CYBERCRIME FUTURES

An Independent Report for AVG Technologies

09-09-2011

HALF THE UK'S 18-35-YEAR-OLDS DON'T UPDATE THEIR ANTIVIRUS SOFTWARE

ONLY 4% OF FRENCH WEB USERS WORRY ABOUT IDENTITY THEFT

56% OF WEB USERS IN GERMANY SAY INDIVIDUALS SHOULD BE RESPONSIBLE FOR THE SAFETY OF THE INTERNET

JUST 2% IN THE CZECH REPUBLIC AGREE

FUTURE POLL

FUTURE POLL

p4	1	Overview
p7	2	Cybercrime – reality, threat, future
p13	3	Smartphones – the PCs in your pocket
p17	4	Wetware – the weakest link
p22	5	Responsibility 2.0
p25	6	A new climate of risk
p30	7	Key take-outs
p32	8	Bibliography and sources

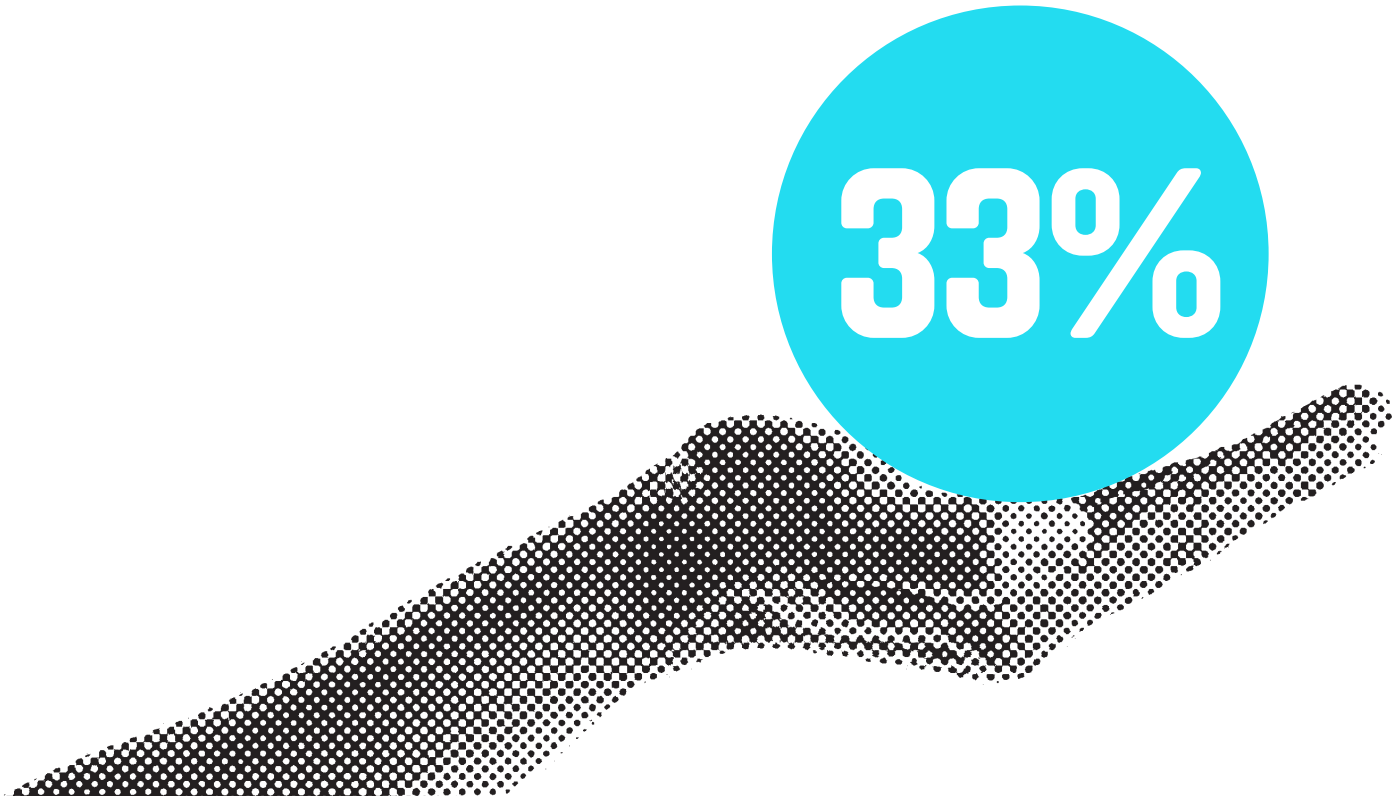
This document	As part of our continuing commitment to sustainability, this document is designed to be easily read and shared in a digital format. If a print version is required, the recommended setting is to print double-sided in a landscape format, bound on the short, left-hand side.
About us	Future Poll is the research division of The Future Laboratory, one of Europe's foremost consumer research, trends, insight, forecasting, and brand innovation consultancies. Via its online network, LS:N Global, it speaks to 300 clients in 14 lifestyle sectors on a daily, weekly and monthly basis.
Contact	For further details about all of our services visit futurepoll.com, or contact info@futurepoll.com and one of our team will call you back. The Future Laboratory: 26 Elder Street, London, E1 6BT, United Kingdom Phone +44 20 7791 2020 Fax +44 20 7791 2021

Introduction

Our connected world brings threats as well as opportunities. Criminals, saboteurs, hackers and thieves are increasingly adept at infiltrating the information technologies we rely on and adapting them to their own ends. The potential havoc this can wreak is unlimited. The solutions, it turns out, are in all of our hands.

1 Overview

Since the first public sites were made available on the world wide web and email began to become a mass communication medium, nearly two decades ago, cybercrime has been a problem for individuals, businesses and organisations. Now, cybercrime has changed.



Internet users in our multinational European survey who say they don't update their antivirus protection regularly, or don't have protection at all

'Technological progress is like an axe in the hands of a pathological criminal.'

Albert Einstein

And while there are actions that governments and the internet security industry can take to alleviate the threats it poses, experts agree that the real answers lie in changing the behaviour of consumers and computer users themselves.

Unless we take responsibility for the safety of our online transactions and the information we share over the internet, the ubiquitous technologies and intuitive interfaces that we will come to rely on in the future will become our greatest vulnerabilities.

Already, criminals are finding new ways to access our finances and data through the smartphones in our pockets – and consumers are worryingly unconcerned about this threat.

In addition, a minority of web users, unprotected against the global threat of cybercrime, threaten the 'herd immunity' of us all. According to our study, nearly 1 in 10 internet users across Europe are not protected against computer viruses and the malicious software – malware – that hackers across the world are constantly creating. Younger internet users are particularly susceptible to this laissez-faire attitude, creating a ticking time bomb for web users around the globe.

As we share increasing amounts of personal information online, and begin to adjust our notions of what privacy means, the rise of social networking is creating new opportunities for criminals as well.

Consumers across Europe fail to agree on whose responsibility it is to keep the internet, and our online information, safe. In our survey, only web users in Germany thought that individuals should shoulder more responsibility than internet service providers, brands and companies, the government or the police.

And, while some industry insiders predict the end of the internet, or the rise of a new breed of 'white-hat' hackers, experts agree that increased individual vigilance about cybercrime – in the home, on the move, in small businesses and in the boardroom – is the only way to combat this growing threat.

1.1 EXPERTS

Yuval Ben-Itzhak: CTO, AVG. A security industry veteran with more than 15 years of global IT security experience

Brian Honan: board member of the Cloud Security Alliance and adjunct lecturer in information security management at University College, Dublin

Sam Jardine: associate, Eversheds Technology, Media and Telecoms practice. Jardine is involved in the daily fight against cybercrime, and specialises in helping companies identify their legal position on reporting data breaches

Neira Jones: head of payment security, Barclaycard. Jones works in the B2B side of the payments business, and is passionate about educating businesses on their need to improve security – particularly around the mandatory Payment Card Industry Data Security Standards (PCI DSS)

Tony Neate: managing director, Get Safe Online. A former police officer, Neate is an expert in cybersecurity and was appointed by the UK government to head its education programme, Get Safe Online

Omri Sigelman: vice-president for marketing and products, AVG Mobilation, a pioneer in the field of mobile security solutions, providing both the tools and services needed to safeguard all Android devices

Professor John Walker: editorial board member of Cyber Security Research Institute. His work with government has ranged from helping the UK's DTI department set the ISO 27001 standards for cybersecurity to more covert work with the secret services at GCHQ and with the CIA

METHODOLOGY

This report by Future Poll, the research division of The Future Laboratory, was commissioned by AVG Technologies to investigate the future of cybercrime and responses to it.

A combination of quantitative and qualitative research and analysis underpins this report, spanning extensive desk and visual research, expert interviews to expand on key themes and a consumer survey.

The survey, conducted online in August 2011, polled the opinions of 7,000 respondents aged 18+ living in France, Germany, Italy, Poland, Russia, the UK and the Czech Republic. Unless otherwise stated, all statistics in this report refer to this survey, and should be credited thereafter as 'Future Poll for AVG Technologies, 2011'.

2 Cybercrime – reality, threat, future

The interconnectedness of the global economy has made us all more vulnerable to major global shocks.

The amount set aside by the UK government to tackle cybercrime

'The greatest trick the devil ever pulled was convincing the world he didn't exist.'

Christopher McQuarrie, The Usual Suspects (1995)

In the wake of the 2008 financial crisis, the Organisation for Economic Co-operation and Development (OECD) began a research project re-examining today's potential 'global shocks' – defined as major, rapid-onset events with severely disruptive consequences covering at least two continents, which begin locally and rapidly spread their impact, through contamination or contagion, to societies and economies. Alongside more familiar threats and disasters – financial crises, pandemics, geomagnetic storms and social unrest – the researchers included 'cyberrisks' for the first time.

The good news is that the OECD's conclusion was that 'very few single cyber-related events have the capacity to cause a global shock'.

That, however, is where the good news ends.

The OECD's report goes on to outline the significant and growing risks of 'localised misery and loss' as a result of computer and telecommunications services being compromised. This is the misery and loss experienced by anyone whose work or home computer has been compromised by a computer virus, or whose data has been stolen by a hacker.

We have come a long way since the dawn of the internet age, when the main threat to personal computers or business networks was from the cyber-equivalent of vandals and pranksters.

Hackers would use code to trick a computer user into downloading a file that would make something unwanted happen. These events ranged from the mildly embarrassing – pranksters who just wanted to fool computer users into emailing love notes to everyone on their contact list, or make a character or message flash up on their screen – to the far more serious: codes which would delete data and cause major damage to computer systems. Typically, these misguided programmers would put a moniker within the code, the way a graffiti artist tags their work.

The threats of previous years have, like viruses themselves, mutated into a far more sinister set of activities. Cybercrime, cybercriminals and their tools are increasingly diverse and sophisticated, with hackers adding spyware to their collective arsenal and vishing, SMiShing and pharming to their day-to-day activities.

CYBERCRIMES OF THE TIMES

Vishing – using features facilitated by Voice over Internet Protocol (VoIP) to gain access to personal and financial information, or to steal credit card numbers or other information used in identity-theft schemes

SMiShing or SMS phishing – a security attack in which the user is tricked into downloading a Trojan, virus or other malware onto their mobile phone or other mobile device

Pharming – a hacker redirects a website's traffic to another, bogus, website

Web users in the Czech Republic, Italy, France, Poland and Russia are more likely to update their antivirus software than they are to get a check-up with the dentist.

THE SPY WHO LOATHED ME

The biggest single change in how cybercriminals operate today is the emergence of spyware. Rather than disrupt a computer, spyware does not let the owner know they have been infected.

Spyware is aptly named. It will sit dormant on a hard drive, monitoring what a person does – or, more particularly, the password and username combinations they type in to access their bank account. Armed with this information, the spyware (often also referred to as a keystroke logger) sends back to a cybercriminal the credentials they need to access a bank account.

Even then, cybercriminals may progress subtly – logging on with fake credentials and diverting small amounts of money to another bank account – before eventually increasing the value of goods purchased through the bank account or diverting larger sums of money to their own accounts.

At the same time, the credentials will be used for ID theft, either by the criminal who placed the spyware on the machine or by a gang to whom he or she has sold on the relevant details. The gang can then open new credit cards and purchase more goods until finally the crime is noticed... and the next new victim's details are ready for use instead.

So while talk of global 'cybarmageddon' may be largely discounted by experts, the real threats of cybercrime to individuals are more local and more personal. Cybercrime now comes in all shapes and sizes – and unless consumers, businesses and governments take action now, it could, in our hyper-connected world, threaten the very fabric of our society.

2.0 FUTURE HACKING – FIVE SCENARIOS

In the near future, as ubiquitous computing technology pervades more of our lives, these threats will grow. The intuitive interfaces that we increasingly value – and depend on – could be threatened by a new wave of digital criminals. Left unchecked, unseen cybercriminals might be able take control of our cars, hack into our homes, control our power supplies and even open prison doors.

2.1 CAR-HACKING

Hackers could take control of your car's door locks, dashboard displays and even its brakes.

Our cars are becoming smarter. Today's cars already include at least 30 separate microprocessor-controlled devices – and some luxury models may have as many as 100 of these electronic control units, which unlock doors, start the ignition and control functions such as brakes and airbags. ABI Research predicts that the number of global users of automotive apps will rise from 1.4m in 2010 to 28m in 2015. Apps range from in-car receivers for internet radio stations such as Pandora to apps that help drivers check things such as tyre pressure.

Increasingly, onboard vehicle safety and security systems operate via mobile telephone and GPS networks. Some offer remote ignition blocking, to prevent stolen vehicles from starting. These technologies have already shown themselves to be vulnerable to hacking.

Last year, in Austin, Texas, more than 100 cars were rendered undriveable after a disgruntled employee hacked into a previously undisclosed black box that was hidden inside each vehicle by the dealership that sold the cars. The technology was designed to remotely disable vehicles if the car owners failed to make payments to the dealership on time.

Researchers at the US National Academy of Sciences Committee on Electronic Vehicle Controls and Unintended Acceleration have also managed to gain access to cars by breaking through authentication systems in their Bluetooth system, which allows a driver to make hands-free mobile phone calls. They also found that, when malicious code was embedded into a digital music file, a song played on the car's stereo could alter the firmware of the car's stereo system, giving attackers an entry point to change other components on the car – gaining control of its locks, dashboard and even its brakes.

2.2 JAILHOUSE ROCKED

Prisoners could be sprung from jail using only a USB stick.

The Stuxnet super-worm, used to sabotage centrifuges at a nuclear plant in Iran in 2009, is a form of malware that can be used to sabotage Supervisory Control And Data Acquisition (SCADA)-based industrial control systems, which manage the devices that control everything from water utilities to gas pipelines to power stations.

According ex-CIA security consultant John Strauchs, prison door systems could also have their vulnerabilities to exploitation by similar hacks. Strauchs recently worked with a hacker known only as Dora the Scada Explorer, to show how prison doors could potentially be opened on command.

Many correctional facilities use programmable logic controllers (PLCs) to manage their security systems and to control doors. Strauchs and his team were able purchase everything they needed to exploit PLCs for $2,500, and to write a program to expose vulnerabilities in just three hours.

Even more worryingly, Strauchs thinks it would be easy for a hacker to introduce malware into a prison through routes such as a staff member's Gmail account, or on an infected USB stick. 'A prison-security electronic system has many parts beyond door control – such as intercoms, lighting control, video surveillance, water and shower control and so forth,' say the researchers. 'Access to any part, such as a remote intercom station, might provide access to all parts.'

2.3 HEALTH SCARE

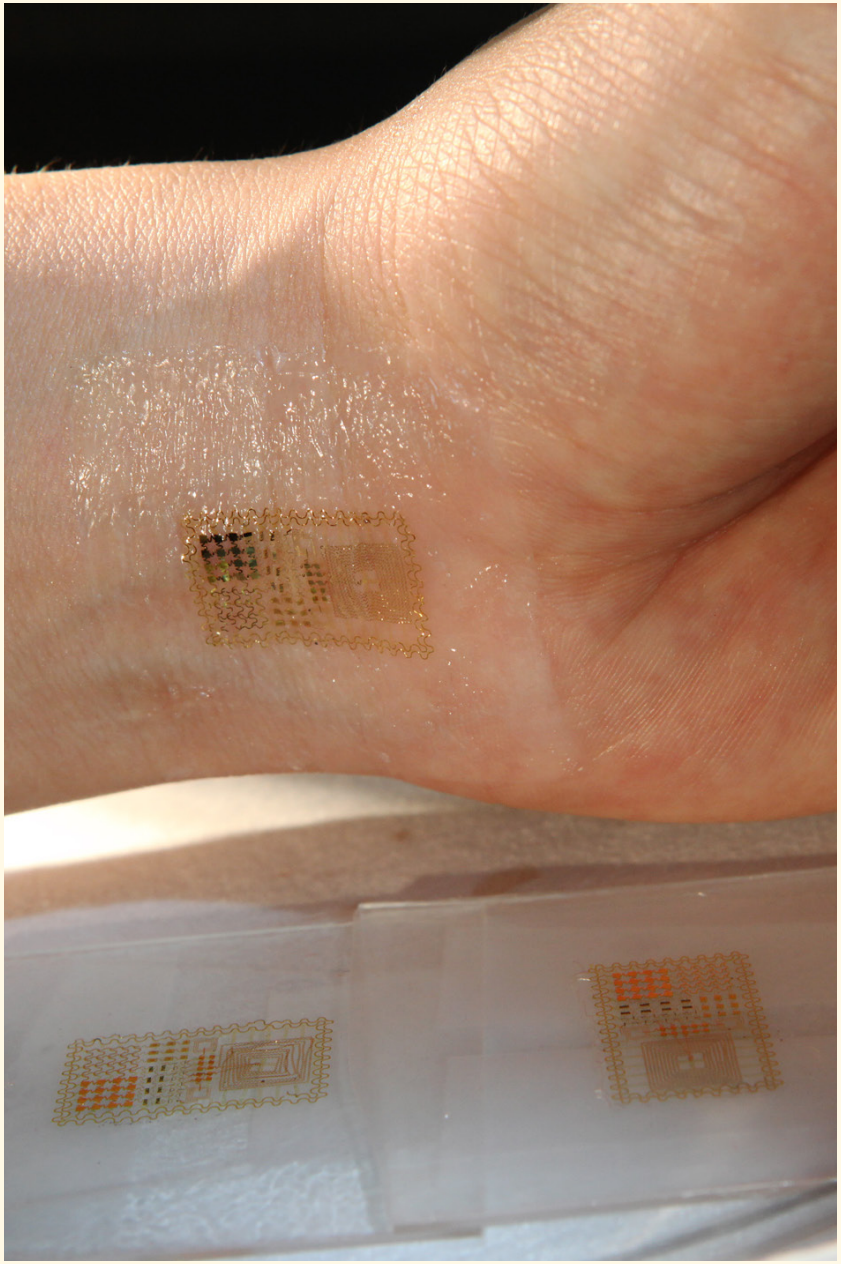
Saboteurs could threaten the wellness technologies we depend on to keep us healthy.

In the future we will use more day-to-day healthcare technology, such as in-home, and even in-body, equipment, for monitoring patients' vital signs and accessing care via mobile telemedicine. Wireless technologies incorporated into medical products will mean that many products that are now tethered to patients, positioned next to hospital beds, or located at nurses' stations, will be transportable.

mHealth and eHealth systems are already using mobile devices to collect vital clinical health data. At present there are more than 40m Bluetooth-enabled health and medical devices in circulation, according to the Bluetooth Special Interest Group, which has just agreed standards for Bluetooth-capable thermometers and heart-rate management products.

To demonstrate the inherent vulnerabilities of these devices, security expert and diabetic Jerome Radcliffe has already hacked into the wireless insulin pump he wears on his body round-the-clock to keep his blood-sugar level stable. He has suggested scenarios in which untraceable attacks could be launched against wireless insulin pumps, pacemakers and implanted defibrillators from a distance of half a mile.

The threat is such that researchers at Massachusetts Institute of Technology (MIT) and the University of Massachusetts have already begun to develop an anti-hacking jamming device that addresses communication security in implantable medical devices, to protect people from the threats of passive eavesdropping or from active attacks which could reprogram medical devices. The wearable shield device can emit a jamming signal when an attacker establishes an unauthorised wireless link between a pacemaker and a remote terminal.



The new era of health monitoring technologies is typified by the Epidermal Electric System created by researchers at the University of Illinois. This ultra-thin, self-adhesive electronic device can effectively measure data about the human heart, brain waves and muscle activity. Photography by John A. Rogers

2.4 SNIFFERS AND BLACKOUTS

Burglars could monitor your activities then reprogram your home security systems from afar.

Forget lurking in the bushes outside your house, checking if your car is there or if a window is left open. Tomorrow's thieves will monitor houses remotely. They will be able to determine when its occupants are generally gone, based on signals indicating when lights are turned off and the alarm system is enabled. Then they will send out jamming signals from the tool, to disable motion sensors and alarms before breaking into the house. Afterwards, they could even start a house fire by overloading the system with commands.

Home automation and security systems that operate through power lines to enable users to control a multitude of devices such as lights, electronic locks, heating and air conditioning systems, and security alarms and cameras, are also vulnerable.

Independent security researchers have already demonstrated tools designed to hack home and business automation and security systems that operate on ethernet networks, or which communicate over the existing power lines in a house.

Criminals can connect a 'sniffer' device to the broadband power network through an electrical outlet, and 'sniff' the signals to gather intelligence about what is going on in a building. This includes monitoring the movements of people in houses with motion-sensor security systems. They can also send commands through the network, to control devices that are connected to it – for example, to turn lights on or off, or to disable alarms and security cameras.

And house-hackers are going mobile. Security researchers are working on a GSM-enabled tool that would allow attackers to receive sniffed data to their mobile phones (at present it is written to external storage) as well as to send commands back to the tool via text messaging.

2.5 GRID-JACKING

Scammers and terrorists alike could find opportunities in hacking into the Smart Grid.

Smart meters will help us manage energy more efficiently in the near future, by providing an intelligent flow of information between our homes and our power suppliers. They are what will enable us to make better use of intermittent energy sources such as wind and solar power.

If left unprotected, however, Smart Grid technologies could open up a new front for fraudsters, hacker groups intent on stealing individual data or even terrorists bent on destabilising whole economies. Consumers could tick their meters backwards, or bypass them entirely, to lower their electricity bills. Hackers could detect when residents are at home or away, and data on home-appliance usage could be shared unknowingly with marketers.

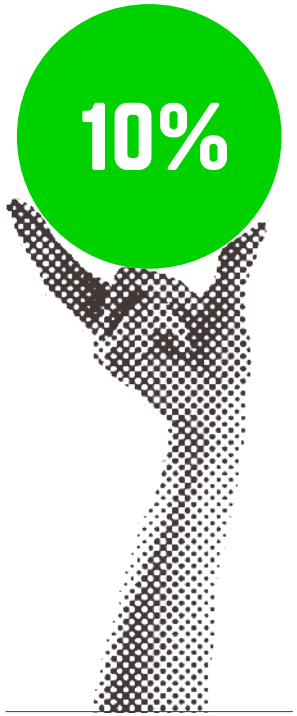
In a worst-case scenario, cyberterrorists hacking into transmission networks could cripple large areas of a country by remotely coordinating electricity overloads to blow up transformers and power equipment.

Smart Grid security is already big business. A key element of the Smart Grid will be the rise in our use of electric vehicles. Vehicle-to-grid technology will enable utility providers to let electricity flow from power lines to car batteries and, importantly, back again – enabling electric vehicle owners to sell unused power back to utility companies. Market intelligence firm Pike Research claims that $432m (£268m, €305m) will be invested in cyber-security innovations for electric cars between 2011 and 2015 – and that, by 2015, the electric vehicle cyber-security market, now valued at $26m (£16m, €18m), will grow to $144m (£90m, €102m) annually.

3 Smartphones – the PCs in your pocket

Our cars, homes and utilities may be vulnerable to cybercrime in the near future, but there is a bigger threat, that many of us are already carrying around all day, every day.

Square reader by Square. As mobile payment systems grow in popularity, industry standard encryption and security systems will have to keep up



Only 10% of web users in the Czech Republic, 13% in Russia and 14% in the UK are concerned about viruses on their smartphone or tablet computer.

Experts call it a cybercrime perfect storm. The rise of spyware, which enables criminals to plunder bank accounts and steal identities undetected, has come at the same time as the smartphone has become the new must-have mass-market device.

Smartphones have computing power and onboard memory that enable owners to perform many functions, such as mobile banking. But their very smartness makes for simple means by which criminals can steal an individual's money.

Criminals can not only gain access to bank account details, they can take money through a far more subtle route: premium SMS. Some text numbers have been designed to allow owners to pay for goods worth several euros, such as music downloads and subscriptions to websites. Cybercriminals are becoming increasingly adept at infecting smartphones with malware that sends out premium SMS messages, from which they can net several euros for every message. Given that few people check their bills closely, the scam can carry on undetected for some time.

Perhaps the most alarming part is that, despite malware's ability to work in the background sending out premium text messages, the public seem not to even know of the potential for their personal mobile phone to commit crime affecting them. Or, if they do, they show no fear of it.

Just 4% of French internet and smartphone users, for example, are concerned about smartphone viruses, compared with more than 1 in 5 (22%) who are concerned about online viruses.

Recent phone-hacking scandals have brought the issue of mobile phone security into the public eye, but the idea of someone listening in to your voicemail will soon seem the least-worrying aspect of mobile-phone security.

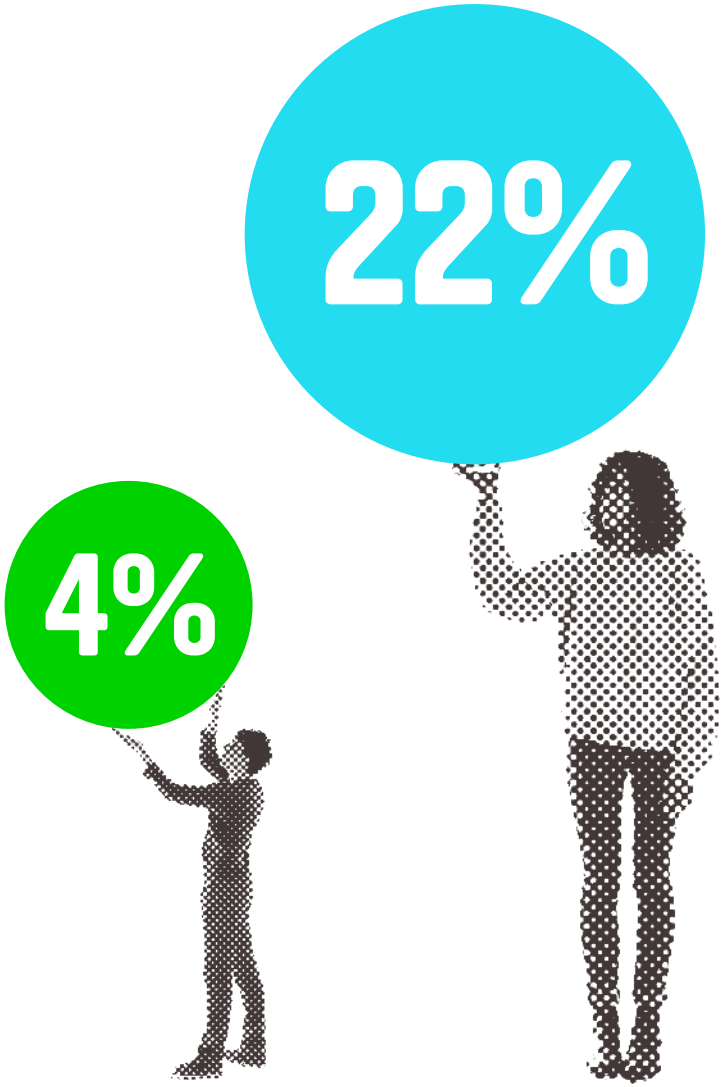
Hackers can gain access to a phone's information by setting up a free wifi hotspot in a public place, or by tricking a user into clicking on an unsecured link that contains malicious code. This would give the hacker a backdoor entry into a phone and all the information on it – including emails and bank details – even if the phone looked as though it was on standby. The code can also be used to record all conversations conducted on a phone – including those where a bank's security questions are answered – or to take photos of a person and their home without them knowing.

The growth of mobile and digital payments further highlights vulnerabilities within the smartphone system.

Near-field communication (NFC) is the technology that will enable users to send information quickly to electronic readers by simply tapping their phones against them. This will turn mobile phones into one-touch payment devices. PayPal's president, Scott Thompson, has already predicted that wallets will be a thing of the past by 2015. PayPal's users now complete up to $10m (£6m, €7m) in transactions each day, and the company is hoping to process $7.5bn (£4.7bn, €5.3bn) in payments through mobile apps by the end of 2011. Market research firm Infonetics predicts that sales of mobile security software will grow by 50% each year to 2014, when they will reach $2bn (£1.2bn, €1.4bn).

Omri Sigelman, vice-president for marketing and products at AVG Mobilation, believes that the true problem lies in people not realising that their smartphones are far more than simply phones. With more computing power than some laptops had only a few years ago, the modern smartphone presents an open target for cybercriminals.

'People still see their smartphone as a phone, so we have a real problem now in that hackers have moved from sabotage to monetising their malware,' he says. 'The problem with a smartphone is that people run their lives through it, and it is connected to everyone you know. There are so many threat vectors, such as SMS, MMS, GPS, email, web browsing and instant messenger – all on one small device that is always connected.'



Just 4% of French internet and smartphone users are concerned about smartphone viruses. More than 1 in 5 (22%) are concerned about online viruses.

PalmSecure by Fujitsu

FUTURE SCENARIO – BIOMETRIC MUGGING

Walletless systems could hand control of your entire life to cybercriminals

Beyond the use of mobile phones as wallets, we'll see payment systems develop in which we need carry no hardware at all. We'll identify ourselves, or pay for goods, by simply waving a hand in front of a detector.

Security systems such as passport control already use biometric identifiers such as fingerprints and irises. Other unique identifiers are our voices, our faces or even the shape of our earlobes.

Fujitsu's PalmSecure system, already used in one Florida school district to enable students to make purchases in its cafeterias, identifies people from the unique pattern of veins in their hands. It shines a near-infrared light onto the hand, then stores the pattern of veins as a unique identifier. It can work as a second authentication factor for existing payment systems – potentially virtually eliminating credit card fraud in stores.

But security experts say that the systems that would link these technologies to our bank accounts or credit cards are still vulnerable to cybercrime. Database security becomes even more important. If back-office systems are hacked, and scanners no longer recognise their biometric data, consumers run the risk of having all access to their finances removed in one go.

4

Wetware: you are the weakest link

Today, the biggest threat to a computer owner's online security is the computer owner him or herself. By not keeping antivirus software up to date, or by sharing too much personal information online, consumers are becoming passive participants in a wide range of cybercrimes.

More than eight in 10 (82%) of computer owners in the Czech Republic, 22% in Poland and one in five in Russia say that they do not update their antivirus software regularly.

THE DEADLY 9%

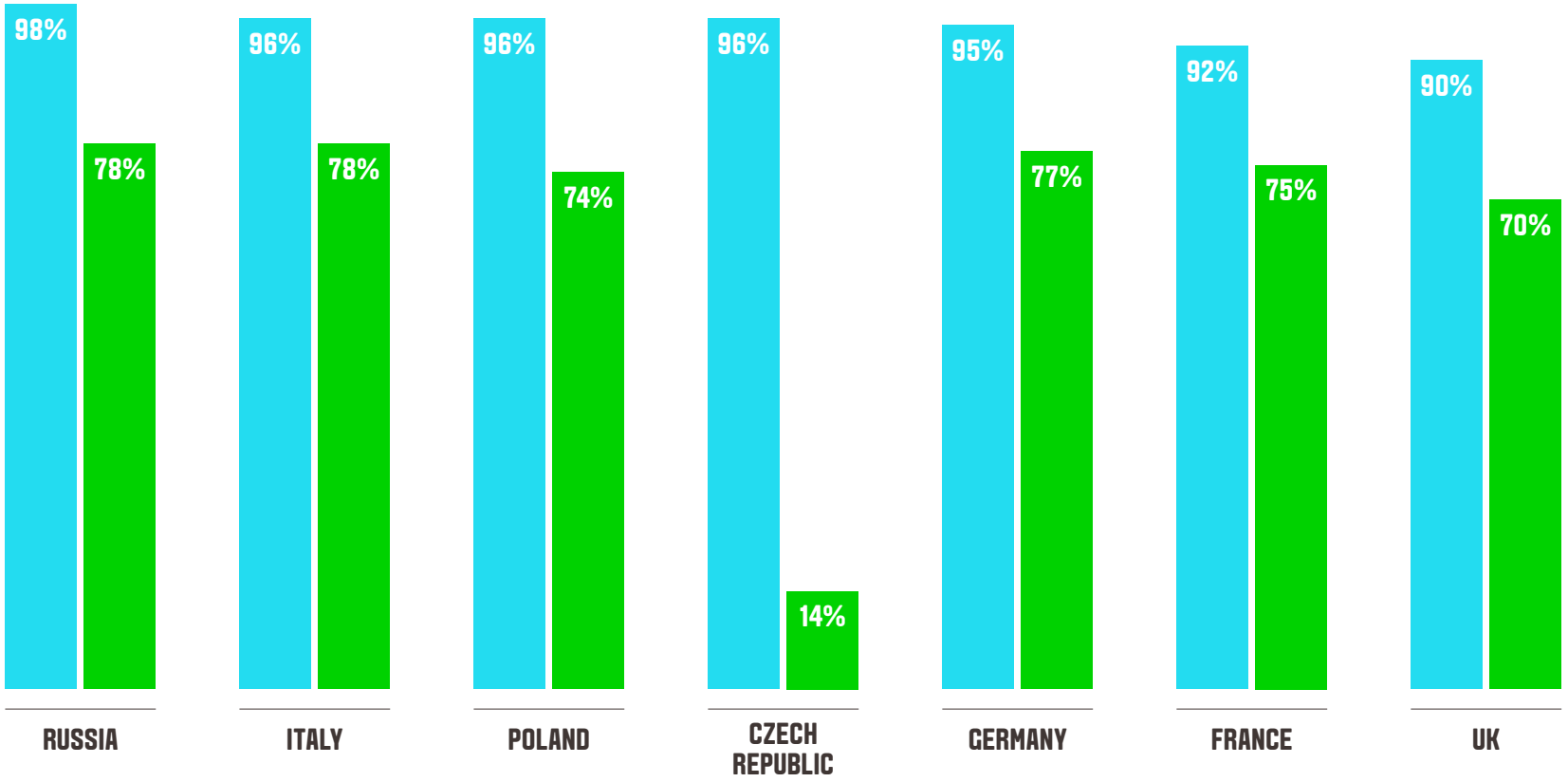
The biggest threat in the future of cybercrime is not the increasing sophistication of cybercriminals. Computer hardware and software will only stay safe if people – or wetware – develop the habits and behaviour needed to maintain protection. Today, the weakest link in the chain of computer security is computer owners themselves.

Our survey shows that, across Europe, internet users are aware of the need for security and antivirus products – and indeed most of them own them.

Among internet users across Europe, fears about a personal computer being infected by malware ranks consistently alongside fears about physical property crimes such as mugging and burglary.

In fact, in Russia, France, the UK and Germany, people are more worried about computer viruses than they are about being mugged.

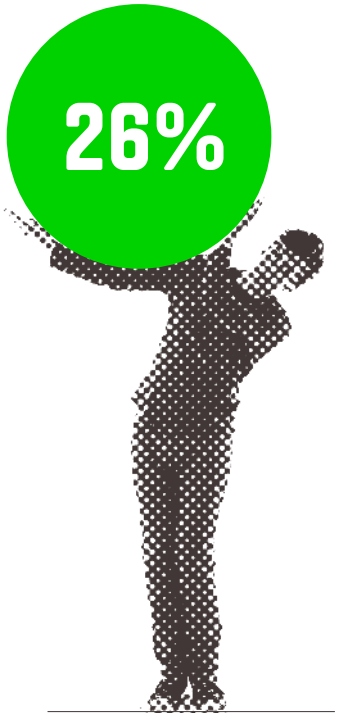
But a significant proportion of these consumers admit that they do not keep their protection up to date. This means that 9% – nearly one in 10 – of internet users in our European survey are not protected against online threats



Web users in our European survey who have anti-virus protection

Key

- Have antivirus protection
- Update it regularly



Only 26% of internet users in the Czech Republic, and 38% of UK internet users, have updated their antivirus software in the past six months

THE IGNORANCE OF YOUTH

In every developed country, there is a whole generation who cannot remember the world before the internet. For these digital natives, or Generation D, born between 1994 and 2002, the use of technology is an inherent, not a learned, part of life. There are 1.2bn 5–14-year-olds in the world, according to data from Euromonitor International – 20% of the US population, 18% of the UK and France, and 13% of Germany is under 14.

Then there are the New Millennials, born between 1982 and 1991, who have grown up with mobile phones and social networking, and live their lives in public in a way that would astonish their grandparents. Across Europe, New Millennials account for 11% of the workforce. Worldwide, there are more New Millennials (2.3bn) than Baby Boomers (1.4bn).

It would be easy to assume that the generations who are growing up with computers, websites and smartphones are the ones most used to considering internet security, the threat of hacking and the need to protect against identity theft.

In fact, the younger age groups in our survey are frequently less likely to proactively protect themselves. In the UK, for example, 70% of internet users update their antivirus software. Among those aged 55 and over this rises to 80%, and for 35–54-year-olds it is 77%. But only just over half of the UK's 18–34-year-olds (51%) keep their antivirus software updated.

In France, where 84% of silver surfers (aged 55+) protect their computers, only 70% of 18–34-year-olds do so. In Germany, 68% of 18–34-year-olds update their software regularly, compared with 82% of 35–54-year-olds and the same proportion of the over-55s.

As these younger generations enter the workforce, this has the potential to be a ticking time bomb for internet security.

FAMILIARITY BREEDS CONTEMPT

Increasing familiarity with digital technology, then, does not necessarily equate with increasing awareness of digital risk. For businesses and individuals, this is a demographic time bomb that threatens to compromise the herd immunity of the online community.

Herd immunity originates as a concept that describes biological infection. Disease relies on critical mass to spread. If a population is dominated by people who are immune to infection, it helps curtail communication of the disease. In the online world, this means that, as long as the vast majority of machines with which an individual computer is in contact are not susceptible to the same malware, infection is less likely. If a computer communicates mostly with machines that are susceptible, herd immunity is lost.

At a point at which cybercrime is becoming harder to detect, younger people are less likely to keep their computers protected. As they are more prolific users of the internet than older generations this constitutes an inherent threat for all internet users. In a recent Ofcom report in the UK, 83% of 16–24-year-olds said that they used the internet regularly via a computer or laptop, compared with 13% of those aged 75 and over. Adding smartphones into the mix only increases the threat. Nearly half of UK teenagers (47%) own a smartphone, says Ofcom, and 16–24-year-olds in the UK are more than 10 times more likely to go online via a mobile than those aged 55 and over.

What is behind this seemingly cavalier attitude to internet security? Tony Anscombe, ambassador for free products at AVG, suggests that younger internet users are less likely to place a value on their virtual, or actual, possessions. ‘Think back to when you were young. You probably didn’t think about someone breaking in to your bank account, because you were too busy doing other things – and you didn’t really have anything in the account in the first place.’

Yet there are signs that, for some age groups, there is some awareness, at least, of the inherent risks in online activity. In a survey by JWT, consumers in the UK and US aged 20–33 had the greatest appetite for social commerce – more than four in 10 (43%) said that they wished there were more opportunities to shop on Facebook. But they were also more likely than other age groups to be wary of the related security implications. Almost eight in 10 (79%) of that age group say that they don’t think Facebook is secure enough to make purchases, and 81% worry about the privacy implications of shopping on Facebook.

Governments and internet security firms will need to exploit this wariness if they are to persuade younger internet users to develop better habits and so ensure the safety of their connected devices.

Groups of consumers leave themselves susceptible to hackers, viruses and identity thieves because of a series of common myths, says to Tony Anscombe, ambassador for free products at AVG.

THE VIRUS DENIERS

Invincibles

Some computer users believe they are invincible. ‘There is a very worrying attitude among users of other platforms that viruses only affect PCs. PCs are a far bigger part of the market and so are therefore affected more, but as recent attacks have shown, others can and do become infected with malware. It is surprising how entrenched this view is, though, particularly among students when I give talks at universities and colleges.’

Clean-livers

Dodgy sites are where malware hides. ‘So many people believe that it is only by viewing porn that they will become infected by malware. They do not realise that any site that has been the target of cybercriminals could have malware on it. And cybercriminals are very clever. They might only put a small part of their rogue code on one site, which may be downloaded unwittingly and not raise the alarm. The code will then secretly download the rest of the malware from another site.’

Trial-anders

Free trials finish, but users think they are still protected. ‘Too many people get a free trial of antivirus software with their new computer, and then think it doesn’t matter that it has run out. They think they’re protected because the program icon is still there. Or they are put off by some vendors charging a lot of money to continue once a free trial is over. The low cost of PCs today also makes the cost of security protection seem comparatively high.’

'People are incredibly trusting when somebody befriends them online.'

Tony Neate, managing director, Get Safe Online

SOCIAL NETWORKING = SOCIAL ENGINEERING

If the weakest link in the internet security chain is the person in front of the computer, security experts are now warning that the rise of social networks is leading to a rise in social engineering.

It was hacker-turned-consultant Kevin Mitnick, author of Ghost in the Wires: My Adventures as the World's Most Wanted Hacker, who popularised the term 'social engineering' when related to cybercrime. It is now the term the internet security industry uses for the art of manipulating people into divulging confidential information, or tricking them into performing actions that lead to them being defrauded.

Experts say that there are parallels here with the automotive industry. For years, opportunist and expert thieves were able to break in to vehicles – and they continued to do so right up to the point when locks were improved and alarms and immobilisers were fitted as standard. To steal a modern car, a thief has to physically get hold of the keys. In the UK, Home Office figures for 2010 show that keys were used in 85% of car thefts in which the method of theft was known. Of these, 37% came from burglaries, and 18% from the owner leaving the keys in the car. Similarly, with computer systems now capable of being comprehensively protected, the easiest way to get into a home or business computer is now through its owner.

So, while recipients routinely laugh at emails from West African strangers offering billions of dollars in return for a consumer's bank details, cybercriminals have moved on to far subtler ways of influencing people to hand over confidential information or money. Confidence tricksters on dating sites and social media services who ask for money soon after befriending someone are the most obvious. More subtly, there are people whose profiles seem so convincing that they can easily worm their way into a consumer's online circle of friends – and then glean valuable information about their lives.

Even security experts are vulnerable to social engineering. When researcher Thomas Ryan created a social network profile for a fictional young female cyber-threat analyst in the US Navy, 'Robin Sage' managed to connect with 226 Facebook friends, 204 Twitter followers and 206 contacts on LinkedIn – many of them in the security, military and intelligence fields.

Tony Neate, managing director of Get Safe Online, believes that many people are unaware of the risks they face through social networks.

'People are incredibly trusting, and when somebody befriends them online they can easily believe they know the person through someone else, or that they met through work,' he says. 'The trouble is, that gives them access to all your posts and information about yourself, such as your birthday and, perhaps through your contacts, your mother's maiden name. And those are two of the first questions any bank will ask as security questions.'

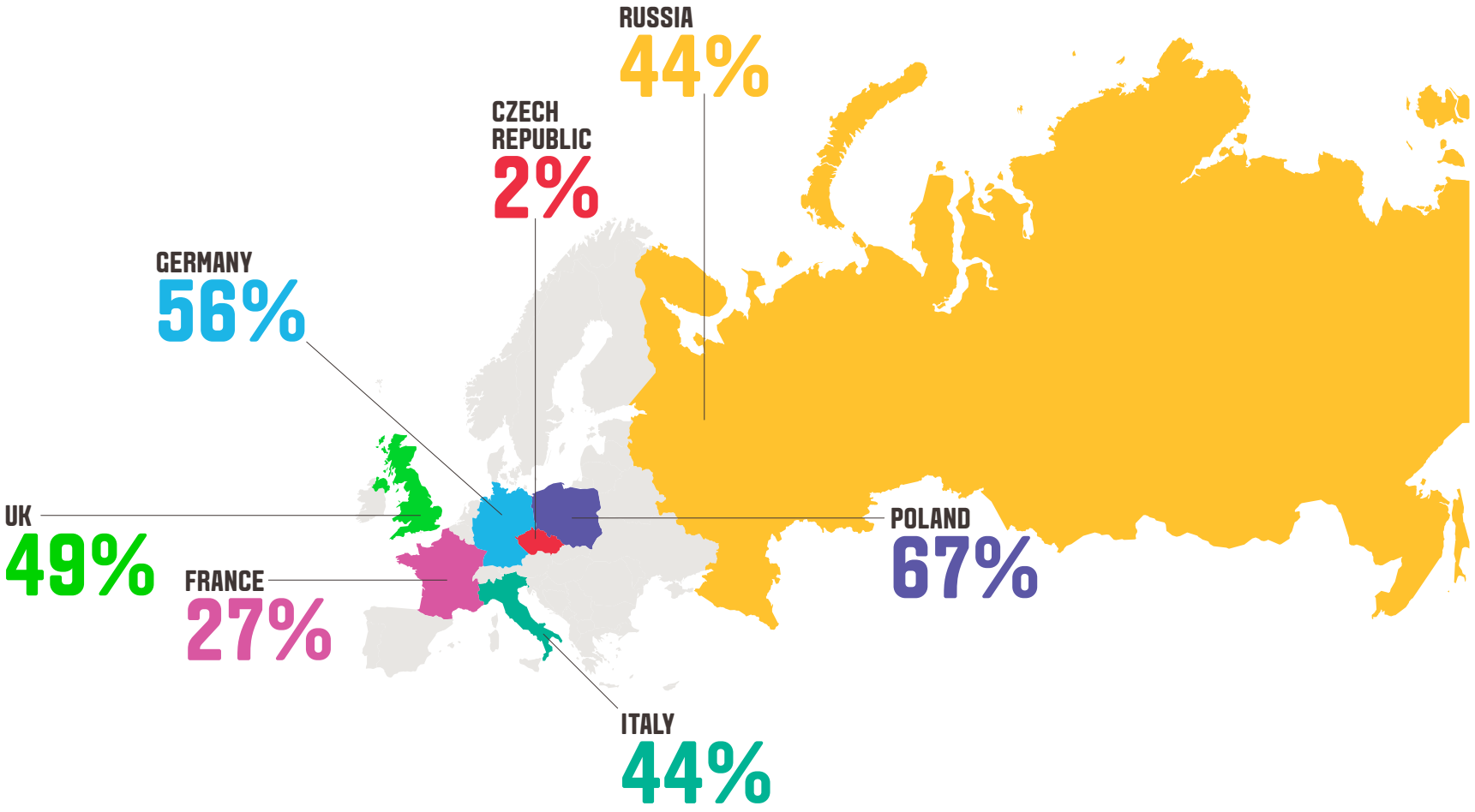
Our survey found that some groups of consumers admitted to being concerned about their computer being infected with viruses, but didn't show the same level of concern about identity theft, which costs the UK £2.7bn ($4.3bn, €3bn) a year, according to the National Fraud Authority. More than one in five (22%) of French internet users, for example, are concerned about computer viruses, but only 4% are worried about ID theft.

FUTURE POLL

5

Responsibility 2.0

Consumers are divided about who is ultimately responsible for internet safety. Who will take responsibility, as the World Wide Web turns into the Internet of Things?



Do you think it is down to individuals to take responsibility for the safety of the internet?

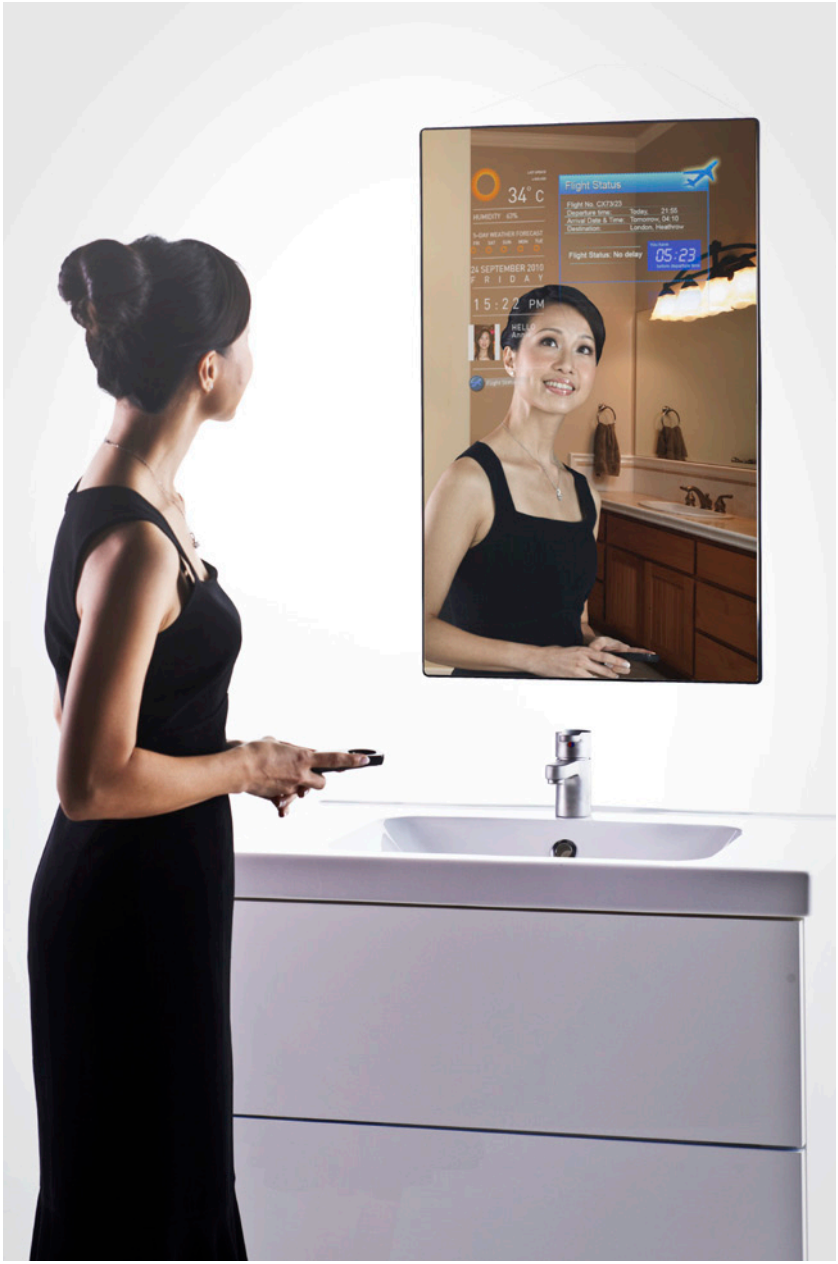
Who do European web users think should be responsible for ensuring the security of the internet and the safety of personal data? In our survey across seven countries, only web users in Germany thought that individuals should take more responsibility than ISPs, brands or website owners.

- Only 27% of French internet users think that they should take personal responsibility for their safety online. Nearly twice as many (52%) believe that it is down to ISPs.
- Almost seven in 10 (69%) of Russian web users, and 75% of Polish web users, think that online brands and web services should be responsible for online safety.
- Nearly six in 10 (59%) of Italians believe that the police should be responsible for online safety.
- German web users were a rare exception, prioritising their own responsibility (56%) against those of ISPs (49%) and site owners (52%).
- Just 2% of web users in the Czech Republic think that it is down to individuals to keep the internet safe.

Consumers are already divided on the subject of who should take responsibility for policing and protecting the web. How will responsibility be managed, as we move seamlessly into a world in which what was once termed the Information Superhighway becomes the Internet of Things? As advances in wireless networking technology, the standardisation of communication protocols and ever-smaller-and-cheaper silicon chips enable sensors to be embedded in objects, and those objects become linkable wirelessly, we may be looking at what David Wall, professor of criminology at Durham University, has called ‘a fourth generation of cybercrime’. AVG Mobilation’s Sigelman warns that ‘with the rise of the smartphone, we’re just at the start of this new wave of connected devices’.

When objects can sense their environment, react to it and communicate with each other, there will, alongside the benefits for consumers and businesses, be innumerable risks. ‘If devices are connected but not protected, there will be all kinds of terrible things cybercriminals could do,’ says Sigelman.

For Yuval Ben-Itzhak, CTO at AVG, this future is just one reason why it is so important for individuals and businesses to report cybercrime to the police – so authorities can no longer claim not to know the depth and breadth of suffering caused by these activities across Europe.



Cybertecture Mirror by James Law Cybertecture International. This smart device brings digital ubiquity to the home. Seamlessly connecting to a cloud-based digital profile, it delivers current information such as weather forecasts, traffic information and personal health readouts

‘When people have a car accident, they have to report it to the police. It needs to be the same for cybercrime,’ he says. ‘The problem is that people don’t have any idea who to report cybercrime to. They normally phone up their bank to remedy any financial loss, but the police will never hear about the crime. If everyone reported cybercrime, then police forces and governments would have a clearer picture of the scale of the problem, and they would have to do something. Unless it is hammered home to them how rife cybercrime is, nothing will be done.’

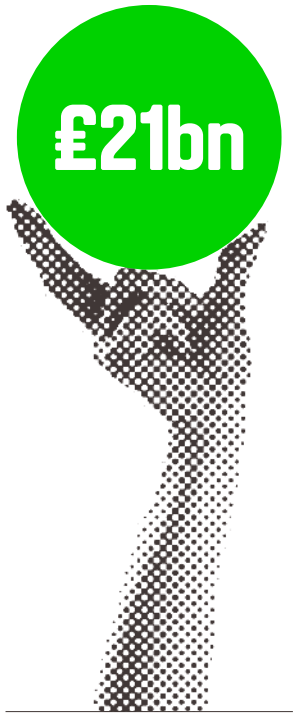
At the same time, Ben-Itzhak believes that some of the responsibility for tackling and preventing cybercrime lies with ISPs. ‘Governments and the police have the problem that, although they can pursue criminals, a lot of the time they cannot act across borders at speed,’ he says. ‘That makes it even more important for the ISPs and hosting companies to stop closing their eyes and act to shut down or block cybercriminals at source. Police forces can talk about tackling criminals, and governments can talk about harsher punishments for cybercrime, but this is largely irrelevant, as the criminals know they are unlikely to be caught and brought to justice. If ISPs acted, they could seriously reduce cybercrime. They are the internet. They can make the difference.’

A new network of international cooperation, new models of business responsibility and consumer education and incentives will structure our responses to cybercrime in the coming decade.

6 A new climate of risk

How will businesses and governments need to react to ensure consumers' safety in a hyper-connected future?

Conference Hall at The Bahnhof Internet Service Provider's Pionen Data Centre, Stockholm, Sweden. This fortified nuclear-proof bunker housed the infamous WikiLeaks files



Cybercrime in the UK is estimated to cost businesses £21bn, consumers £3.1bn and the government £2.2bn a year, according to the UK Cabinet Office

For businesses, experts warn that the stakes are far higher than many firms realise. Brian Honan, a lecturer in cybersecurity and a board member of the Cloud Security Alliance, maintains that if governments fail to rise to the challenge set by cybercrime, the worst-case scenario is that the internet as we know it will no longer be fit for purpose.

'If the problem of cybercrime is not resolved, it could lead to an erosion of consumer and business confidence about conducting commercial transactions online,' he says. 'If the cost of dealing with cybercrime is too great – if investing in technologies to protect systems, or an individual exposing their financial and personal details is too high a price to pay – then these parties will simply stop using the internet for such transactions. The internet will then cease to be a platform for e-commerce or other sensitive transactions.'

Others are less quick to predict the end of the net, but maintain that multiple and sophisticated responses are the only way to combat the increasing diversity of cybercrime.

An increasingly networked world, for example, demands new jurisdictions and protocols for law enforcement.

Cybercrime is the ultimate global industry. Hackers, and the criminal gangs that employ them, work across national borders, so cybercriminals and their victims are hardly ever in the same country, explains Sam Jardine, associate at Eversheds' Technology, Media and Telecoms practice. 'There is no international legislation to help find and bring criminals to justice. Even what would seem a very simple question – where a person should stand trial – is not always clear. Is it where they committed the act, or where the victim was located?'

Jardine is unimpressed by international efforts to tackle this issue so far. 'There is a draft EU law in the making, and Washington has produced a policy paper, but to date all we have had are conventions where people in the business talk about the issues. What is needed is a treaty to handle cybercrime. But it has to be a treaty with teeth – one through which law enforcement agencies can cooperate and bring cybercriminals to justice, either in their own country or in the victim's country.'

Honan agrees. 'The biggest challenge for governments is information-sharing, to allow for better cooperation, both nationally and internationally, in dealing with the threat. This includes sharing intelligence on criminal gangs: how they operate, their techniques and how to bring them to justice. It also includes cooperating with the private sector to share details of threats, defensive strategies and alerts about potential attacks.'

Businesses, on the other hand, need to acknowledge the new climate of risk. Not least, warns Neira Jones, head of payment security at Barclaycard, because security issues have an impact on that most precious of commodities – consumer trust.

'Corporations need to move information security to the boardroom and deal with it as an issue of corporate governance, which is a language that top executives understand. This is not only a technology issue. If you suffer a security breach, customers will desert you – and they will tell everyone on their enlarged list of social media contacts all about it, too.'

'There is no international legislation to help find and bring criminals to justice. What is needed is a treaty to handle cybercrime. But it has to be a treaty with teeth.'

Sam Jardine, associate, Eversheds

Corporates should be reminded that only a tiny percentage of hacker attacks are sophisticated, says Jones. 'By far the majority of attacks, including the recent Sony breach, are SQL injections. These have been well known about for more than a decade, and remedies are widely available. The next-most-common are hacks that rely on people not changing the default passwords that come from vendors, or on people not replacing these with strong passwords. These make it so easy for cybercriminals to get in to systems. Simply using better password management, and deploying widely available protection against SQL injections, would protect companies from the vast majority of attacks. It is sad that so many companies don't do this.'

Smaller businesses, she adds, 'need help with education, because they do not always realise the implications of not having security software, or of not keeping it up to date'. Robert Gorby, global head of SMB marketing at AVG, believes that this is largely because smaller businesses just hope for the best.

'Most small and medium businesses don't have an IT manager, and they're just so busy running the company that they don't install or update internet security software,' he says. 'They often think that just enabling automatic patch updates to their operating system and software is protecting them, but that still leaves them very vulnerable. If a cybercriminal gets into their network, they could be put out of business. They could lose data they could never get back again, they might have their bank accounts emptied, and the loss of reputation if any client information is compromised is just irrecoverable.'

He adds that the internet security industry needs to better understand the behaviour of small business customers. 'Businesses need software that can update in the background and not interrupt a company's work day, and they need easy-to-use tools designed specifically for SMBs. Sometimes, people get fed up with updates because they slow down the network to a point where the business has to stop for a while. Many products are also far too complex. They're cut-down versions of enterprise systems that are just too clunky and hard to configure.'

In addition, the rise of consumerisation – where employees bring devices from home into the workplace and connect them to workplace systems – brings new risks.

'A business can think it is doing well by keeping an internet security product updated and running properly, but then it opens itself up to the risk of third-party devices connecting to its network from within its offices,' says Gorby.

Already, around 72% of firms surveyed by Aberdeen Group say that they allow employees to use their own smartphones or tablets for work, four times as many as at the end of 2008. And Colgate-Palmolive, which launched a Bring Your Own Device program earlier this year, estimates that it will save $1m a year in licence fees for the 524 employees who have signed up to use personal BlackBerrys at work.

'It is a massive new threat vector that many people haven't thought about when they encouraged smartphone use in and out of the office. At the very least, companies need to insist that all staff have passwords to lock their devices, so a thief cannot easily access them. Yet few do. And they need to ensure that the devices being connected to the network are protected by internet security software.'

'There is, in the end, no forced entry in cyberspace. Whoever gets in enters through pathways produced by the system itself.'

Martin Libicki, senior management scientist, RAND Corporation

FROM PATCHES TO NUDGES

Ultimately, a more connected world demands a new way of thinking about ways to encourage business and individual take-up of threat protection. Governments, the financial sector and the internet security industry will all need to consider how to incentivise safe internet practice.

For some, this is about emphasising a balance of economic incentives. If the net result of cybercrime is the theft of money from a bank account, or a copied ID that is used to buy products online, it is usually banks and credit card companies that foot the bill. Where is the financial incentive for the ordinary consumer to take internet security seriously?

AVG's Gorby predicts that this is set to change. Just as drivers are not covered by insurance if they leave keys in the ignition of an unattended vehicle, businesses will start to be expected to take more responsibility for their own security. 'In the US, the PATCO Construction Company failed in the courts to force Ocean Bank to cover its losses, because a judge reasonably decided that it hadn't protected itself against SpyEye malware,' he says. Patco ultimately lost $345,000 after $589,000 was siphoned out of its bank account. 'In fact, it was the bank that had alerted the company to the theft. We think this is a landmark case, because it's the start of the banks turning round to companies and saying that if they don't protect themselves, they can't expect banks to pick up the bill.'

Governments, meanwhile, have a tripartite responsibility. They have to protect national security from potentially state-sponsored hackers, and they need to protect many millions of private citizen records held on local and national government databases. In addition, they have a responsibility to help educate the public, argues professor John Walker, who sits on the ISACA Advisory Group and is an editorial board member of the Cyber Security Research Institute.

Walker's work with the UK government has ranged from publicly helping departments to set standards for cybersecurity, to more covert work with GCHQ and the CIA. This experience has taught him two things: that governments need to educate consumers, and also to ensure that they are well-informed. 'People understand that they need to keep their car roadworthy and not to drink and drive. We need governments to run similar public campaigns to hammer home the importance of cybersecurity,' he says. 'Government departments themselves also need to become much better at their own security. Many of the conversations I have had with high-ranking officials in charge of department security have left me surprised that the people in charge don't know as much as they should.'

Other experts conclude that nudge policies proposed by Richard Thaler and Cass Sunstein can help governments, users and businesses to do the right thing.

'We have to consider the possibility that some users might be aware of the risks of cybercrime and have calculated that they are not worth the effort to combat,' says Tony Anscombe from AVG. 'Take the premium SMS example. Many phone users would probably say they would rather have a faster phone and lose €1 a month than slow it down with an antivirus product or go to the hassle of sorting out the problem. Similarly, this could be true of some laptop and computer users – they would rather take the minimal risk of losing a small amount of money than spend the whole time with a perceptively slow computer.'

Using Thaler's ideas of choice architecture, the internet security industry would invest more in understanding consumer behaviour, and consumers could be helped to make the right choices at the right times.

This is why the future of cybersecurity could ultimately lie in the hands of an anonymous teenager in a back bedroom in some European suburb. Journalist Misha Glenny, author of Dark Market: Cyber Thieves, Cyber Cops and You, writing in the Financial Times, offers a solution.

'Most hackers develop their skills while in their early teens. It is time to seek them out, by identifying them while they are still at school while still allowing them to experiment and absorb hacker culture, and then recruiting them. Sifting our classrooms for the hackers of tomorrow sounds a little drastic, but this is the norm in emerging cyberpowers such as Russia, China and Israel. And whether we like it or not, we are competing with them. We need not resort to the blackmail and bribery of authoritarian states. Instead, our governments can offer positive incentives, so this new generation of digital natives – many of whom will, in any event, develop advanced hacking skills – can put their unusual abilities to good use.'

ANTIVIRUS PROTECTION ACROSS ALL COUNTRIES IN OUR MULTINATIONAL EUROPEAN SURVEY

67% have antivirus protection and update it regularly

21% have antivirus protection and update it occasionally

7% have antivirus protection and don't update it

2% don't have antivirus protection

3% don't know

7 Key take-outs

- Cybercrime is on the increase as the tools and tactics used by hackers to previously cause disruption to machines and networks have become monetised by criminal gangs, through bank fraud and ID theft
- Smartphones are no longer just phones – they are mini-PCs, and consumers are failing to realise that this makes them as vulnerable to cybercrime as a computer. Money can be taken almost unnoticed through premium-rate SMS fraud that consumers are unlikely to spot
- Consumers are aware of the need for antivirus protection, but nearly one in 10 of our survey respondents fail to keep their protection updated. The 18–35 age group is often particularly susceptible to this
- The Internet of Things will soon become part of our connected world, opening new opportunities for hackers to cause harm and havoc

CONSUMERS MUST:

- Install security tools and keep them updated
- Allow automatic updates for the software and operating system they are running
- Extend this stance to their smartphones, laptops, netbooks and tablet devices
- Report cybercrime to the police
- Put pressure on people they know to take internet security seriously
- Remember not to reveal sensitive information online, particularly in social media

BUSINESSES AND WEBSITE OPERATORS MUST:

- Protect, and keep protection updated for all computers and mobile computing devices that are brought in or taken home by staff, contractors, clients and visitors
- Take steps to protect against SQL injection attacks. These have been around for more than a decade, yet are still the most frequently used hacker tool for stealing confidential data with ease
- Promote strong password management, with password and username combinations that are not easy to guess and which include a combination of letters and numbers
- Seek advice on better protection only after the basics have been sorted
- Equate online security with corporate governance and brand protection, and make it a boardroom issue. This is not just a technology debate

GOVERNMENTS AND POLICE AUTHORITIES MUST:

- Educate the public about the need to protect themselves and one another through having internet security tools that are updated and protecting against social engineering attempts online, particularly in social media
- Take cybercrime seriously, and have channels through which it can be reported to the police and acted on and, hence, through which more accurate figures can be collated
- Establish cross-border treaties with teeth that allow investigators to pursue cybercriminals and bring them to justice with far greater speed and ease than is now possible
- Think ahead when recruiting and training experts in internet security and cybercrime trends

FUTURE POLL

8 Bibliography

OECD (2011). **The International Futures Programme**. [Online] Available from: http://www.oecd.org/futures

Brown, I. and Sommer, P. (2011). **Reducing Systemic Cybersecurity Risk**. IFP/WKP/FGS(2011)3. Paris: OECD/IFP

UK Office of Cyber Security and Information Assurance in the Cabinet Office / Detica (2011). **The Cost of Cyber Crime**. London: Detica

Motavalli, J. (2010). The Dozens of Computers That Make Modern Cars Go (and Stop). **New York Times**. 4 February 2010. Available from: http://www.nytimes.com/2010/02/05/technology/05electronics.html

Future Crimes (2010). **100 Cars Remotely Hacked: The Back-Door in Your Vehicle May Not Be the One You Think**. [Online]. Available from: http://www.futurecrimes.com/article/100-cars-remotely-hacked-the-back-door-in-your-vehicle-may-not-be-the-one-you-think-2/

ABI (2010). **Automotive Software Applications**. [Online]. London: ABI. Available at: http://www.abiresearch.com/research/1004898

Kharif, O. (2010). GM, Ford, Nissan Bring Smartphone Apps to Cars. **Bloomberg Business Week**. 18 November 2010. [Online]. Available from: http://www.businessweek.com/technology/content/nov2010/tc20101117_352847.htm

Naone, E. (2011). Taking Control of Cars From Afar: Researchers Show They Can Hack into Cars Wirelessly. **MIT Technology Review**. [Online]. 14 March 2011. Available from: http://www.technologyreview.com/computing/35094/?ref=rss&a=f

Anthony, S. (2011). Black Hat Hacker Details Lethal Wireless Attack on Insulin Pumps. **Extreme Tech**. [Online]. 5 August 2011. Available at: http://www.extremetech.com/extreme/92054-black-hat-hacker-details-wireless-attack-on-insulin-pumps

Storm, D. (2011). Jamming Signals To Stop Hackers From Lethal Pacemaker Attacks. **Computer World**. [Online]. 23 August 2011. Available from: http://blogs.computerworld.com/18842/jamming_signals_to_stop_hackers_from_lethal_pacemaker_attacks

Wall, D.S. (2008). Cybercrime and the Culture Of Fear: Social Science Fiction(s) and the Production of Knowledge about Cybercrime (Revised Feb. 2011), Information, Communication & Society (11): 861-884.

Newman, T. Rad, T. Strauchs, J. (2011). **SCADA and PLC Vulnerabilities in Correctional Facilities**

Zetter, K. (2011). Researchers Say Vulnerabilities Could Let Hackers Spring Prisoners From Cells. **Wired**. [Online]. 29 July 2011. Available from: http://www.wired.com/threatlevel/2011/07/prison-plc-vulnerabilities/

Hacking Extreme Disclosure Expose. (2011). Hacking Home Automation Systems Through Your Power Lines. [Online]. 6 August 2011. Available from: http://hackingexpose.blogspot.com/2011/08/hacking-home-automation-systems-through.html

Gallucci, M. (2011). California Adopts First Standards for Cyber Security of Smart Meters. **Inside Climate News**. [Online]. 4 August 2011. Available from: http://solveclimatenews.com/news/20110804/california-adopts-first-standards-cyber-security-smart-meters

Pike Research (2011). **Utility Investment in Cyber Security for Industrial Control Systems to Total $4.1 Billion by 2018**. [Online]. 23 August 2011. Available from: http://www.pikeresearch.com/newsroom/utility-investment-in-cyber-security-for-industrial-control-systems-to-total-4-1-billion-by-2018

Ungerleider, N. (2011). Car Jack-Jacking: Cybersecurity Is The Next Challenge For Electric Vehicles. **Fast Company** [Online]. 16 August 2011. Available from: http://www.fastcompany.com/1773951/the-next-challenge-for-electric-cars-cybersecurity

Warnock, K. (2011). Iowa State Team to Examine Smart Grid Vulnerabilities. **Iowa State Daily**. [Online]. 20 January 2011. Available from: http://www.iowastatedaily.com/news/article_98b7795c-24ce-11e0-81b1-001cc4c002e0.html

Saenz, A. (2011). PayPal Predicts Wallets Will Die by 2015... Thanks, but I'll Keep Mine for Now. **Singularity Hub**. [Online] 31 July 2011. Available from: http://singularityhub.com/2011/07/31/paypal-predicts-wallets-will-die-by-2015-thanks-but-ill-keep-mine-for-now/

Infonetics (2011). **Security Client Software**. [Online] Cambell, California: Infonetics. Available from: http://www.infonetics.com/pr/2011/2H10-Security-Client-Software-Market-Highlights.asp

Wasserman, T. (2011). Mobile Hacking: How Safe Is Your Smartphone? **Mashable**. [Online]. 13 July 2011. Available from: http://mashable.com/2011/07/13/mobile-hacking-security/

Mims, C. (2011). Beyond Cell Phone Wallets, Biometrics Promise Truly Wallet-Free Future. **MIT Technology Review**. [Online]. 8 March 2011. Available from: http://www.technologyreview.com/blog/mimssbits/27057/

Libicki, M.C. (2009), **Cyberdeterrence and Cyberwar**. Santa Monica: RAND Corporation

Euromonitor (2010). **Shrinking Global Child Population**. [Online]. 27 August 2010. Available at: http://blog.euromonitor.com/2010/08/shrinking-global-child-population.html

Hof, R. D. (2011). Bring Your Own Device. **MIT Technology Review**. [Online]. 15 August 2011. Available from: http://www.technologyreview.com/business/38182/page1/

UK. National Fraud Authority (2010). **Identity Fraud Costs UK £2.7 Billion Every Year**. [Online]. London: NFA. Available from: http://collections.europarchive.org/tna/20110203091302/http://www.attorneygeneral.gov.uk/nfa/WhatAreWeSaying/NewsRelease/Pages/identity-fraud-costs-27billion.aspx

Travis, A. (2011). Car Crime Fall Key to Historic Low in Crime Rate. **The Guardian**. [Online]. 16 June 2011. Available from: http://www.guardian.co.uk/uk/2011/jun/16/car-crime-fall-historic-low

Vijayan, J. (2010). Fake Femme Fatale Shows Social Network Risks. **Computer World**. [Online] 22 July 2010. Available from: http://www.computerworld.com/s/article/9179507/Fake_i_femme_fatale_i_shows_social_network_risks

Chui, M. Löffler, M. and Roberts, R. (2011). The Internet of Things. **McKinsey Quarterly**. [Online] March 2010. Available from: https://www.mckinseyquarterly.com/The_Internet_of_Things_2538

Thaler, R. H., Sunstein, C. R. and Balz, J. P., (2010). Choice Architecture (2 April 2010). Available from: http://ssrn.com/abstract=1583509

Haselton, B. (2009). Let Big Brother Hawk Anti-Virus Software. **Slashdot** [Online]. 6 May 2009. Available from: http://yro.slashdot.org/story/09/05/06/1331247/Let-Big-Brother-Hawk-Anti-Virus-Software

UK. Ofcom (2011). **Communications Market Report: UK**. London: Ofcom. [Online] Available from: http://stakeholders.ofcom.org.uk/market-data-research/market-data/communications-market-reports/cmr11/uk/

JWT Intelligence (2011). **Social Commerce** [Online]. Available from: http://www.jwtintelligence.com/2011/07/social-commerce/

Mitnick, K. (2011) **Ghost in the Wires: My Adventures as the World's Most Wanted Hacker**. New York: Little, Brown & Company

Glenny, M. (2011). We Must Learn How the Hackers Think. **Financial Times**. 17 June 2011. [Online]. Available from: http://www.ft.com/cms/s/0/bf28f5a8-990d-11e0-acd2-00144feab49a.html#axzz1XAJ9XvgV