet Retailer, February 2016. https://www.internetretailer.com/2016/02/17/us-e-commerce-grows-146-2015

These figures perhaps reflect variations in global online banking usage. In the USA there will be almost 150 million online banking users by 2017[5] and penetration of the technology has already reached 85 percent in Denmark and the Netherlands, while penetration in Germany is just 51 percent and in Italy 28 percent[6].

Online shopping sites were rated as second most trustworthy, with an overall trustworthiness score of 50 percent. This was highest in the USA (55 percent) and Spain (56 percent). This isn't surprising considering that there are 205 million online shoppers in the USA[7] who spent $256 billion in 2015[8].

Not surprisingly, social channels and social media advertising scored the lowest when it came to confidence that consumers' private details would be protected. Social media channels scored a low 16 percent, while social media advertising scored 14 percent on the trustworthy scale.

We also discovered that 45 percent of the sample uses collaboration or storage sites online — such as Dropbox, iCloud or Google Docs. Usage was highest amongst the 18-35 year-old age group at 65 percent. Looking at the usage from a regional point of view, this figure was higher in Spain (57 percent) and Italy (55 percent). However, 62 percent of respondents in the UK, France and Germany stated they didn't use these types of sites at all.

Of the 1,566 respondents that did use these types of sites, 96 percent rated them as secure, stating they felt they kept their data and personal details safe.

Experience of cybercrime

The research uncovered that 45 percent of consumers had been a victim of cybercrime. There were some variances when it came to age, with 37 percent of 55+ year-olds becoming victims compared to 56 percent of 18-34 year-olds. While this might seem counterintuitive, this could possibly be as a result of the younger age group using more technology as part of their everyday lives, compared to older respondents.

Looking at regional figures, 63 percent of respondents in France and Italy and 62 percent in Spain reported being victims. The UK and USA demonstrated the lowest instances of falling victim to fraud (35 percent and 39 percent, respectively).

When asked about the types of cybercrime they had experienced, the most cited example was receiving false requests to "reset a password" for social media account logins (20 percent). This figure was highest in France (36 percent) and Italy (33 percent).

Other types of cybercrime included:

- An email that impersonated a company to solicit personal information and was used for identify theft— 17 percent overall, with Sweden (42 percent) and Spain (31 percent) being well above the average
- A virus that attacked their computer and retrieved personal information — cited by 14 percent of the sample, with figures in Spain (33 percent) and Germany (22 percent) being the highest
- An email scam that involved wiring money to a fraudulent source — cited by 14 percent of the

Business email spoofing scam

A business email spoofing (BES) scam is an email sent in a business environment that impersonates a person's identity, often using a lookalike domain name spoofing the organisation's primary sending domain. These scams take advantage of the trust relationships within an organisation by anticipating an employee's willingness to be less suspicious of an email from a company executive. According to Trend Micro, in two years there have been 22,143 incidents across at least 79 countries, costing businesses more than $3 billion[9].

Social engineering

Social engineering is a method used by cybercriminals to trick people into revealing information, like personal data or corporate credentials, by using techniques like phishing, pretexting (creating a believable scenario) or baiting.

Phishing

Phishing is used by cybercriminals to steal personal information, often through emails that look like they are from genuine sources. These emails typically ask for data like a credit card number, account number or passwords[10]. In the UK alone, these scams cost UK consumers £174 million in 2015[11].

Malware

Malware is malicious software that is used by hackers to compromise computers with the intent of stealing money, intellectual property, or personal data[12]. According to Internet security firm Symantec[13], between 2014 and 2015, the number of new malware variants increased by 36 percent.

sample, with France (23 percent) and Italy (22 percent) being most affected

- Receiving an email that impersonated a company and duped the consumer into logging into a lookalike website from where they stole financial login credentials — cited by 10 percent with Spain (26 percent) being the highest
- Receiving a fake invoice where a legitimate vendor account was compromised and false requests for payment were made — cited by 10 percent, with the highest instances coming from Germany (23 percent) and France (22 percent)

When asked about the industry in which the criminal activity took place, 30 percent of incidents originated

[9] Billion-Dollar Scams: The Numbers Behind Business Email Compromise. Trend Micro, June 2016. http://www.trendmicro.co.uk/vinfo/uk/security/news/cybercrime-and-digital-threats/billion-dollar-scams-the-numbers-behind-business-email-compromise
[10] What is phishing? PhishTank. https://www.phishtank.com/what_is_phishing.php
[11] Moore, Michael. "Phishing Scames Cost UK Consumers £174m in 2015," January 2016. http://www.techweekeurope.co.uk/security/cyberwar/uk-phishing-attacks-rise-2015-183964#X4kAX1BF6DL75K0g.99
[12] Avast Software. https://www.avast.com/c-malware
[13] Internet Security Threat Report. Symantec, Volume 21, April 2016. https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf?aid=elq_&om_sem_kw=elq_16390062&om_ext_cid=biz_email_elq_&elqTrackId=283a3acdb3ff42f4a70ab5a9f236eb71&elqaid=2902&elqat=2

in the banking and finance industries. This was especially high in the Netherlands (49 percent) and Italy (41 percent). Other kinds of companies involved in online fraud included:

- Online Services (like payment household bills, internet, electricity, telephone, etc.) (17 percent)
- Social media (11 percent)
- Consumer Goods (e.g. Electronics, clothing, DVDs, fashion, apparel) (10 percent)
- Entertainment (5 percent)

The consequences of online fraud

Among respondents who said they were victims of cybercrime, 16 percent said they lost money as a result. On a regional level, this was slightly higher in the USA, Germany and Denmark (18 percent) and much lower in Spain, where only 7 percent of the sample suffered this type of loss.

Overall, when asked about the amount of money that was stolen, 46 percent lost up to £250, 29 percent lost between £251-£1,000, and 20 percent lost more than £1,000. Of this amount, 4 percent of the sample lost more than £10,000. Large losses (of £10,000 or more) were higher in Denmark (13 percent), the UK (8 percent) and USA (7 percent).

Empty Wallet - Average Loss per Country

- UK £1,627
- USA $1,840
- Netherlands €1,414
- France €971
- Germany €496
- Italy €580
- Spain €453
- Denmark kr18,396
- Sweden kr15,622

Loss of money wasn't the only consequence of cyberattacks. Four in 10 consumers stated they experienced fear of using online services in the future, which was higher in Spain (50 percent of consumers). Other consequences of being a victim of cybercrime included:

- Damage to technology (e.g. malware infection on a computer) — 24 percent
- Dissatisfaction with the brand involved — 21 percent
- Identify theft — 12 percent

Of those that experienced fraud, only 35 percent reported the incident to an official body, such as the police. There were regional differences when it came to alerting authorities with 51 percent of consumers in France, 44 percent in the USA and 41 percent in the Netherlands reporting the incident. This figure was lowest in Spain where only 23 percent reported the incident, and 20 percent in Sweden.

Identity theft

Identity theft is a prevalent concern — particularly in the UK and USA. In the UK, fraud protection agency Cifas states that in the first three months of 2015 the number of identity theft victims increased by 31% compared to 2014[14]. Across the Atlantic, in the USA, about 15 million people have had their identities stolen each year, which equates to financial losses of more than $50 billion[15].

[14] "Number of identity theft victims 'rises by a third,'" BBC, May, 2015.
http://www.bbc.co.uk/news/uk-32890979
[15] Identity Theft Victim Statistics. Identity Theft and Scam Prevention Services.
http://www.identitytheft.info/victims.aspx

Precaution, prevention and awareness of the threat landscape

While the issue of cybercrime and online safety is an ever-present one, it is not stopping consumers from using the Internet to shop, bank, book travel or pay their bills. This is largely because there are ways to mitigate the risk posed by transacting in an online environment which includes taking certain precautions.

Safeguarding online behaviour

Our research did reveal that consumers are not in the dark when it comes to their online security. When asked about typical precautions taken when online, more than half (54 percent) of respondents said they only entered their details on websites of familiar brands. This was most prevalent in Italy (63 percent) and Denmark (60 percent).

Other precautions taken online include:

- Half of consumers check for the padlock symbol and https in the address bar, and only proceed with a purchase when these appear. This option is particularly popular with those in France (63 percent) and the UK (59 percent)
- 48 percent of respondents use different passwords for different sites, with more consumers in Germany (62 percent) making use of this option
- 43 percent of consumers use privacy settings on social media, particularly those in the 18-35 age group (54 percent). This approach is used more often in the USA (51 percent) and the UK (47 percent)
- More than four out of 10 (42 percent) respondents regularly reset their passwords, with the highest occurrence in the USA (52 percent) and Spain (50 percent)
- Almost two-thirds (64 percent) keep their online accounts to a minimum. This was higher than the overall average in the USA (42 percent) and Germany (37 percent)

More aware of online risk

Along with these safeguards when transacting online, we found that consumers demonstrated a good awareness of the tactics employed by online scammers and criminals to steal money, personal details or perpetrate other crimes.

Consumers were most aware of business email scams that try to trick users into revealing personal information or credentials, with an overall awareness of 96 percent, with half of the respondents stating they were very aware of the tactics. This figure was highest in Germany (61 percent) and Denmark (60 percent).

In addition, we found that 94 percent of respondents were aware of emails impersonating brands for fraudulent purposes requiring website login or registrations. Respondents in the Netherlands (98 percent) and Germany (96 percent) were more aware of

94

94 percent of respondents were aware of emails impersonating brands for fraudulent purposes requiring website login or registrations.

this tactic than the overall average. A further 45 percent of consumers said they were very aware of this scam, with only 15 percent stating they were only slightly aware.

When asked about scams involving paid advertisements in web browsers, there was an awareness of 88 percent with the highest awareness in Italy (93 percent) and Spain (91 percent). Of the overall figure, 33 percent of the sample was very aware, which was highest in Denmark (42 percent) and the USA (39 percent).

Other tactics included:

Scams on social media that direct users to fraudulent websites in order to steal credentials or personal information

- There was an overall awareness of 89 percent, with the Netherlands at 96 percent and Italy at 96 percent
- Of this figure, 34 percent said they were very aware, and only 20 percent said they were slightly aware

Mobile apps masquerading as legitimate apps to infect your phone and steal your user credentials

- With an overall awareness of 78 percent, Italy (89 percent) and Spain (88 percent) scored the highest
- Of that figure, only 25 percent were very aware, while 22 percent were slightly aware (36 percent in Spain) and 22 percent not aware at all (35 percent in France)

Scams built around file-sharing on cloud services via spoofed emails

- Consumers showed a 77 percent overall awareness, with the Netherlands (90 percent), Italy (85 percent) and Denmark (85 percent) citing the highest figures
- Of this figure, 24 percent were very aware, which rose to 31 percent in the Netherlands and 27 percent in the USA

29%

Of those that have accessed the Dark Web [...] 29 percent used it to purchase items.

The Dark Web

However, there are elements of cybercrime that consumers are not that familiar with. In addition to cyber attackers and criminals becoming more sophisticated, one of the challenges in properly mitigating the risk they pose, is the Dark Web. This portion of the Deep Web is filled with black markets where stolen credit card data can be traded, hackers recruited and illicit goods bought and sold[16]. Its anonymity, coupled with the prominence of untraceable crypto currencies, such as Bitcoin, makes it nearly impossible to track criminals, and increasingly difficult for brands to protect themselves against.

Despite 37 percent of consumers stating they didn't know what the Dark Web was used for, the rest of the sample displayed varying levels of understanding. Nearly half of the consumers in the study (49 percent) believe the Dark Web is used for criminals to sell illegal goods, stolen identities or personal information. In addition about a third (35 percent) believe it is to search for items not found on the mainstream Internet and over a fifth (22 percent) believe it is to protect privacy and anonymise browsing behaviour. Of the respondents, 7 percent say they have used an anonymous browser, like Tor, to access the Dark Web, with this highest in France (11 percent) and amongst those aged 18-34 (17 percent). Of those that have accessed the Dark Web, over half (55 percent) did so out of curiosity, with 48 percent saying it was to anonymise their internet activity and 29 percent used it to purchase items.

[16] Patterson, Dan. "How to safely access and navigate the Dark Web," TechRepublic, July, 2016. http://www.techrepublic.com/article/how-to-safely-access-and-navigate-the-dark-web/

Customer loyalty, perception and brand damage

Online shopping is increasing exponentially, as more organisations see the value in bolstering their physical shopfronts with digital platforms, or in having an online presence exclusively. According to Statista, the worldwide business to consumer (B2C) market is worth a staggering $1.47 trillion[17]. And with the recent spate of high-profile cyberattacks on global brands, organisations can no longer afford to fall victim to cybercriminals. As a result, brands need to ensure they are properly protected online, both in terms of safeguarding their revenue and reputations.

This sentiment is reinforced by our research —almost eight out of 10 (78 percent) consumers say cyberattacks on companies affect their perceptions of those brands, which could have a detrimental impact on the bottom line. According to a 2016 KPMG study[18], retailers could lose 20 percent of their customers as a result of cyberattacks.

The figure of 78 percent includes 29 percent of consumers saying that these companies should have had procedures in place to prevent cyberattacks. This expectation was highest in Italy (34 percent) and the UK (32 percent).

Looking at the specific ways in which consumers believed brands were affected by cyberattacks, overwhelmingly 71 percent of the subsample identified reputation damage. The figure was highest in the UK (81 percent) and Germany (80 percent), and lowest in Denmark (47 percent) and Italy (52 percent). Consumers also said they thought these attacks would reduce brand trust (65 percent), which was most cited in Germany and the USA, both at 76 percent. In addition, levels of engagement with affected brands were also believed to be impacted. 64 percent of consumers said they thought people would be careful of interacting with the brand in the future — 77 percent in the USA and 75 percent in the UK — while 53 percent said people would stop engaging with the company. This was most cited by respondents in the USA (68 percent) and Germany (67 percent).

Our research also found that consumers had certain expectations when it came to interacting with organisations online. Three-quarters of respondents felt that brands should have a fraud protection strategy in place to protect consumers. This attitude was more prevalent in the USA (82 percent) and UK (78 percent). In addition, 63 percent of consumers felt that brands should also focus on educating customers about online fraud — which a much higher percentage in Germany (73 percent). A further 54 percent of respondents stated organisations should implement more sophisticated logins and passwords.

This finding is underscored by the appetite respondents demonstrated for additional security measures. We found that consumers said they would feel more secure online if the organisations they interacted with used additional measures such as stronger passwords (77 percent) and biometric security measures, such as fingerprinting technology (69 percent). Interestingly, the most popular additional security method was two-factor authentication — a combination of something known (like a password) and something held (like a digital token) — that was cited by 80 percent of consumers. Two-factor authentication was especially popular amongst Spanish (91 percent) and German (88 percent) respondents.

[17] Statistics and facts about global e-commerce. Statistica. https://www.statista.com/topics/871/online-shopping/
[18] https://home.kpmg.com/us/en/home/insights/2016/08/cyber-attacks-could-cost-retailers-one-fifth-of-their-shoppers-kpmg-study.html

Conclusion

E-commerce presents a great opportunity for brands to generate revenue. Consumers benefit from more convenient shopping, banking and online bill pay. However, cybercriminals are also capitalising on the rise of sensitive transactions over the internet and exploiting these opportunities to defraud consumers.

With this prevalence of cyberattacks and cybercrime, perpetrated against both brands and consumers directly, there needs to be a multi-layered approach to online security and brand protection, in order to make sure cybercriminals are removed from the equation.

For consumers, it is about having the confidence to transact with brands online and have the assurance that their personal details and payment data will be kept safe. If they have this confidence, they will be inclined to spend money with the brand and remain loyal. As a result, brands need to ensure that they themselves can offer this protection against cyberattacks, keep their customers' data safe and ultimately protect their bottom line.

On the positive side, despite 45% of consumers being the victim of cybercrime, there is excellent awareness of the threat landscape and the tactics attackers are using to trick them. There is also a general acknowledgement by consumers that there are precautions being taken, as well as additional safeguards that can be used. In addition, consumers are looking to the brands themselves to do more when it comes to security, education and stopping cybercrime.

As the levels of sophistication of hackers and cyber attackers increase, organisations need to ensure that their efforts keep pace with market changes. This includes delving into areas of the web that were previously not considered — such as the Dark Web. Making use of technology solutions, security and brand protection experts can go a long way toward developing this multi-layered approach and ensuring neither consumer nor organisation is affected by cybercrime.

Methodology

The research was carried out on behalf of MarkMonitor® by leading research agency Opinium. The survey was carried out online between 26 August and 05 September 2016 on a sample of 3,457 global consumers aged over 18. The research covered nine countries — UK 1,002; USA 1,014; Denmark 209; France 201; Germany 208; Italy 218; Netherlands 201; Spain 204; and Sweden 200. Of those surveyed, 1,580 (46%) were male and 1,877 (54%) were female.

About MarkMonitor

MarkMonitor, the leading enterprise brand protection solution and a Clarivate Analytics flagship brand, provides advanced technology and expertise that protects the revenues and reputations of the world's leading brands. In the digital world, brands face new risks due to the Web's anonymity, global reach and shifting consumption patterns for digital content, goods and services. Customers choose MarkMonitor for its unique combination of advanced technology, comprehensive protection and extensive industry relationships to address their brand infringement risks and preserve their marketing investments, revenues and customer trust. For more information, visit **www.markmonitor.com**.

About Clarivate Analytics

Clarivate Analytics accelerates the pace of innovation by providing trusted insights and analytics to customers around the world, enabling them to discover, protect and commercialize new ideas faster. Formerly the Intellectual Property and Science business of Thomson Reuters, we own and operate a collection of leading subscription-based services focused on scientific and academic research, patent analytics and regulatory standards, pharmaceutical and biotech intelligence, trademark protection, domain brand protection and intellectual property management. Clarivate Analytics is now an independent company with over 4,000 employees, operating in more than 100 countries and owns well-known brands that include *Web of Science, Cortellis, Thomson Innovation, Derwent World Patents Index, CompuMark, MarkMonitor* and *Techstreet*, among others. For more information, visit **www.clarivate.com**.

More than half the Fortune 100 trust MarkMonitor to protect their brands online.
See what we can do for you.

MarkMonitor Inc.
U.S. (800) 745-9229
Europe +44 (0) 207 433 4000
www.markmonitor.com

MarkMonitor
Protecting brands in the digital world

Clarivate Analytics