PRIVATE VIEW ON CYBER

How can we stay protected in the digital age?

In this edition of PRIVATE**VIEW**, we focus on cybercrime. Fraud is now the crime most commonly experienced in the UK. How we protect ourselves, our families, and our businesses is increasingly important.

In 2016 there were an estimated 3.6 million fraud incidents in the UK, with 1.9 million of those cyber-related[1]. Criminals see wealthy individuals as easy targets, as their assets may be less secure than businesses, although just as valuable.

Furthermore, the invasion of personal privacy and reputational risks are also a major concern. Rapid changes in technology have meant that all aspects of our personal lives are more at risk. Attacks are becoming increasingly sophisticated and complex. Connecting our devices to our bank accounts, online shopping accounts, and home appliances, mean that a hacker can potentially tap into one device or account, which in turn gives them access to more of our details than ever before.

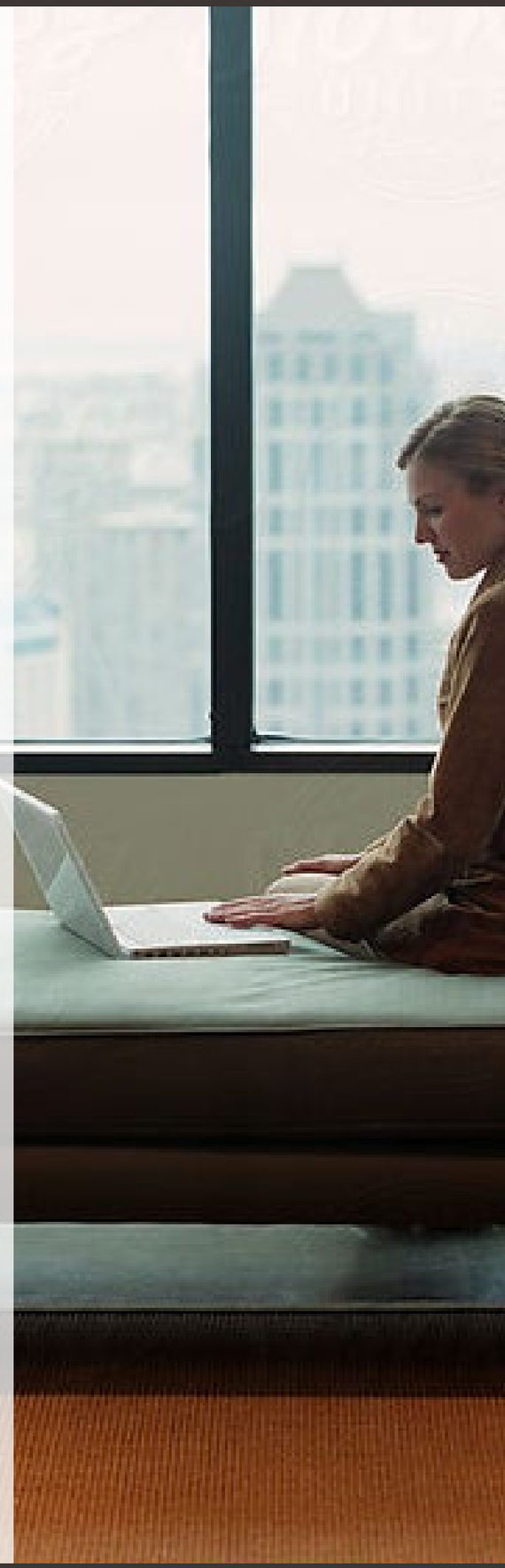
Phishing, whaling and the Internet of Things are new terms that every individual now needs to be aware of. In this publication we explore how to identify, be vigilant against and even seek justice following attacks on both our personal lives and our business ventures.

Thank you to our guest contributors for their insights. If you would like to follow up on any of the topics raised, please get in touch with the BDO contacts.

HELEN JONES
On behalf of the Private Client Services Partners

1 https://www.ons.gov.uk/aboutus/transparencyandgovernance/freedomofinformationfoi/internetuseandcybercrime2006to2017

PRIVATE**VIEW** *ON **CYBER***



NEW KINDS OF CON

SOCIAL ENGINEERING

Technology users in today's world are much more aware of the cyber risks that affect them than the previous generation. We typically imagine cyber criminals to be technologically savvy individuals who outsmart the victim using their extensive knowledge. An increasing number of cyber criminals utilise social engineering, defined as 'the use of psychological manipulation of people into performing actions of divulging confidential information', to add a dangerous new dimension to cybercrime.

PHISHING SCAMS

Phishing scams are a type of social engineering in which an email purports to be from a trusted colleague, friend or organisation. They are increasing in their sophistication on a daily basis and examples inlcude:

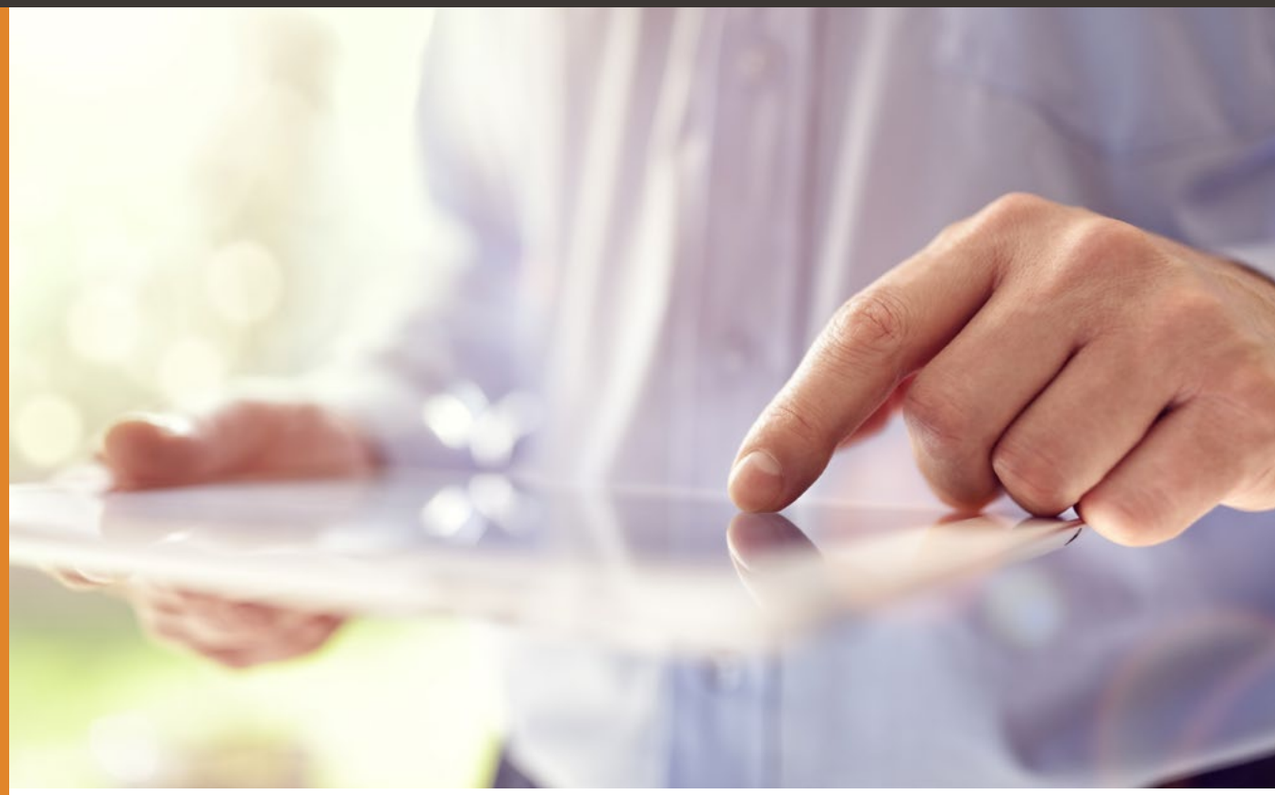
- Emails written in a casual format, with a simple request such as 'please take a look at the following article' or 'open the attached schedule', which often leads the target to provide information like their username and passwords. These emails can appear to come from trusted sources and appear genuine.
- Emails sent pretending to be from another employee asking for a quick transfer of money e.g. "I'm in a meeting now so can't speak but please transfer the amount to XXXX, their bank details are XXXXXXX. This is really urgent, please action immediately".

RANSOMWARE

There are numerous stories of ransomware being spread through downloading attachments or clicking links in innocent looking emails. A quick online search will reveal the many victims of the CryptoLocker virus, victims are required to transfer around $500 in bitcoin to recover their files which have been encrypted by the ransomware.

Users should also be aware of the more sophisticated "Whaling" attacks. Whilst in essence these are the same as phishing scams, the perpetrator will target powerful, wealthy individuals through a legitimate looking business email – often having researched their target.

Always 'think', 'challenge' and 'verify' if an online request may seem unusual or excessive.



91%
OF **CYBER-ATTACKS** START WITH A PHISHING EMAIL[1]

30%
OF PHISHING EMAILS GET OPENED[1]

OVER
400,000
PHISHING SITES WERE DETECTED EACH MONTH IN 2016[1]

SINCE YOU STARTED READING THIS PAGE, THE COST OF CYBERCRIME TO THE UK ECONOMY HAS BEEN
£188,604[2]

1in10 PEOPLE IN ENGLAND AND WALES HAVE BEEN THE VICTIM OF CYBERCRIME IN THE PAST YEAR[3]

1 Data provided by an external consultant, Cybercrowd, for BDO
2 http://www.business2community.com/infographics/internet-security-essentials-small-businesses-2017-infographic-01747572#SwPX389E62l6BloH.97
3 https://www.theguardian.com/uk-news/2016/jul/21/crime-rate-online-offences-cybercrime-ons-figures

Consider the risk of connecting your devices

The Internet of Things (IoT) is a growing opportunity for cyber fraud. The term refers to individuals being able to access everything they need at the click of a button on internet enabled devices.

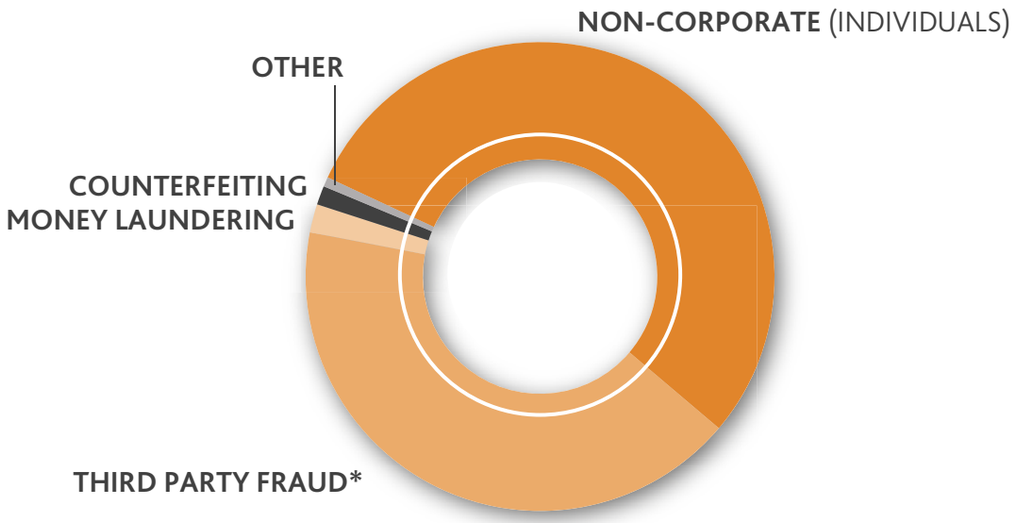
However, criminals and fraudsters now have access to even more of our personal data through previously inanimate objects including fridges, televisions and energy meters.

Criminals can take advantage of flaws in online security. It is suggested that all new appliances, capable of being hooked up to the internet, should carry a rating showing how secure they are. It comes after leaked documents showed that intelligence agencies worked with the CIA to turn Samsung televisions and smartphones into bugging devices that can record conversations and take photographs. There have been stories of laptop webcams being hacked and switched on remotely, as well as other devices listening in to conversations – companies are now using this information to target you with the right kind of advertising.

A recent police statement on the IoT explained: "It's not just that they [cyber-criminals] are going to get into your fridge and find out how many yoghurts you eat a week. The fact is that your 'internet of things' are all plugged into the same network and that provides the criminal with a back door into your home network".

BDO's Fraudtrack report 2017 found that in 2016, individuals (rather than corporate entities) were again the most common target for fraudsters…

Split of reported fraud cases against individuals 2016



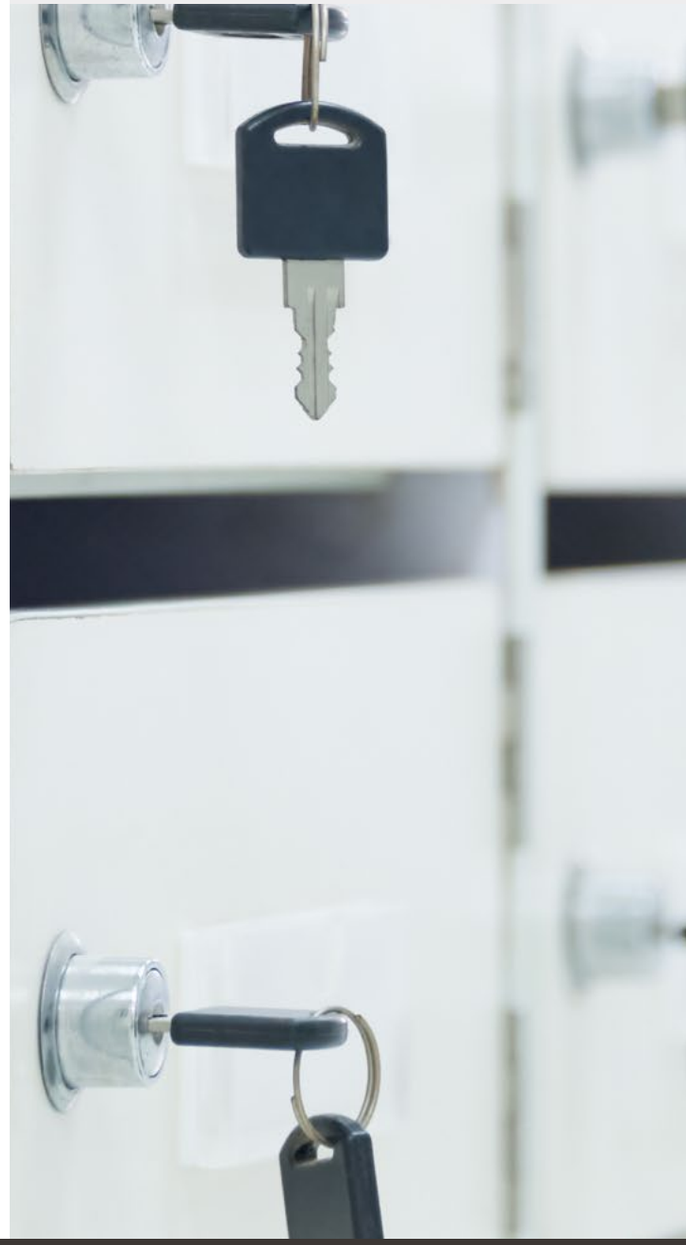
* Which is committed by either customers or suppliers.

DID YOU KNOW?

- Applications on smartphones nowadays can have the ability to track your location. This could mean that you and your family member's movements could be being monitored unless you review such settings.
- Our fridges and heating systems can now be digitised and controlled remotely. However, if data is available demonstrating when your fridge is empty, or your heating system has been off for a week, criminals could use these technologies to establish when your house is empty.
- Devices such as Siri and Amazon's Alexa are marketed for their ease and efficiency – you can call out to Alexa from your living room and ask her to play a certain song. However, if she's always listening, what else will she hear, and who else could access the recording?
- CCTV monitoring systems are now more and more accessible from smartphones, which in turn could lead to easy access to a criminal who is checking up on the everyday activity and routines of your household.

STAY PROTECTED

Download and install software updates which will contain critical security fixes to ensure that your devices are protected against the latest vulnerabilities and threats.



IS AGE JUST A NUMBER?

Your age can make you a target for certain fraudsters.

A report published by the charity Age UK found that over half (53 per cent) of people aged 65+ believe they have been targeted by fraudsters and a staggering half a million older people have fallen victim to lost savings.

Looking at the other end of the age spectrum, according to Ofcom's Media Use and Attitudes 2015 report, the average time spent online by young adults almost tripled from 10 hours and 24 minutes each week in 2005 to 27 hours and 36 minutes in 2014; and has potentially risen further since then considering the now ubiquitous nature of our smartphones. Although being more familiar with the concept of cyber security, the younger generation are sharing more and more of their lives online, and the lack of focus on privacy can make them prime targets for cyber criminals.

The report also found that four in five social media users log in to the most popular social media platforms (Facebook, Twitter, LinkedIn, Instagram or Tumblr) at least once a day. Almost 70% of these users say they feel comfortable giving away personal information on the internet, including their home address, and a quarter say they don't read website terms and conditions or privacy statements at all.

With the ever increasing need to speed up processes when logging into accounts, all of the major smartphones now offer their owners the ability to 'autofill' email addresses and save passwords for future purchases. The relaxation of these security check-points can allow hackers access to multiple accounts across a range of sites and in turn gain immediate access to bank account details, email addresses, telephone numbers and even mailing addresses.

In recent years, students were warned to be vigilant against fraudulent emails purportedly from the Student Loans Company ('SLC'). According to the SLC, since April 2011, over 2,700 students have had their bank details changed in an attempt to divert their student funding into a third party account.

Even if adults are aware of the threat, the pressure to educate children effectively is growing.

41%

OF TEENAGERS HAVE BEEN TARGETED FOR BANK DETAILS

HOW CAN WE PROTECT OUR TEENAGERS AND YOUNG ADULTS?

Have regular conversations and share articles, press coverage and news around fraud and new cyber hacks with your children. Educate yourself and your loved ones.

Ensure basic privacy settings are in place for all devices used to access the internet and social media accounts.

Give guidance on only handing personal information to trustworthy sources and the importance of having strong, complex passwords, that are not used for multiple accounts.

IDENTITY AND PRIVACY

Is money the least of our worries?

Cyber criminals aren't only after money; your identity and personal details may be the bigger prize. So while a one-off high value purchase from an Amazon account may seem desirable, there is often more value from knowing someone's personal details.

Stealing account details can buy the criminal's time to build a picture of your identity. They can then monetise seemingly harmless data in indirect ways and use them in more complex identity fraud scenarios. If a scammer can access your emails and bank account details, it won't take them long to build up a list of further targets and a picture of your daily activities and contacts – from the wealth manager emailed every month, to the trust company being visited as part of an overseas trip, to the real estate adviser who stores contact details in relation to a forthcoming property transaction.

The November 2016 Morgan Stanley Investor Pulse which focused on the worries of cybercrime targeting wealthy individuals found that 72% of respondents said identity theft was their biggest worry, ahead of the threats of both terrorism and major illness.

How easy is it to steal someone's identity and personal details?

The first step a hacker would typically take is to identify the name of a target individual, which they will internet search to find all available social media accounts, or other information that will help them build the profile of a target. This is all information which is easy accessible.

A common next step will be to trigger a 'forgot my password' email. Through this, they are able to work out parts of the person's email address – websites usually show the email address with some characters blanked out. However, by doing the same on other social media sites, hackers can fill in the missing gaps.

Recent news stories have covered data sources stolen from organisations such as websites and banks being posted on the Dark Web (the part of the internet invisible to standard search engines). Hackers can also utilise these data sources to identify email addresses, and thus obtain a matching password.

More than half of UK adults are risking their online security by using the same password for most if not all websites they visit, according to research by regulator Ofcom.

Ofcom's study found 55% of adult internet users use the same password, while 26% say they tend to use easy to remember passwords such as birthdays or names, potentially opening themselves to a higher level of account hacking.

Once a hacker cracks a password, it's very likely they can access online shopping accounts which store bank details and billing addresses.

DID YOU KNOW THAT FRAUDSTERS CAN:

- Send an e-card or invitation to your email address and track your location when you open it?
- Work out when you are out of the country? If they can access your emails, they can find out your latest hotel and flight bookings
- Make copies of keys? If you post a photograph of a set of keys online, celebrating a new house purchase, sophisticated hackers can copy these keys using a 3D image.

Read our top tips for protecting your identity.

Reputation and privacy risk

Alongside the financial risks of cyber threats comes the ever present need to manage reputation and protect privacy – to understand the potential threats that the digital age brings and to be prepared.

Reputation management and protection of privacy has many aspects. We spoke with the law firm, Schillings, who specialise in protecting the reputation and privacy of international families in times of crisis. Of the online threats they highlight:

- Be aware of your digital footprint – how much information is available about you and your family members, your business interests?
- Given the risks of a cyber-attack and the theft of your private and confidential information – consider who is looking at your personal data. Who might want to buy it and how could this be used against you?
- Highly sophisticated smear campaigns can develop from negative comments on-line to deliberate malevolent attempts to sabotage your reputation. The almost instant communication of messages through social media compounds the necessity of swift action, particularly online.
- Recognise that reputation and privacy threats can often be avoided or reduced by predicting when the risks are particularly high and taking clear steps to be more vigilant at these times.

Rachel, who specialises in Digital Privacy, discusses the key risks:

"Families and businesses are unnecessarily increasing their risk to the most common threats to their reputation and privacy because they are not making the link between the risks of the theft of their private and confidential data and the impact this can have on their reputation and privacy.

"At Schillings, we see lots of deliberate attacks on families by those opposed to them. With increasing frequency, they are pursuing stolen or publicly available information to gain an edge regarding public interest.

"Reputation and privacy are now more fragile and more easily destroyed than ever before. The speed of dissemination means stories work their way into the grain of the internet very quickly. Coupled with today's plethora of news sources and that everyone with a smartphone is a publisher, it has never been easier for someone with an agenda or an axe to grind to create a fake news campaign targeting a family, a family member or a business.

"The trick is to get interested in your private and confidential information, as well as your publicly available data, before someone else does."

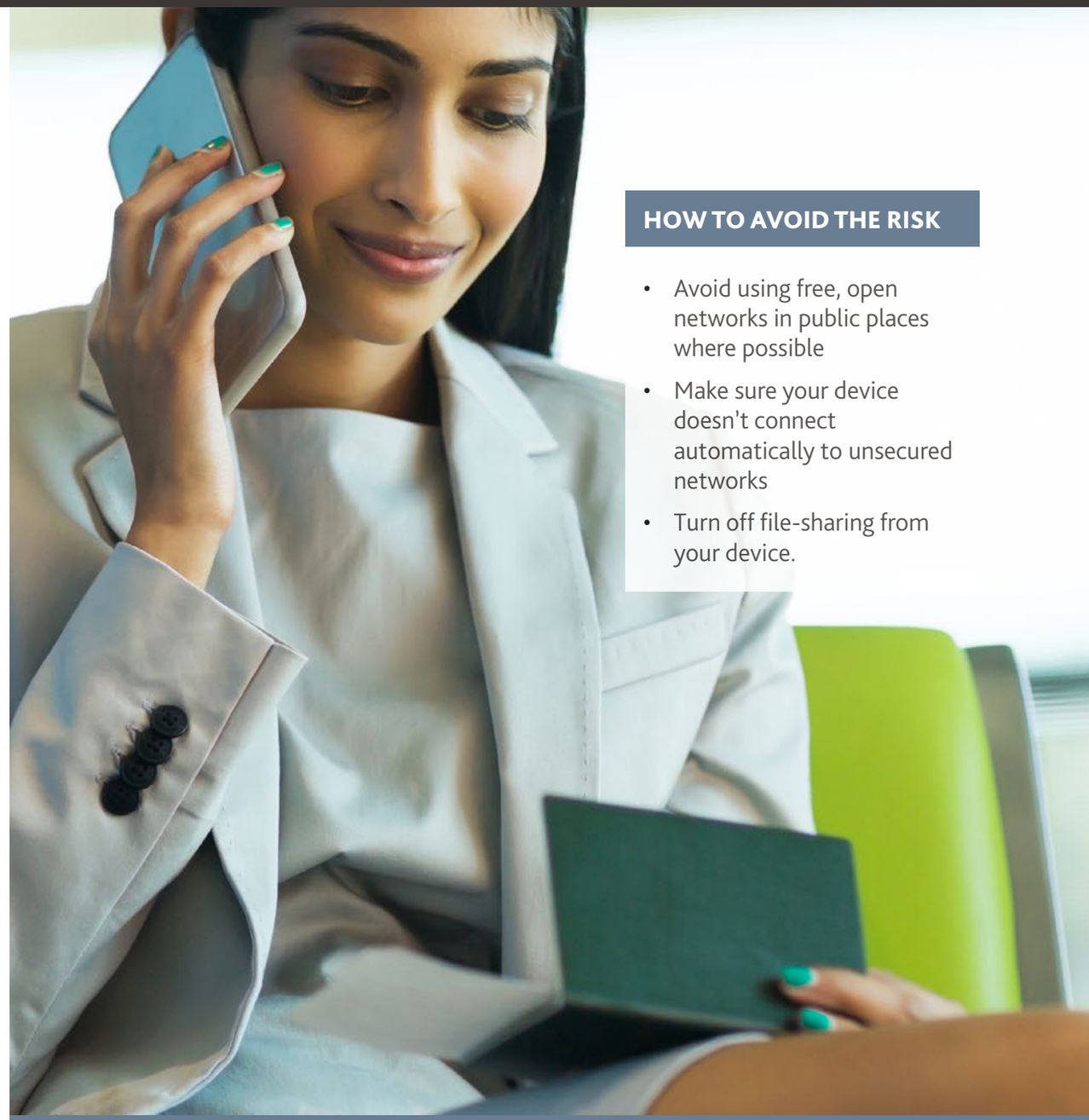
INTERNATIONAL CONNECTIONS

Do you know the risks of using unsecured networks when travelling?

Regular travellers are familiar with long periods of waiting in airports and the need to stay in contact at these times. Most airports are well connected with various Wi-Fi offerings, but this has been leveraged by cyber criminals to access and steal personal data.

Research conducted by the Better Business Bureau (BBB) found that hackers use free airport Wi-Fi networks to access travellers' personal data. The BBB warns that hackers are now taking advantage of this convenience and setting up fake Wi-Fi connections designed to steal personal data from unsuspecting travellers.

When searching for connections, individuals may find cleverly named network connections, sometimes named something as simple as "Free Wi-Fi" which sounds like a legitimate network offered by the establishment. This wireless network will often be an open, unencrypted network; thus not offering protection against others eavesdropping on one's communication. If a rogue wireless access point has been set up, the user will still be able to surf the Internet, but they'll be doing it through a hacker's computer. The hacker could be stealing information like passwords, credit card and bank account details, and social security numbers. Beyond simply stealing keystroke information as the user enters various types of data, if the device is set to share files, whole documents from the computer can be accessed and stolen.



HOW TO AVOID THE RISK

- Avoid using free, open networks in public places where possible
- Make sure your device doesn't connect automatically to unsecured networks
- Turn off file-sharing from your device.

THE DARKHOTEL

In addition to being wary of public Wi-Fi access points, regular travellers need to be aware of a growing trend in cyber criminals targeting the networks of popular, often luxury, hotels across the globe. A well publicised, international event, hosted by a famous hotel acts as a beacon for fraudsters – high-profile guests who set themselves up for a week in the hotel, meeting key advisers and partners, are often easy targets. In a story that hit the news in 2016, it was established that hackers entered a hotel's system days before a particular wealthy individual stayed there for an event, waiting for him to check in before hacking into his laptop and accounts.

AN OFFSHORE ADVISER MAY HOLD YOUR PERSONAL DATA – ARE THEY READY FOR GDPR?

One of the biggest changes in data regulation will come into force in May 2018. The **General Data Protection Regulations (GDPR)** applies to European Union (EU) businesses as well as to any organisation, anywhere in the world that processes the personal data of EU citizens. It sets certain benchmarks and rules for the way consumer data is treated. Fines will be levved for non compliances.

If your personal data is affected, you should ask your service providers what they are doing about GDPR.

CHARITY FRAUD

Charities remain a key target for fraudsters. With funds and donations coming in and out of the charity from a variety of sources, wealthy individuals as trustees and board members, and complicated governance structures, it is of little surprise that charities of all sizes can fall foul to cyber-attacks and fraud.

The Charity Commission, along with counter-fraud organisations such as the Fraud Advisory Panel and National Cyber Security Centre, produce a wide range of guidance and tools for charities to counter fraud.

Guidance to charities, following the worldwide WannaCry ransomware attack in May 2017, included:

- Install system updates on all devices as soon as they become available
- Install anti-virus software on all devices and keep this updated
- Create regular backups of your important/ business critical files to a device that is not left connected to your network, as any malware infection could be spread to that too
- Do not meet any stated demands and pay a ransom – this may be requested via Bitcoins (a form of digital or 'crypto' currency)

If you are involved with a charity, either as an ambassador, significant donor or trustee, it's important that the charity take their cyber security obligations seriously. As discussed elsewhere previously, cyber criminals tend to go for the easy targets. Ensure that your charity understands the risks and puts appropriate protection strategies in place. They should undergo regular penetration testing, adhere to robust information security standards and have reputable external auditors.

In 2017, the Fundraising Regulator (FR) stated that more needs to be done about fraudulent crowdfunding websites. Unfortunately, fraudsters exploit others' hardships and tragedies and set up clone online fundraising sites. In 2017, after recent terror attacks in London, fake JustGiving sites were set up and spread quickly throughout social media making it difficult to differentiate the genuine pages.

Keep an eye out for clues such as:

- When was the site set up and how many donors does it currently have?
- If a charity is supposedly associated with the fundraising, is their logo and website linked?
- Check that the website URL looks legitimate – if in doubt, get in touch with the site administrator.

The cost of fraud to UK charities is unknown. Estimates vary widely but it could be as much as £2bn a year. Whatever the amount, the impact of fraud is keenly felt in a sector where even small amounts count.

We discussed the ever-growing threat of fraud and online scams to charities and philanthropists with Dr Stephen Hill of the counter-fraud charity Fraud Advisory Panel. Dr Hill is a Trustee Director of the Fraud Advisory Panel, which was established by the ICAEW and he chairs its cybercrime interest group working with colleagues from the public, private and voluntary sectors.

Stephen – what are the most popular scams facing charities?

Charities face the same fraud risks as other organisations and businesses, as well as some that are a little more unique to the sector itself, such as fundraising fraud.

Some of the most common online scams are fake fundraising websites, which often appear in the immediate wake of natural or humanitarian crises or during religious festivals (such as Ramadan), and phishing emails which can either target charities directly for information (CEO fraud is a good example) or impersonate them to trick donors. Charities that make their bank account details publicly available are also at risk of having fake direct debits set up on their accounts by fraudsters.

Are charities with wealthy individuals as trustees or regular major donors at higher risk of cybercrime/fraud?

Potentially. Not because of their involvement with a particular charity or charities per se, but because of their high net worth.

Over recent years we have seen the emergence of 'whale phishing', where fraudsters specifically target certain individuals because of their wealth or reputation to trick them into disclosing personal or financial information such as passwords and credit card details, which are then used for malicious or illegal purposes. These emails are becoming increasingly sophisticated and often use information collected from sources like LinkedIn, Facebook or Instagram to make them sound more genuine.

In circumstances where individuals are also trustees of charities, this might extend to attempts to obtain information about their charities too. Charities often hold a lot of valuable and sensitive information about their donors, beneficiaries and partners – the trustee, in this case, then becomes a high-profile link between themselves and the organisation.

DR STEPHEN HILL
ICAEW FRAUD ADVISORY PANEL

Are charities doing enough to deal with this risk?

In recent years we have seen a significant step-change in attitudes toward fraud – by regulators and individual charities alike – to engage with the issue in a positive and proactive way. Many organisations are offering fraud awareness training sessions to board members and their trustees.

This is supported by two national conferences on fraud, a dedicated charity fraud awareness week and the establishment of the 'Charities against Fraud' partnership which comprises over 40 charities, professional representative charitable bodies and other not-for-profit stakeholders working together to combat fraud against the sector.

Find out more about Charity Fraud Awareness Week.

PRIVATE ACTION

It is a common misconception that only the Crown Prosecution Service (CPS), government agencies and other public bodies can bring prosecutions. In England and Wales a private prosecution can be brought by any private individual or body – including the victims of cyber fraud.

Wealthy individuals who have fallen victim to crime are increasingly exploring the option of private prosecutions.

WHAT IS A PRIVATE PROSECUTION?

The CPS defines a private prosecution as 'a prosecution started by a private individual, or entity who/which is not acting on behalf of the police or other prosecuting authority'. A 'prosecuting authority' includes, but is not limited to, an entity which has a statutory power to prosecute.

It is, put simply, a criminal prosecution pursued by a private person or body and not by a statutory prosecuting authority. For all other purposes it operates in exactly the same way as a criminal prosecution brought by the State.

The Fraud Advisory Panel offers a useful help sheet on Private Prosecutions, discussing how they work in practice and contact information.

WHY WOULD AN INDIVIDUAL CONSIDER A PRIVATE PROSECUTION?

One particular high profile private prosecution case was brought by businessman Murli Mirchandani, against Mr Ketan Somaia in 2014.

Mr Somaia had made deliberate and dishonest representations to Mr Mirchandani to persuade him to make short term loan payments to him to the value of £13.5 million, with the assurance of high rates of interest and investments in business opportunities. He then used the money to fund his own lavish lifestyle and support his own failing companies, without returning a single penny to Mr Mirchandani. Mr Mirchandani reported the matter to the police, however they declined to investigate. He then commenced a private prosecution and following a lengthy trial, Mr Somaia was found guilty of 9 counts of obtaining a money transfer by deception and was sentenced to 8 years imprisonment. He was later subject to a £20m confiscation order and was ordered to pay Mr Mirchandani £18m in compensation.

REPORTING CRIMES

It is important to report all instances of cybercrime however small, to ensure crime stats are accurate and to help prevent future cases. For a central point of contact for information about fraud and cybercrime, contact Action Fraud, the national fraud and cybercrime reporting centre.

Overleaf, BDO Forensic Services partner Stephen Peters further explores the basics of private prosecution and the costs of pursuing them. ▶

In an interview with Tamlyn Edmonds, partner and co-founder of specialist private prosecution firm Edmonds Marshall McMahon, BDO forensic services partner, Stephen Peters, runs through the basics of private prosecutions, in the context of cyber fraud, as well as discussing the costs and barriers involved in pursuing them.

Tamlyn, to start with – why have most individuals not heard of private prosecutions before?

Often victims of crime, both individuals and companies, are not aware that private prosecutions are an alternative option to relying on the state to act and can often be a cheaper and quicker alternative to civil action.

Whilst the need for the pursuit of private prosecutions has greatly diminished since the creation of the Crown Prosecution Service (CPS), they are now on the rise again due to the current climate of austerity, budgetary constraints of traditional law enforcement bodies and increasingly complex crimes. This is especially so in the area of cybercrime and fraud.

Why would anyone pursue private prosecution rather than let the police/CPS simply do their job?

The main reason is down to the fact that the police and other traditional law enforcement agencies have suffered massive cutbacks over recent years and no longer have the resources to dedicate to certain types of crime.

Investigation of economic crime and cybercrime in particular, has borne the brunt of austerity measures with the loss of specialist economic crime teams within police forces and lack of specialist knowledge. This can leave victims of these types of crime feeling increasingly frustrated at lack of police action, making private prosecutions an attractive option in the pursuit of justice.

Rapid advances of technologies and the growth of the internet has changed the face of crime. High net worth individuals are often the target of cyber related crimes as the returns for the criminal are potentially high compared with the low risk of getting caught. Private prosecutions can provide the victim with an effective alternative to state action.

Are private prosecutions worth pursuing in terms of cost?

The costs of a private prosecution can vary depending on the size and complexity of the case. Large fraud cases with multiple defendants will obviously be far more expensive than a small straightforward theft or fraud case. One of the most important aspects to private prosecutions relates to the recoverability of costs incurred in bringing the prosecution.

Courts are entitled to order payment out of central funds to compensate a private prosecutor for any expenses incurred by them. This includes both legal and investigative costs and any expert fees that were necessary for the prosecution where those costs are incurred in the proceedings. It is important to note that the Court can make an award for costs out of central funds irrespective of the result, so it does not matter if the defendant is convicted or acquitted - the private prosecutor can still be compensated for the costs of bringing the prosecution.

Who would pursue a private criminal prosecution – individuals or just big companies?

The simple answer to this question is that anyone can. There is no requirement that a private prosecutor be the victim of the crime, or connected to the crime that they wish to prosecute. Any person or entity having 'legal personality', including companies and charities, has the ability to pursue a private prosecution.

Thanks Tamlyn, it will be interesting to see if the number of private prosecution cases continue to rise as the cyber threat to all of us stays ever-present.

TAMLYN EDMONDS
PARTNER & CO-FOUNDER,
EDMONDS MARSHALL MCMAHON

STEPHEN PETERS
FORENSIC SERVICES PARTNER,
BDO UK

THE BUSINESS OF PREVENTION

A top agenda issue

Cyber-attacks are becoming increasingly sophisticated and complex, representing a substantial risk both to businesses and to us all as individuals. How businesses protect themselves and keep ahead of cyber criminals is a top agenda issue.

According to 500 global business leaders as surveyed in the BDO Global Risk Landscape report 2017, disruptive technologies, reputational risk and cyber are the challenges most likely to test businesses over the next ten years.

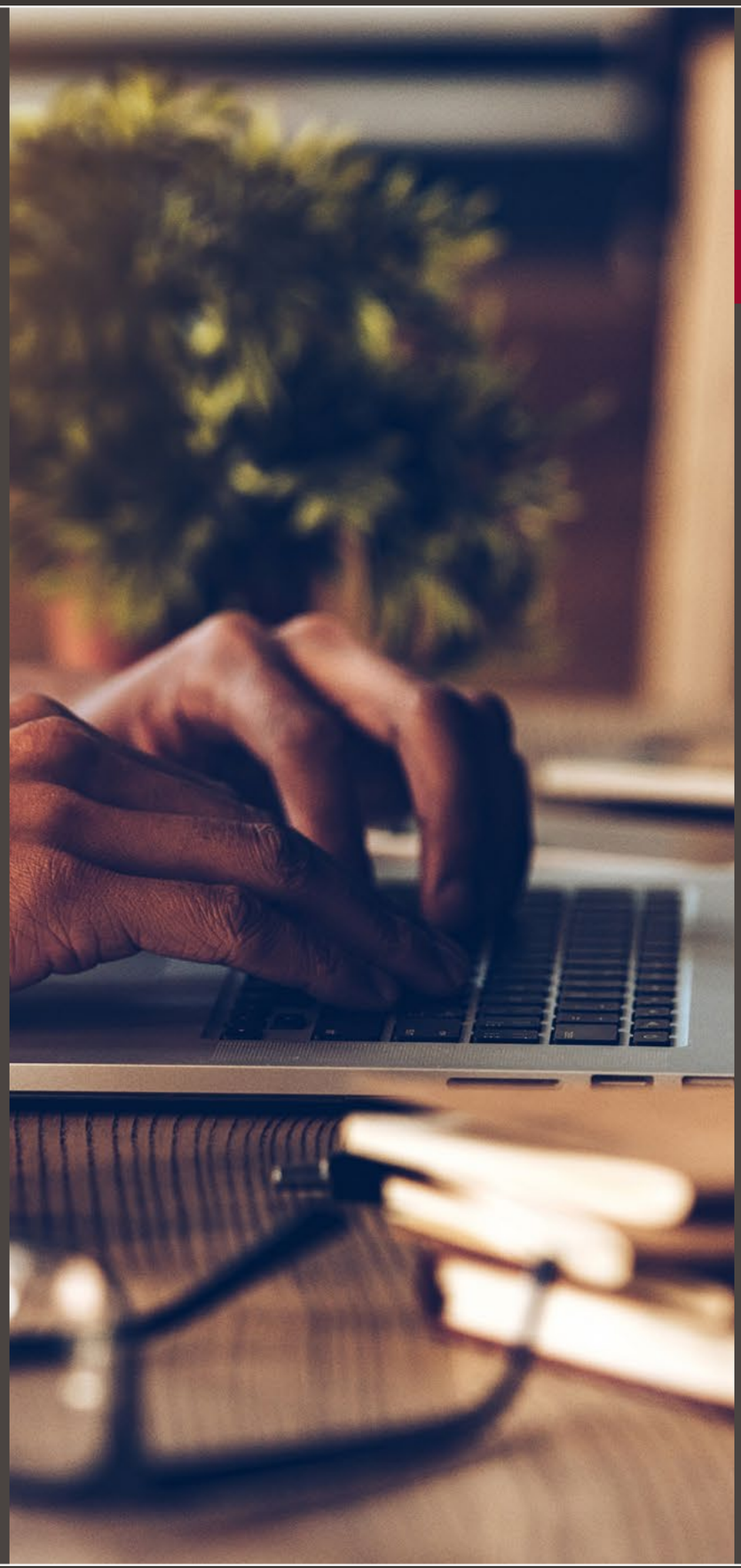
For any organisation, it's essential to protect both customer data and corporate reputation. So in order to prevent becoming a target, businesses are investing in:

CYBER RISK ASSESSMENT – identification of key risks and gaps specific to the individual business environment.

CYBER SECURITY MONITORING – these range from some relatively inexpensive network monitoring tools, to a fully managed outsourced monitoring service.

CYBER INSURANCE – many insurance companies now offer insurance to protect against internet-based risks. This is a new offering to the market that aims to protect businesses depending on what they choose to insure.

Best practice for businesses is to develop an organisation cyber security strategy in order to minimise the risks. See overleaf where we outline the questions that business leaders should ask themselves in order to develop an effective strategy.



10 TOP TIPS
TO STAY PROTECTED AT HOME AND AT WORK

1. Download the latest software updates to ensure all of your devices and gadgets are protected.
2. Never share you passwords with anyone and change them regularly. Consider using a Password Manager or Password Vault to generate and store your passwords.
3. Enable multi-factor authentication where this service is offered as this provides an extra layer of security in addition to passwords when logging into accounts.
4. Only access secure networks and turn-off file-sharing from your device when using public networks.
5. Watch out for phishing emails by treating unknown emails with suspicion and be cautious when clicking email links and opening attachments.
6. Research apps to determine whether they are safe before downloading and think about the information you are allowing the app to access.
7. Ensure basic privacy settings are in place for all devices used to access the internet and social media accounts.
8. If you are a director, owner or trustee of an organisation ensure that the risks are understood by carrying out a cyber risk assessment specific to the individual business environment.
9. Take advantage of the security offered by transaction providers such as PayPal and major credit card providers, who provide consumers a 'safety net' against fraudulent activity.
10. Avoid using auto-fill where possible and don't store bank card details on websites.

DEVELOPING AN ORGANISATIONAL CYBER SECURITY STRATEGY

Organisations are increasingly adpoting countermeasures to minimise the risks of a cyber-attack. A Cyber Security Strategy is an essential tool. Businesses should make sure this is aligned to the nature of the threats and vulnerabilities, risk appetite of the business and the level of investment available to enhance security arrangements.

In developing the organisation's approach, asking some fundamental questions can help determine how secure the business really is and what else needs to be done.

01

Do all staff have a robust understanding of the data theft, transactional fraud and sabotage threats that face the business?

02

Will the controls both at the network gateway and the application level prevent an opportunist attacker and disrupt a persistent attack?

03

How do we protect the business' "crown jewels" (most valuable data and assets) from theft, disruption or a sabotage attack?

04

Are the the right tools and processes embedded across the business to detect and attack or breach promptly?

05

What is the business's response plan in the event of a breach? What plans are in place to minimise potential impact?

06

Does management and the IT team think about cyber security insurance? If so, what are you insuring against?

07

Due to the changing threats that emerge, how does the business access the latest threat intelligence insights that are available?

ADDITIONAL INFORMATION

Cyber Security – How BDO's Cyber and Information Security team can help you understand precise threat scenarios and vulnerabilities and bring the latest insights to you and/or your business.

BDO Global Risk Landscape 2017 – Looking at the major risks facing business leaders and how disruptive technologies present both risks and opportunities.

REFERENCES AND USEFUL INFORMATION

1. MARTIN EVANS AND KATIE MORLEY, 2017. Home gadgets open to hackers. The Telegraph, 24 July. Available from http://www.telegraph.co.uk/news/2017/07/24/internet-things-will-leave-home-gadgets-vulnerable-hacks-senior/.
2. BDO FraudTrack 2017. BDO UK LLP. Available from: https://www.bdo.co.uk/en-gb/insights/advisory/forensic-services/bdo-fraudtrack-2017
3. CAROLINE ABRAHAMS, 2015. Only the tip of the iceberg; fraud against older people. Available from: http://www.ageuk.org.uk/documents/en-gb/for-professionals/consumer-issues/age%20uk%20only%20the%20tip%20of%20the%20iceberg%20april%202015.pdf?dtrk=true
4. Adult's media use and attitude, 2015. OFCOM. Available from: https://www.ofcom.org.uk/__data/assets/pdf_file/0014/82112/2015_adults_media_use_and_attitudes_report.pdf
5. JOSIE GURNEY-READ, 2014. Students warned about phishing email. The Telegraph, 18 December. Available from: http://www.telegraph.co.uk/education/universityeducation/student-finance/11300035/Students-warned-about-phishing-emails.html
6. JAVIER ESPINOZA, 2015. Four in ten teenagers 'fall victim to cyber fraudsters', says survey. The Telegraph, 22 April 2015. Available from: http://www.telegraph.co.uk/education/educationnews/11555189/Four-in-ten-teenagers-fall-victim-to-cyber-fraudsters-says-survey.html
7. Infographic: Cyber Security by the numbers, 11 November 2016. Morgan Stanley. Available from: http://www.morganstanley.com/ideas/identity-theft-protection
8. UK adults taking online password security risks, 23 April 2013. OFCOM. Available from: https://www.ofcom.org.uk/about-ofcom/latest/media/media-releases/2013/uk-adults-taking-online-password-security-risks
9. Schillings: https://www.schillingspartners.com/
10. Better Business Bureau: https://www.bbb.org/en/us/
11. GAVIN DAVIS, 2016. General Data Protection Regulations - Am I bovvered? BDO UK LLP. Available from: https://www.bdo.co.uk/en-gb/insights/advisory/technology-advisory/general-data-protection-regulations
12. JOSH HALLIDAY, 2017. Call for fundraising pages to be regulated amid fraud concerns. The Guardian, 17 April. Available from: https://www.theguardian.com/society/2017/apr/17/call-for-fundraising-pages-to-be-regulated-amid-concerns
13. Fraud Advisory Panel: for more information about the Charity Fraud Awareness Week visit here: https://www.fraudadvisorypanel.org/charity-fraud/charity-fraud-awareness-week/
14. https://www.fraudadvisorypanel.org/wp-content/uploads/2015/04/Fraud-Facts-21B-Private-Prosecutions-April13.pdf
15. Fraud Facts, Issue 21, April 2013. Fraud Advisory Panel. Available from: https://www.fraudadvisorypanel.org/wp-content/uploads/2015/04/Fraud-Facts-21B-Private-Prosecutions-April13.pdf
16. Action Fraud: http://www.actionfraud.police.uk/
17. Edmonds Marshall McMahon: http://www.emmlegal.com/
18. BDO Global Risk Landscape Report 2017. BDO UK LLP. Available at: https://www.bdo.co.uk/en-gb/global-risk-landscape-2017/home
19. Risk and Advisory Services Brochure. BDO UK LLP. Available at: https://www.bdo.co.uk/en-gb/insights/industries/aim/risk-and-advisory-services-brochure

NATIONAL CYBER SECURITY STRATEGY 2016 – 2021

The National Cyber Security Strategy 2016 to 2021 sets out the government's plan to make Britain secure and resilient in cyberspace. Find out more: https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021

FOR MORE INFORMATION:

HELEN JONES
Private Client Services Partner
+44 (0)20 7893 2072
helen.jones@bdo.co.uk

GAVIN WILLIAMSON
Fraud and Forensic Investigations Partner
+44 (0)20 3219 4123
gavin.williamson@bdo.co.uk

JASON GOTTSCHALK
Technology Risk Assurance Partner
+44 (0)20 3219 4536
jason.gottschalk@bdo.co.uk

KAREN MEENDERINK
Head of Streams / Markets, Sales & Clients
+44 (0)118 925 4448
karen.meenderink@bdo.co.uk

www.bdo.co.uk/privateclients

HB009899