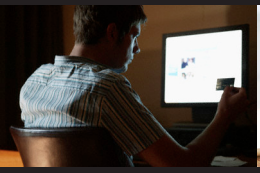
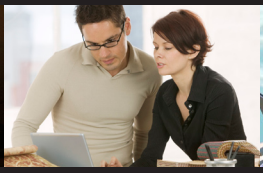
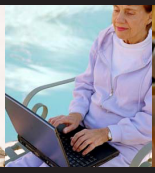
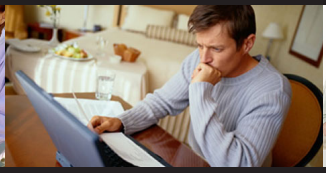
DON'T PUT YOUR ID AT RISK

THE GUIDE TO PROTECTING YOUR INFORMATION ONLINE









symantec™

moneysupermarket.com®
the price comparison site

Introduction to the risky business guide

Trusting the web with your personal data is becoming a risky business, both for consumers and for companies.

More and more questions are arising about the security - or lack of it - of online and offline information. That's why we decided to carry out the Risky Business survey. We wanted to get a snapshot of how consumers and businesses felt about the current situation, and what they were doing about it.

Through the survey, we wanted to find out exactly how safe our personal data is; how security conscious we are, how we feel about the organisations that hold our data, and how companies get affected when data gets lost or stolen.

As part of the research, Symantec and MoneySupermarket.com spoke to 1000 consumers and 600 businesses in the UK.

We also carried out a large social experiment in central London, offering five pound gift vouchers to people in the street, to see exactly how much personal information they would give away for free. The answer, by the way, is a lot.

The survey helped us to find out other things too. Do consumers or businesses think they are more responsible for ensuring that personal information stays safe? When it comes to online data breaches, do consumers blame companies, or do companies blame consumers for being careless when using the web?

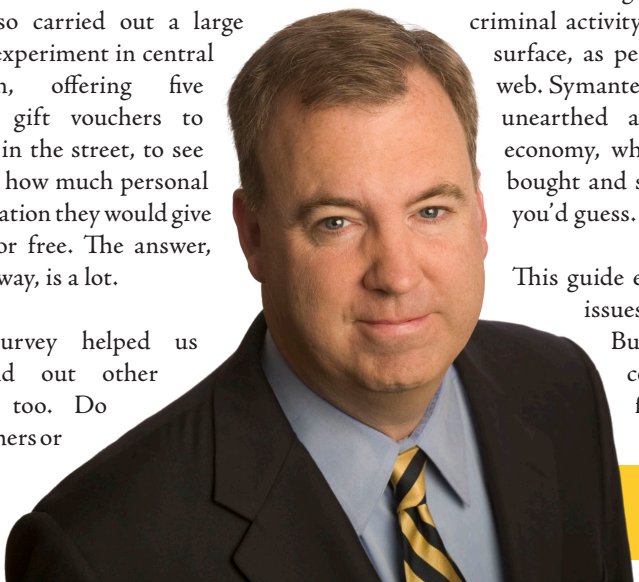
Although there is responsibility on both sides, the strong emotions in both camps may surprise you.

We found out exactly how many people believe their personal information is not secure in the hands of the companies who hold that data. We also found out how many people think that reckless or repeated data breaches should be punishable by jail sentences.

We also asked consumers how their shopping habits have changed in the light of the credit crunch.

In addition, we got an insight into the criminal activity that goes on below the surface, as people innocently surf the web. Symantec research has previously unearthed a massive underground economy, where whole identities are bought and sold for less money than you'd guess.

This guide explores some of the key issues arising from the Risky Business survey, and we are confident that you will find it interesting and informative reading.



John Brigden, Senior VP EMEA, Symantec

Just how much data do you share online?

– an average human online footprint

Richard Archdeacon, Director of Innovation Group EMEA, Symantec

Ecotourism is a way of visiting interesting places around the globe and leaving a light footprint.

Travelling around the web, on the other hand, leaves a surprisingly heavy 'online' footprint - heavier then you'd realise.

As we browse, fill in forms and do our shopping, we leave vital personal information with everyone from retailers to banks and government departments.

In fact, simply surfing the web can mean passing on information about ourselves and our browsing habits to hidden organisations.

In its legitimate form, this "identity leakage" then gets passed on to marketing firms and other organisations, with our business research discovering that 17 per cent of companies pass on customer data to their partners.

We also found that companies held all sorts of personal information on their computer systems.

For example, 92 per cent of them recorded peoples' names, and 80 per cent their phone numbers, as you'd expect. Three quarters of companies grab people's e-mail addresses as well.

Besides that, 49 per cent hold date of birth information, and 45 per cent hang onto your bank details. A third of them record credit card details, and 12 per cent store your passport information.

But if you think that's bad, imagine how much information we give away for free on social networking sites like Facebook, Bebo and MySpace. It only takes a little bit of detective work for a fraudster to link together various bits of personal information that they can find online.

Using various sources, criminals are able to link up names with dates of birth, bank details, phone numbers and e-mail addresses with relative ease – ultimately rebuilding your identity from what is initially a variety of harmless "identity leaks".

And they're not afraid to use our children's social networking sites to get information about us and our households. Fraudsters can turn even a small clue into a full record on a child and parent. They, in turn, trade and sell that private data to make money.

To give you an idea of just how quickly this can be done, our own research has found that criminals are able to get hold of complete identities for as little as 50p a go, and can then exploit this to make up false credit cards and so on.

It's inevitable that we're going to leave an online footprint, but the question should then be how we manage it afterwards.

Where, when and how data goes missing

Richard Archdeacon, Director of Innovation Group EMEA, Symantec

There are some interesting parallels between data that's held online on computers, and 'offline', in paper files or on disk.

For one thing, as we've seen on the news, information can get lost or stolen whether it's in a folder, on a laptop, or on a web server, and consumers are well aware of this.

Our consumer research found that a huge 75 per cent of people are concerned by how much data companies hold about them, both online and offline. In fact, 57 per cent of people believed that large companies were most likely to lose their data.

Half of the people expected to lose data paying for something on the Internet; 36 per cent expected to lose it through a Government department; and 57 per cent paying by credit card in a shop.

Securing data held offline is relatively straightforward. For starters, you can lock your documents in a cabinet.

Destroying old credit and store cards, and receipts and letters showing your account details is also good practise. Many individuals and businesses use paper shredders to ensure their personal information is well and truly destroyed.

On the other hand, the risks of losing information online, or having it stolen, have become far greater than the offline risks. It's easier for criminals to swipe data from the web than break into your home.

Phishing is one of the main techniques used by web criminals to steal information. These scams attempt to gather sensitive information by masquerading as trustworthy e-mails or websites.

User error is also responsible for sensitive data falling into the wrong hands. The web user might fail to check the security of a site, or click onto a web site that installs 'key-logging' software that swipes their private information.

But the big unknown is exactly how much personal information is lost by public and private organisations - of all sizes.

One survey suggests that 60 per cent of public and private sector organisations fail to report data security breaches to their customers, and half fail to tell the police or authorities.

Our own business research shows that companies have experienced a mix of external and internal data breaches, as well as data loss. It only takes one or two pieces of identity data to fall into criminal hands for them to start being able to build a picture of your real identity, ultimately turning it into a format that they can use for criminal gain.

However, most businesses, 84 per cent, blame consumers, saying they should do more to protect themselves when it comes to data risk.

But underlying all of these data losses, our research has found, is an underground economy running on cybercrime servers. Criminals are becoming increasingly sophisticated, taking advantage of lapses in security to trade confidential consumer data, and buy and sell our stolen identities. As with any market, once an identifiable revenue figure is attached to a product, in this case consumer data, demand will quickly increase.
Risky Business

How to identify a secure website

Guy Bunker, Chief Scientist, Symantec

One of the great things about the Internet is the variety of websites out there. At one end of the spectrum, you've got pages created by fans and hobbyists who seem to know everything about their favourite subject.

At the other end of the spectrum, you've loads of great shopping, news and entertainment websites. Our research discovered that a staggering 75 per cent of people are more likely to shop online for items now than they were six months ago. That translates as a load of credit card and personal details whizzing through cyberspace.

But how do you actually know you've arrived at a website that's secure, and not one that will try to give you a virus, or steal your personal information?

Many Internet villains are just waiting for you to click on a link in a spam e-mail they've sent out. When your browser opens up their website, which might mimic an authentic banking or retail site, they've got you.

Surprisingly, our research also found that 18 per cent of people don't bother to check the security of the websites they use. But fortunately, there are several easy checks that you can carry out to ensure you're using trusted sites.

Firstly, look for the padlock icon in your browser's status bar before submitting financial information through a website.

This little icon tells you that your information is secure during transmission. What's more, if you double-click on the padlock, you can view the website's security certificate, to check it's a reliable site.

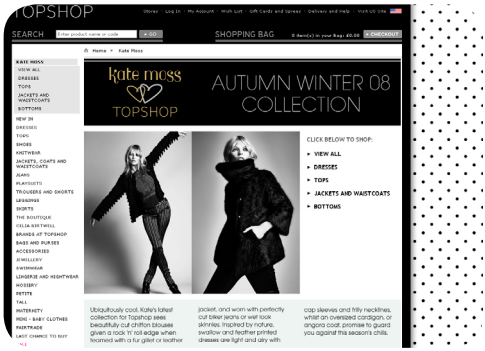
Another thing you can do is rely on recommendations for websites from friends that you trust. By sticking to the trusted brands and sites, and not straying too far off the beaten track, you can lower your security risk.

Also, make sure you always type in the URL yourself, and don't just use links from other web pages or e-mails. By doing this you are less likely to be sent off to a harmful site.

Finally, having top quality security software is an absolute must. Not only can it protect you from spam, computer viruses, and hacker attacks, it will also protect you from opening up websites that are known, or suspected to be bad news.

What not to do

DON'T browse the web without good security software
DON'T click on web links in spam e-mails
DON'T send personal information using sites you don't trust



Changes in the banking code

Caroline Cockerill, Norton Online Safety Advocate

Earlier this year, several changes were made to the Banking Code. This is the code of conduct banks use to ensure they're acting in the consumer's interest.

One of the changes holds the individual liable for any online fraud or financial loss if they do not have adequate protection on their PC. That is, if they don't have "up-to-date" anti-virus protection.

This has implications for both online banking customers, and users of financial trading and information sites.

The code itself advises customers to keep their PCs secure, telling people to use up-to-date antivirus and spyware software and a personal firewall and to keep their passwords secret.

The new code shifts liability for online banking fraud to the consumer. Our research found that 80 per cent of people were not aware of the changes.

For banks and retailers, among others, online security is a huge issue. Over the years, these organisations have lost tens of millions of pounds because of fraudsters.

As a result, there's been a shift in thinking in the business world, and our research reflects this.

84 per cent of businesses in our survey believed consumers should do more to protect themselves when it comes to data risk.

It's clear that the results of the credit crunch continue to affect both businesses and consumers.

Businesses, and banks in particular, are becoming more wary and security conscious, as the bottom line is ever more important.

For consumers, it has made them look again at their spending behaviour. For example, our research found that 84 per cent of people agree or strongly agree that the credit crunch has made them shop around for better deals.

Three quarters of people said they are more likely to shop online for items now than they were six months ago, and this is a massive change in shopping behaviour.

But for the fraudsters, it means there are more people online to target.

What consumers need to know

In March 2008, changes were made to the Banking Code.

One change allows British banks to refuse to compensate victims of online fraud.

The code says that banks may refuse to compensate victims if they fail to follow advice to use up-to-date anti-virus, anti-spyware and personal firewall software

Consumer faith in companies and brands

Caroline Cockerill, Norton Online Safety Advocate

Losing customer data can have a terrible effect on a company's brand equity. Companies invest millions of pounds building their company brand and identity to gain the consumers' awareness and trust.

So, imagine the brand carnage when a laptop is stolen, or worse still, is left in the back of a cab - containing vital customer information. The effect on brand equity can be devastating.

According to our research, consumers are not all that forgiving either, when it comes to data breaches. We found that nearly four out of five people believe their personal information is insecure in the hands of the companies who hold that data.

An even higher number, 89 per cent of people, believe that reckless or repeated data breaches should be a criminal matter and punishable by imprisonment. Four out of five people said there should even be a 'one strike and you're out' rule when it comes to data loss.

We also found that 57 per cent of people consider large companies to be untrustworthy, and most likely to lose their data. As a result, 93 per cent of people said they would not provide personal details to a company which had past problems of losing data.

When it came to our business research, we found that companies were well aware of the problems.

More than half believed that recent high-profile data breaches have had an impact on how willing consumers are to hand over their data. Three quarters of businesses said they would expect to lose customers if a data breach occurred in their company.

Almost half of the firms reckoned that the impact of a data breach on their business would be the immediate loss of customers. Whilst 59 per cent said it would be harder to attract new customers, when the dust had settled.

Consumers are also growing aware that their personal data frequently gets sold on to other companies, or falls into the hands of cyber criminals.

The downside for businesses is that this all takes a toll on their brand equity.

The value of your personal data

Guy Bunker, Chief Scientist, Symantec

What price would you put on your personal data? As part of our consumer research, we asked people to put a monetary value on different pieces of their identity. In other words, this is the vital information that we all use when making transactions on the Internet.

Most people thought that their name was worth about a pound, and 89 per cent would happily share it with someone they didn't know.

But when it came to their date of birth, people were a little bit more wary. Only 23 per cent of people said they would share it with someone they didn't know, and people tended to put a value of £100 on it.

As for other pieces of important information, bank and credit card details, passports and password information, most people valued these at £100 apiece. Only 1 per cent of people said they would share their bank details, passport or password information with someone they did not know.

In reality - and this may come as a shock - your personal information isn't worth all that much to the cyber criminal, unless they're dealing in bulk.

A recent Symantec Internet Security Threat Report found that UK bank account details are being sold in bulk on "cyber crime supermarket" style underground economies, for as little as £5 an account.
We also observed a new phenomenon of bulk buying of confidential consumer data, where criminals are packaging up personal details in bargain bundles.

For example, during the last six months of 2007, bundles of 50 credit card numbers were for sale at just £20 each – a miniscule 40p a card - and 500 credit card bundles were available for £100, which is even less per card.

As well as credit cards, whole identities are available for sale on the cyber supermarket, with a significantly larger price tag.

Our researchers also found that identity trading is on the increase, with some details being sold for as little as 50p. Even stolen eBay accounts are up for grabs. Plus, as the underground economy grows, cyber criminals are constantly changing and adapting their methods of achieving identity fraud.

So if you were to ask how much your identity is worth at the moment? It's all a case of supply and demand. If you've protected it well, it won't have a value per se, as it's safely your own, but once it has a value and is being traded, it could be too late to worry about it.

Symantec personality profiles and how to reduce risks

Tim Newhouse, Moneysupermarket.com

We don't all use the web the same way. Your age, financial status and where you live can help indicate what sort of web surfer you're likely to be.

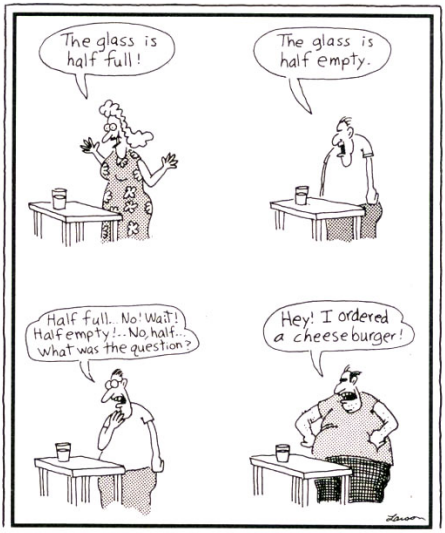
Sophisticated cluster analysis in the research identified five main personality profiles in Britain.

Wealthy Warriors are the group least affected by the credit crunch. Having accumulated their wealth over the years, their need to shop around for better deals isn't as great as that of others.

Cagey Crunchers are the most price-conscious consumers. They have been affected by the credit crunch in one way or another, and incessantly look for the best bargains online.

Serene Surfers have quite a neutral attitude towards the credit crunch. Being web-savvy, this middle-aged group are enthusiastic Internet shoppers and more likely to shop online now than they were six months ago.

Restless Retributionists are younger people seeking out the cheapest prices in the wake of the credit crunch. They are highly concerned about the number of companies who keep their personal information and think repeated data breaches should be a criminal matter.



The four basic personality types

Optimistic Ostriches are happy-go-lucky … at the moment. They are indifferent to the credit crunch, only somewhat concerned that some of their data could be insecure, and don't place high value on this information.

When you've worked out which personality type most closely matches you, check out the guide below for your best strategy going forward:

How to reduce your online risk

Wealthy Warriors: With more wealth to protect, only use secure transaction sites, get good quality security software, and guard your usernames and passwords.

Cagey Crunchers: Carry on shopping on secure websites, as you already do. Change your passwords frequently and stick to recommended sites for your bargain hunting.

Serene Surfers: As relatively new Internet shoppers, avoid marketing surveys that want lots of private information, and avoid clicking on spam email 'special offers'.

Restless Retributionists: As relentless shoppers, make sure you change your passwords frequently, avoid trading personal data for cheaper deals, and guard your PC with good security software.

Optimistic Ostriches: Ostriches are slap-dash when it comes to security so tighten up in all areas, and go to annualcreditreport.co.uk to make sure you haven't been a victim of identity theft.

Being a responsible digital citizen - our advice

John Brigden, Senior VP EMEA, Symantec

Our research findings indicate that there are strong feelings on both sides when it comes to who should secure our personal data.

Consumers feel strongly that businesses should keep their information safe. Businesses, including the banking industry as we've mentioned, say it's down to consumers to practice safe surfing.

In reality we all know consumers need to work in partnership with companies to protect our data. Companies can suffer brand damage, but at the end of the day, it's the individual who's personally affected by identity theft.

As more and more people choose to use the web for shopping, banking and entertainment, it's more important for us to become responsible digital citizens.

This means we all have a responsibility to look after our own data and passwords, use adequate and high-quality computer security, and use the web in a safety-conscious way.

Companies clearly have responsibilities to protect consumer data, and these are outlined in the law, and 'codes of conduct'.

But consumers are also responsible when it comes to protecting their own data.
We have learned how easy it is for criminals to get hold of our details, and create bank accounts and credit cards using stolen identities.

Ignorance is no longer an excuse - it's time for all web users to act and become responsible digital citizens.

Here are five things you can begin doing immediately to safeguard yourself against cyber criminals.

Use Security Software

All web users should use high-quality security software to protect them from viruses, spam, hacker attacks and malicious websites.

Practice Safe Surfing

Ensure your browser has its secure settings turned on, to block malicious web pages and web applications. Safe surfing can also be aided by typing in a web address yourself, rather than following a link you can't vouch for.

Stick To Trusted Brands

By sticking to the trusted brands and sites, and not straying too far off the beaten track, you can lower your security risk. Also, use recommendations for websites from friends you trust.

Ignore Dodgy E-mails

It is good practice not to click on web links in e-mails from people you don't know or trust, or that look official but you suspect may be 'phishing' scams.

Look For the Padlock

Look for the padlock icon in your browser's status bar before submitting financial information through a website. This tells you your information is secure during transmission.

Thanks for reading.


symantec™


moneysupermarket.com®
the price comparison site