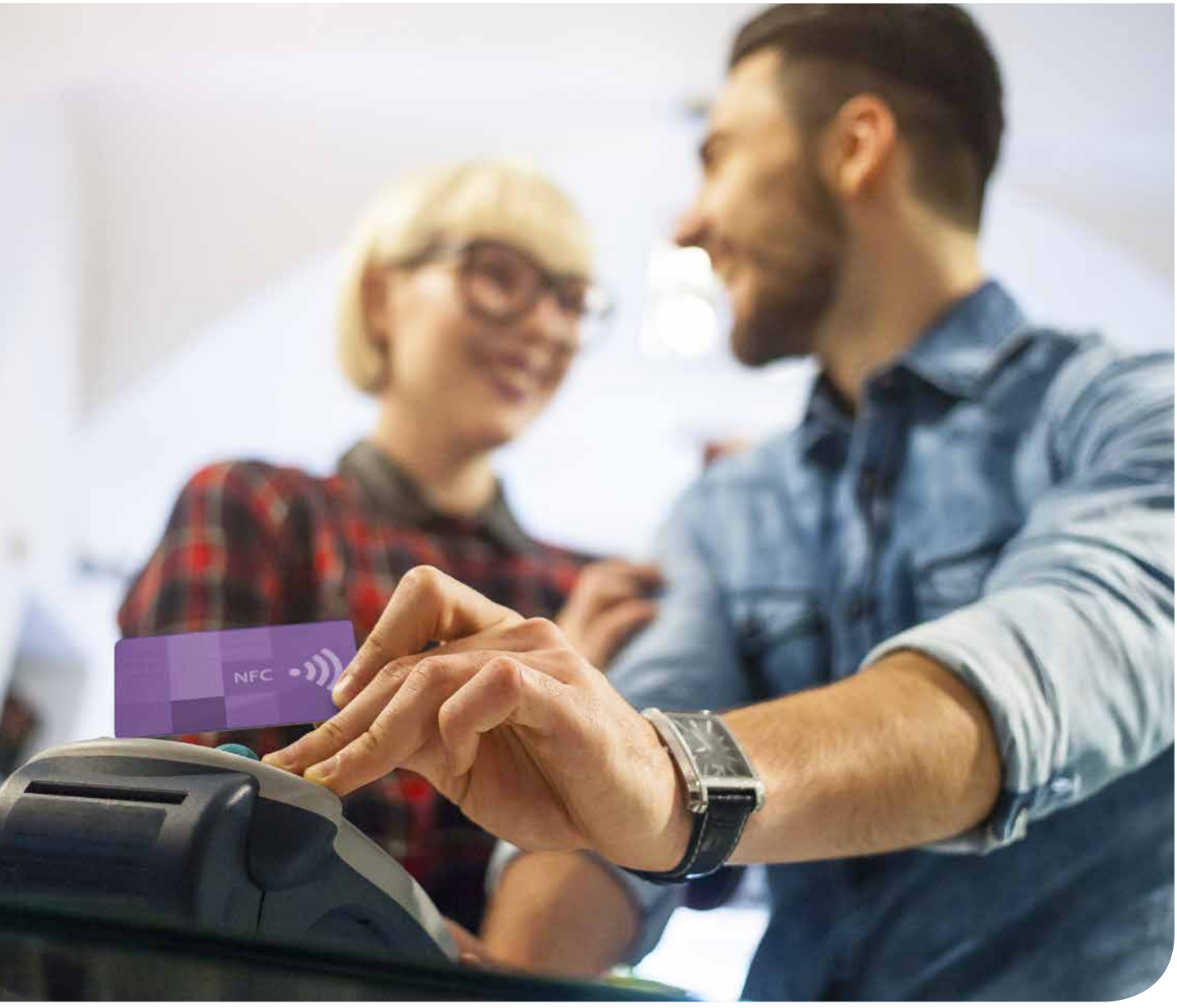
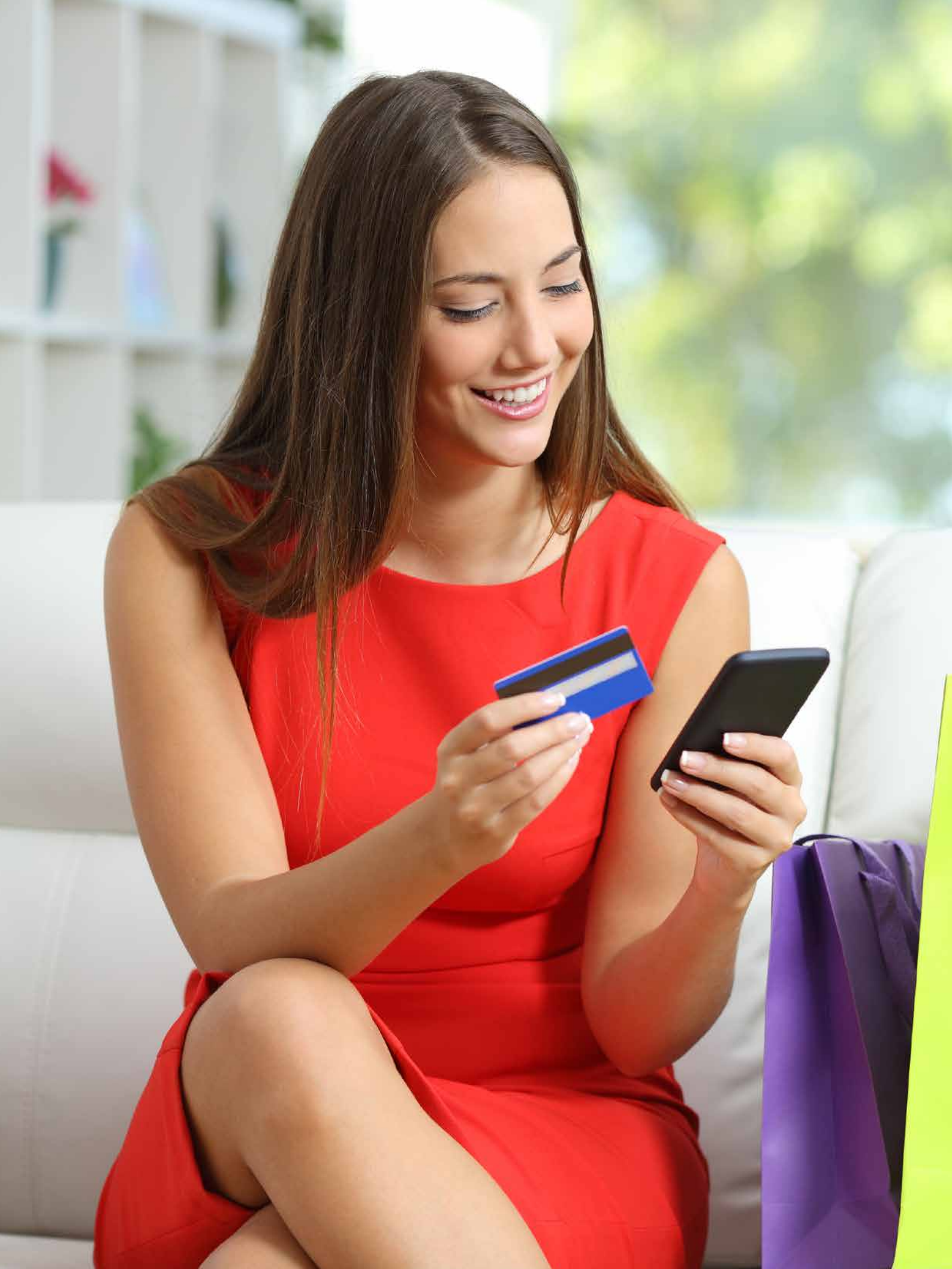
gemalto
security to be free



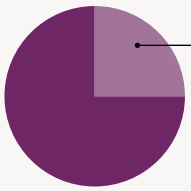
Data Breaches and Customer Loyalty Report

Broken Trust: Tis the Season to Be Wary



Breakdown of trust between consumers and companies

Trust is essential in building relationships, and for organizations that hold vast quantities of customer data, this is especially the case. The following are key findings from a recent global survey of consumers conducted by Gemalto on the impacts of data breaches on customer loyalty.



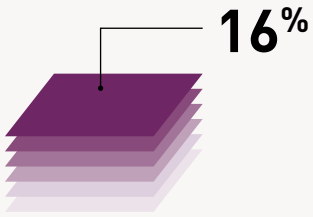
Only one quarter (25%) of consumers surveyed believe that companies take the protection and security of their data very seriously.Of the employed respondents, only around two fifths (38%) feel that their employer takes the protection and security of employee data very seriously.

31% of respondents have been a victim of a breach

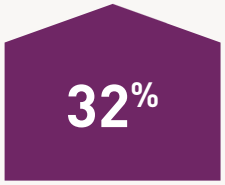
27% have been a victim of fraudulent use of financial **or** personally identifiable information

8% have been a victim of fraudulent use of financial **and** personally identifiable information

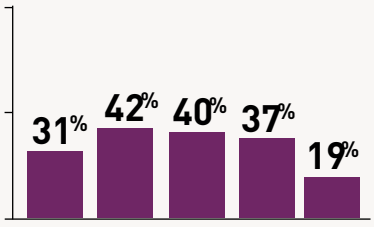
23% of consumers who have been a victim of a breach are considering taking legal action against the company that was breached.



Consequently, around one in six (16%) consumers expect that they will -or think that they could - be the victim of a breach within the next twelve months.



Many (32%) simply not knowing how likely they are to be breached. This perhaps indicates that consumers are beginning to lose faith in companies' abilities to protect their data.



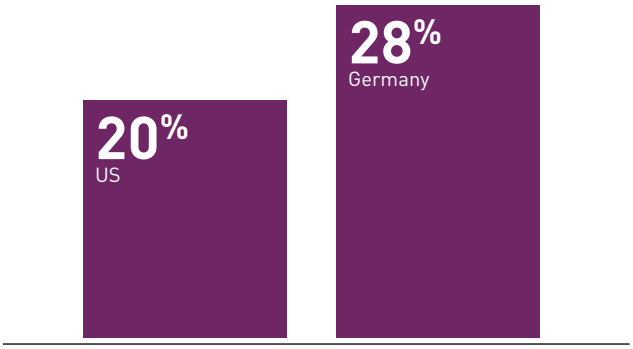
The survey revealed that 31% of consumers have already been affected by data fraud in the past. Around four in ten state the most likely causes for being a victim of a breach are visiting a fraudulent website (42%), phishing attacks (40%) or clicking a fraudulent web link (37%). The emotional impact of data breaches has also created apprehensive feelings towards businesses with nearly one fifth (19%) feeling they are likely to be a victim of one within twelve months to three years.

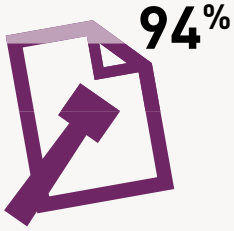
Companies Bear the Most Responsibility for Protecting Customer Data

69% of consumers feel that responsibility for protecting customer data lies with the company. For respondents from Japan, this difference is starker with 79% of consumers feeling that responsibility lies with the company. It is clear that consumers expect companies to have solutions in place to protect their data, and ultimately maintain/earn their trust by providing these solutions are effective.

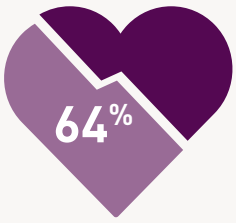
Many companies may not have the necessary security measures in place. Even for those that do, there is always the possibility that a breach may occur resulting in customers' personal information being exposed. This, according to surveyed consumers, is likely to have a detrimental impact on companies' relationships with their customers.

As well as pursuing the fraudsters, consumers are also going after organizations as they placed their trust with them. Those in Germany are more likely to have taken - or are considering taking - action against companies, than the other markets, with those in the US the least likely to say this (28% and 20% respectively).





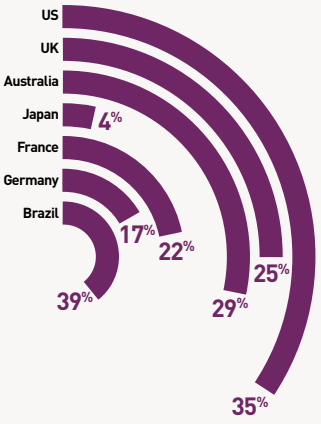
Almost all (94%) respondents would take, or would consider taking legal action against any of the parties involved in exposing their personal information in the future



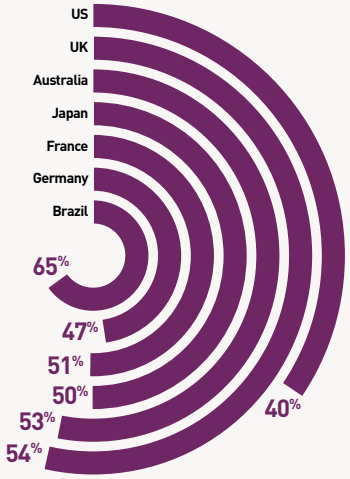
Nearly two-thirds (64%) would be likely to end their relationship with the company if financial and sensitive information was stolen. These are the potential pitfalls of a breakdown in consumer trust.

Regional Key Findings

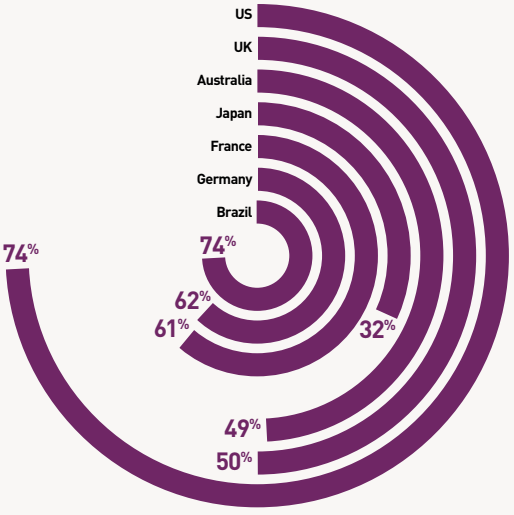
Percentage of respondents that feel companies take security very seriously



Percentage of respondents that would end relationship if financial and sensitive info is stolen/lost



Percentage of respondents that feel risk to data increases during holiday shopping season



Gap in awareness and education

The fact that the majority (75%) of surveyed consumers do not think that companies take the protection of their data very seriously suggests that action needs to be taken. Companies need to increase their security measures and they need to communicate how consumers can better protect themselves from data theft.

31%

31% have been a victim of a data breach

27%

27% have either been a victim of fraudulent use of financial or personally identifiable information

One in ten (12%) of these respondents are unaware of the most likely causes leading to them being breached

This poses the question: how do these consumers know how to prevent a breach occurring in the future?

The risk of mass-market websites

If companies do more to communicate the security measures that they have in place to protect their customers' data (assuming that they have such measures) this may help consumers to feel more at ease and reassured that companies are doing all that they can to protect their personal information. However, the onus does not, or should not, lie only with organizations. Consumers can also take measures to protect themselves against possible breaches.

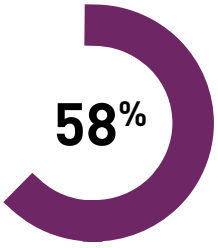
90% of consumers feel that there are apps and websites that pose risks to the protection and security of their personal information

55% of consumers believe that social media sites expose them to the greatest risk.

43% of consumers believe that banking apps or websites expose them to the greatest risk.

40% of consumers believe that adult content sites expose them to the greatest risk.

This is perhaps not surprising as nearly half (47%) of consumers don't use multi-factor authentication when accessing their social media accounts. They are not taking all steps possible to protect their personal information. Social media is used by the masses on a daily basis, and personal information such as date of birth, address or phone number etc. is usually easily accessible within these sites. Should fraudsters gain access to consumers' social media data, they may find all the necessary personal information to aid them in stealing an identity and/or accessing further sensitive information. Additionally, just 25% of surveyed consumers that actively use online retail accounts say that all of the online retail apps/websites that they use require two-factor authentication to secure online transactions.



Banks at least do things differently. Around three in five (58%) respondents who actively use online/mobile banking state that all of their banks use two-factor authentication to secure their internet banking, with a further 25% saying that some of their banks do. It is possible that mass market websites, such as social media and retail sites, could benefit from following the example set by the banks to avoid risking punishment from consumers in the future. Implementing mandatory two-factor authentication has the potential to avoid mass exposure of customers' personal data. Failing that, consumers must be made aware of the importance of using such a facility.

However, there might be only so much organizations can do. Despite the concerns that consumers have with mass market websites - not to mention recent coverage of high profile breaches - most consumers (54%) admit that they tend to use the same passwords across their accounts, a well-known faux pas when it comes to security. Surveyed consumers from Japan are far more likely (68%) than consumers from any other country to use the same password across accounts, with those from Germany least likely (39%) to do this.

2015 Holidays: unlikely to be a season of joy

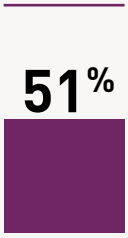
While this season presents financial opportunity for companies, if they do not uphold consumers' trust it could turn out to be an opportune season for fraudsters instead.

59% of respondents feel that the threat to their personal information increases to some extent during the holiday season

Summary

Organizations need to take responsibility for securing customers' personal data, as it is less likely that consumers will do so themselves. Once the right security solutions are in place, such as encryption and multi-factor authentication, companies should consider an education campaign to inform consumers about the measures. Equally important will be educating consumers about the measures that they can take to protect their own data, such as using different passwords for various accounts. In the long term, this will prove advantageous for companies and consumers, and leave out the fraudsters.

Half (51%) think that they are likely to be a victim of a breach, during this period



Demographics

Independent technology market research specialist Vanson Bourne was commissioned by Gemalto to undertake the research on which this report is based. 5,750 consumers were interviewed during October and November 2015. 1,500 interviews in the US, 500 in Brazil and 750 in each of the following countries: UK, Australia, Japan, France and Germany. To qualify for the study, consumers had to actively use online/mobile banking, social media accounts or online retail accounts.

> 5750 Consumers

> 1500 Interviews

Gemalto offers one of the most complete portfolios of enterprise security solutions in the world, enabling its customers to enjoy industry-leading protection of digital identities, transactions, payments and data – from the edge to the core. Gemalto's portfolio of SafeNet Identity and Data Protection solutions enable enterprises across many verticals, including major financial institutions and governments, to take a data-centric approach to security by utilizing innovative encryption methods, best-in-class crypto management techniques, and strong authentication and identity management solutions to protect what matters, where it matters. Through these solutions, Gemalto helps organizations achieve compliance with stringent data privacy regulations and ensure that sensitive corporate assets, customer information, and digital transactions are safe from exposure and manipulation in order to protect customer trust in an increasingly digital world.

GEMALTO.COM

gemalto
security to be free