Three-quarters of UK consumers would walk away from a business that has been hacked

Submitted by: Origin Comms Ltd
Wednesday, 8 June 2016

- Centrify study shows only half think companies take enough responsibility for customers' security

- Banks and HMRC perceived as best at dealing with hacks, while retailers and travel sites are below par

A new study from Centrify (https://www.centrify.com), the leader in securing enterprise identities against cyberthreats, reveals that 75 per cent of adults in the UK would stop doing business with, or would cancel a membership to, an organisation if it was hacked. This suggests, however, that a quarter would carry on using that company, despite the security risks to both personal and financial information.

The study of 2,400 people across the UK, Germany and the US, looks at consumer attitudes towards hacking and how likely consumers are to continue transacting with businesses, including retailers, banks, government, travel, health and hospitality organisations, after a cyber attack.

To some degree, most consumers expect to be hacked today, with 73 per cent in the UK admitting that it has become normal or expected for businesses to be hacked. Despite this, only half feel that they are taking enough responsibility for the security of their customers' or members' personal information.

Most people believe that the burden of responsibility for security falls to the business. About two-thirds in each country rated organisations as a 9 or 10 on a 10-point scale in terms of how responsible they should be for preventing hacks and securing the personal information of their customers.

Individuals most likely to take their business elsewhere following a data breach include those who have had their personal information compromised in a hack previously, people who are tech savvy and who shop regularly online.

"If three-quarters of customers are prepared to walk away from a business if it has been compromised, then what kind of message is this sending to those organisations?" says Bill Mann, Chief Product Officer at Centrify. "We would say that it is a very clear call to action to those businesses to sort out their processes and do everything they can to protect confidential customer information.

"When companies put customer data at risk they are really putting their entire business at risk. People simply will not tolerate doing business with potentially risky organisations, so it's time for them to take full responsibility for their security and put the proper measures in place once and for all," Mann adds.

Banks and tax office good, retailers and travel sites bad

According to the survey, financial institutions have the best reputation when it comes to dealing with security breaches compared to other sectors. They top the list of seven different industries in terms of

how well they handle security issues for their customers, although government/local government and HMRC come in a respectable second. Worryingly, retailers rank fourth and travel sites fifth in each country, while membership and hospitality businesses are the lowest ranked.

The Centrify study also shows that organisations are increasingly going public with news of security attacks and data breaches, often notifying their customers directly. Around one third in the UK have been notified of a hack. Of those notified of a hack, less than half (45 per cent) of those in the UK found out that their personal information, such as an address or credit card information, had been compromised.

Monitoring bank transactions and changing passwords – both with the hacked organisation and on other sites – are the most common steps suggested by organisations after advising customers of a hack. It is less common for a business to recommend that customers request any kind of alerts, such as a fraud alert, or to consider a security freeze, or implement multi-factor authentication.

The Centrify study and infographic can be found at: www.centrify.com/identity

Notes for editors:

Top tips for consumers:

- Use good password hygiene – do not use the same or similar password across multiple online accounts, and do not use personal information or easily guessed words in a password.
- At the very least make sure your most critical accounts have the strongest passwords.
- Never hand out personal or financial details to those sending emails asking for them, even if they look genuine, and keep a close eye on your bank statements.
- Online payments – check for a padlock symbol in the browser or use safe systems like PayPal.
- Ask your bank, email or other online services provider if they offer other forms of security, e.g. multi-factor authentication (password + a token, PIN, text or biometrics) – and if they do, enable it.

Top tips for businesses:

- Educate customers about good ‘password hygiene’ – make it core to your security policy.
- Make sure you offer alternatives to just passwords, such as multi-factor authentication or biometrics, and let your customers know about them.
- Educate your own staff and have clear security policies internally. Also, control who has access to what data, giving privilege access only to those who need it as part of their job.
- Encrypt sensitive data, including customers’ credit/debit card details.
- If your site has been hacked, inform customers as soon as possible. Under the new EU General Data Protection Regulation (GDPR), a business will be required to notify the ICO (Information Commissioner’s Office) of a data breach no later than 72 hours afterwards, unless it is able to demonstrate that the breach is unlikely to result in a risk for the rights and freedoms of individuals.

Methodology

The Centrify survey was conducted online among 2,400 adults in the UK, US and Germany (800 in each). It was conducted in late February and early March 2016. In order to ensure a representative sample, the data in each country was weighted slightly by region, gender, income, and age.

About Centrify

Centrify is the leader in securing enterprise identities against cyberthreats that target today's hybrid IT environment of cloud, mobile and on-premises. The Centrify Identity Platform protects against the leading point of attack used in data breaches — compromised credentials — by securing an enterprise's internal and external users as well as its privileged accounts. Centrify delivers stronger security, continuous compliance and enhanced user productivity through single sign-on, multi-factor authentication, mobile and Mac management, privileged access security and session monitoring. Centrify is trusted by over 5000 customers, including more than half of the Fortune 50.

Contact:

Amanda Hassall, PR Consultant, Origin Comms
T: +44 (0) 16 2882 2741
M: +44 (0) 78 5535 9889
E: amanda@origincomms.com