



## Cybersecurity for everyone

Help and advice for staying safe at home, at work,  
online and on the move





## What's inside

### **INTRODUCTION** 3

Welcome; from the Fidelity International Head of Technology, Ian Thompson.

### **USING SOCIAL MEDIA** 4 - 7

Think about what information you put on social media and who can see it.

### **MOBILE DATA SECURITY** 8 - 10

How to keep your mobile device safe and your data secure on the move.

### **KEEPING KIDS SAFE** 11 - 13

Protect & support children as they discover the online world.

### **PASSWORD SECURITY** 14 - 18

Some tools and ideas for creating and managing good, secure passwords.

### **CYBER CRIME** 19 - 26

New forms of communication mean new types of crime, be aware.

### **WORKING TOGETHER** 27 - 30

What to expect from Information Security at work and why it matters.

### **STAYING SAFE** 31 - 33

A round up of our top digital security tips and techniques.



**Ian Thompson**  
HEAD OF TECHNOLOGY *Fidelity International*

## Cybersecurity for everyone

**Cybersecurity is an essential part of how we operate at Fidelity.<sup>1</sup> We employ a range of cybersecurity defences, ensuring we are vigilant in protecting our own information and that of our clients, which they have entrusted us with. This Cybersecurity booklet contains much information on the need for cybersecurity awareness, providing a jargon-free guide to simple and effective practices.**

This is just as important in our personal lives as it is at work. Modern digital communication methods enable us to share our lives with family, friends and work colleagues instantaneously. It has enhanced many areas of our home lives, at the same time impacting the education, mental and social development of children and teenagers.

With all the advantages, it is sometimes easy to forget that when connected to an online world, we can also be exposed to the downsides. This Cybersecurity booklet is also designed for you to take home and share with your family and friends, providing practical help and advice for staying cyber safe at home, when online and on the move. **1**

<sup>1</sup>[www.fidelity.co.uk](http://www.fidelity.co.uk): *How Fidelity protects you and how you can protect yourself.*



## Take care what you share

Social media can be a hugely fun and powerful way to keep in touch with old friends (and make new ones), share interests and keep up to date with the latest trends. Unfortunately, sites like Facebook, Twitter, YouTube, Pinterest and LinkedIn are just as popular with criminals, you may be surprised to find out why.

Of the **3.17 billion** internet users there are an estimated **2.3 billion** active social media users. Each of these has an average of **5.54 social media accounts**. Social media use has risen by **176 million** in the last year alone.

Source: brandwatch.com

<sup>2</sup> *Mashable.com: 10 People who have lost their jobs over social media mistakes.*

## CYBERSECURITY FOR EVERYONE

### USING SOCIAL MEDIA

Anyone who has spent time on social media knows exactly why it's so addictive and entertaining. You can get instant, live responses and feedback on your opinions and sometimes even take part in conversations that can make a real change to people's lives; influencing anything from what someone wears or eats to the government and politics of a nation.

But everyone knows there is a dark side to social media too. We have all read stories about 'over-sharing'<sup>2</sup>, perhaps you even know of someone who, for example, failed to get a job because a search of their name brought up compromising holiday pictures posted on Facebook.

The real danger from social media use though is the active criminal who uses what they find for their own benefit. What follows is a look at what information data hackers are after, and what they can do with it once they've got it, as well as some general advice on staying safe and not sharing more about yourself than you mean to.

#### **Anatomy of a hack**

Let's say I am a hacker and I want to take over your online identity. When you sign up to anything on the internet, from online banking to webmail, you will be asked to provide the answers to a number of security questions. Usually these are things like; your



mother's maiden name, your pet's name, your date of birth, your childhood nickname and so forth.

Now think about your social media accounts. If I have your email address how much research would it take me to get the answers to those questions? Are there pictures of your pet on Facebook, do you mention its name? Does anyone use your nickname in the comments section? Is your birthday mentioned?

You get the idea, right.

## CYBERSECURITY FOR EVERYONE

### USING SOCIAL MEDIA

Overall, **60 percent** of teen and young adult internet users have shared pictures of themselves on social media, followed by pictures of friends and family. **Half of teens and young adults** also commonly share status updates about what they are doing.

Source: statista.com

Once I've done my social media research I just need to click on the 'Forgotten your password' link in your webmail account. And from there I simply use the personal details I discovered to answer your security questions.

Now I have command of your primary email account I can use that to go through all your online accounts (don't forget, I can see all your mail so I know what you are signed up to) and click on 'password reset'. This will send a reset request to the mail account I now control allowing me to change all your passwords, locking you out.

Consider for a moment how much damage a hacker could do to your life if they had that kind of access. Could they fill in a loan application? Apply for a credit card? Buy anything they wanted on Amazon? Or just use it to know your most intimate secrets...

#### **Be careful what you share**

The first step to staying safe while still enjoying social media is this: think before you post. Be wary of putting up any information that could be used to break into your online accounts. That means guarding your home address, email addresses, phone numbers and date of birth. Consider using your security questions as another layer of security, treat them like a password; fill in the answers using made up, complex codes or phrases.

#### **Keep the public and the private separate**

Everyone wants to share personal things sometimes. If you need to then the best thing you can do is post *privately*.

Check the privacy and security settings on your social media sites so that only family and friends can see your pages. The settings are there for a reason.<sup>3</sup>

#### **Try not to let the world know where you at all times**

Telling everyone where you are at all times also let's them know where you're not; home.

Anyone watching your Twitter feed (or Foursquare, Google Buzz time-line etc) knows exactly when the best time to is to turn up to your home uninvited and steal your stuff.<sup>4</sup>

#### **Tidy up after yourself**

If you have stopped using a site, delete the account. Don't leave it lying around, unattended for anyone to pick up...

#### **Think twice, post once**

What you post online stays online, forever. Always take some time to think if what you are about to share is something you will still be happy for anyone to see in a years time (or even in the morning...).

**What happens on social media stays on Google, forever.**

”

YourSocial.com

<sup>3</sup> *identity.utexas.edu: How to manage your social media privacy settings.*



Imagine someone you respect reading your post, feel uncomfortable? Or try this; would you have a permanent tattoo of that post on your body? If the answer is no then it's probably best not to hit 'send'.

**Know who your friends are**

It can be exciting to build up a big list of 'friends' but how well do you know all of them?

In fact, how well *can* you know such a big, diverse group of people?

If you trust them like you trust your family then by all means share everything. But would you, for instance, let them into your home when you are not in? If not, think twice before you let them into your confidence.

**If something looks or feels suspicious, delete it**

Requests to sign up to something you haven't heard of, friend requests from people you don't know, online advertising and unknown links in emails and tweets are all ways cybercriminals try to steal your personal data. Do some research before you click. Or just delete it. 🚫

<sup>4</sup> *Pleaserobme.com: Raising awareness about over-sharing.*



## Digital security to go

If you regularly take your mobile device; tablet, smart phone, or laptop, with you when you go out you need to take digital security just as seriously on the move as you take it at home. As well as being easier to lose (or just leave behind) you are taking your device out of the controlled environment of your protected, personal WiFi into the big, bad world.

There are over **2.6 billion** smartphone users worldwide. **87%** of people always have their smart phone at their side and in 2016 **more searches** took place on mobile devices than on computers.

Source: [deviceatlas.com](http://deviceatlas.com)

These days we increasingly store sensitive data; emails, financial and work details, company profiles, travel itineraries etc on our mobile devices. We want to instantly access and edit this data whenever we want and wherever we are.

It's also increasingly common to use portable hardware to access information stored in the cloud. Digital storage services like Dropbox, Evernote, Microsoft OneDrive and Apple iCloud mean we are walking around with our whole data portfolio accessible in our pockets or bags.

Add to this the increasing use of smart phones as credit cards, smart keys and health monitors (amongst other applications) and you can see why it's essential you stop unauthorized users treating it as a treasure trove of your personal data.

And since your mobile device goes everywhere you do the odds of it being mislaid, lost, hacked or stolen are pretty high. Well, OK, that's the price we pay for instant access, but there are steps you can take to minimise the risk.

#### **Use the in-built features**

One of the simplest and most effective things you can do to protect your data is to take a minute to look through the security settings on your device. Using a screen lock which requires a

pass code to deactivate might be all you need to foil a casual, unauthorised user.<sup>5</sup>

#### **Find and erase**

Android, iOS and Windows operating systems all include remote find/lock/wipe features as standard. Make sure you enable and familiarise yourself with these features so you are ready to use them quickly if your device goes missing.

#### **Mobile Wi-Fi security threats**

If you are using the free WiFi in a coffee shop, library or other public place make sure you verify the name of the network with staff or on signage before connecting. On a Windows device check the *Security Type* shows as WEP or WPA2, on Mac iOS look for a padlock symbol under the WiFi settings.<sup>6</sup> When you are done browsing make sure you log-off any services you were signed into. Then, tell your device to forget the network.

#### **Back it up**

Before you leave your home make sure all your data and settings are backed up, at least then all you will lose is your hardware...<sup>7</sup>

#### **Get a mobile Firewall**

Use a 'travel router' that plugs into the ethernet jack of

<sup>5</sup> *Lifehacker.com: How to encrypt and hide your entire operating system from prying eyes.*

<sup>6</sup> *Lifehacker.com: The best browser extensions that protect your privacy.*

<sup>7</sup> *tabtimes.com: Security firm reveals the damage of lost & stolen mobile devices.*

### How phones are most commonly stolen

IDG Research and Lookout Mobile Security conducted a survey of 2,403 respondents who said they had their smart phone stolen at some point during 2014.



your hotel or business centre WiFi to create an instant, secure hotspot which can offer additional protection against malicious users connected to the same WiFi network. On many models you can specify a unique password as an additional safeguard.

Most laptops have a software firewall installed as standard but these can be disabled by viruses and other malicious software. Using your own wireless router adds a highly efficient layer of extra security.

### Stay up to date

Be sure that all devices are fully patched and up-to-date with security and system software and turn on the auto update feature for your installed apps.

### Lock it or lose it

If you have a portable computer consider investing in a good quality cable lock. A cable lock is a thin, steel rope that fits into a slot in your computer and can be securely locked around any solid object (like a wall bracket or metal pole). They can be cut through in time but it makes your computer a much less attractive target for an opportunistic thief than an unsecured one.<sup>8</sup>

According to Kensington, a manufacturer of computer locks, 40% of laptops are stolen from private offices. Just because you are at work doesn't mean you are safe.

### Most important of all

Keep your device with you, or in eyesight at all times! 

**One laptop** is stolen every **53 seconds**. **70 million** smart phones are lost each year, with only **7 percent** recovered.

**80 percent** of the cost of a lost laptop is from data breach.

Source:  
channelpronetwork.com

<sup>8</sup> *consumerreports.org: Smart phone thefts rose to 3.1 million in 2013.*

## Safer surfing for children

Children love computers and the internet, it's really that simple.<sup>9</sup> Many parents know their kids would be online all day if they were allowed and that's because all children see is the good stuff. Games, videos, cats, videos of cats, chatting to friends, cats, answers to any question you could possibly think of, made up celebrity gossip, pop music, Google Earth and, um, cats.

**One in five** 8 to 11 year olds and **seven in ten** 12 to 15 year olds has a social media profile. The ChildLine website received over **3.2 million visits** – **5 per cent more** than in 2013/14

<sup>9</sup> *Internetmatters.org:*  
*Helping parents keep their children safe online.*

Source: nspcc.org.uk

## Children who grow up with the internet believe everything they read online.

”

Ofcom,  
Children and Parents:  
Media and Attitudes report

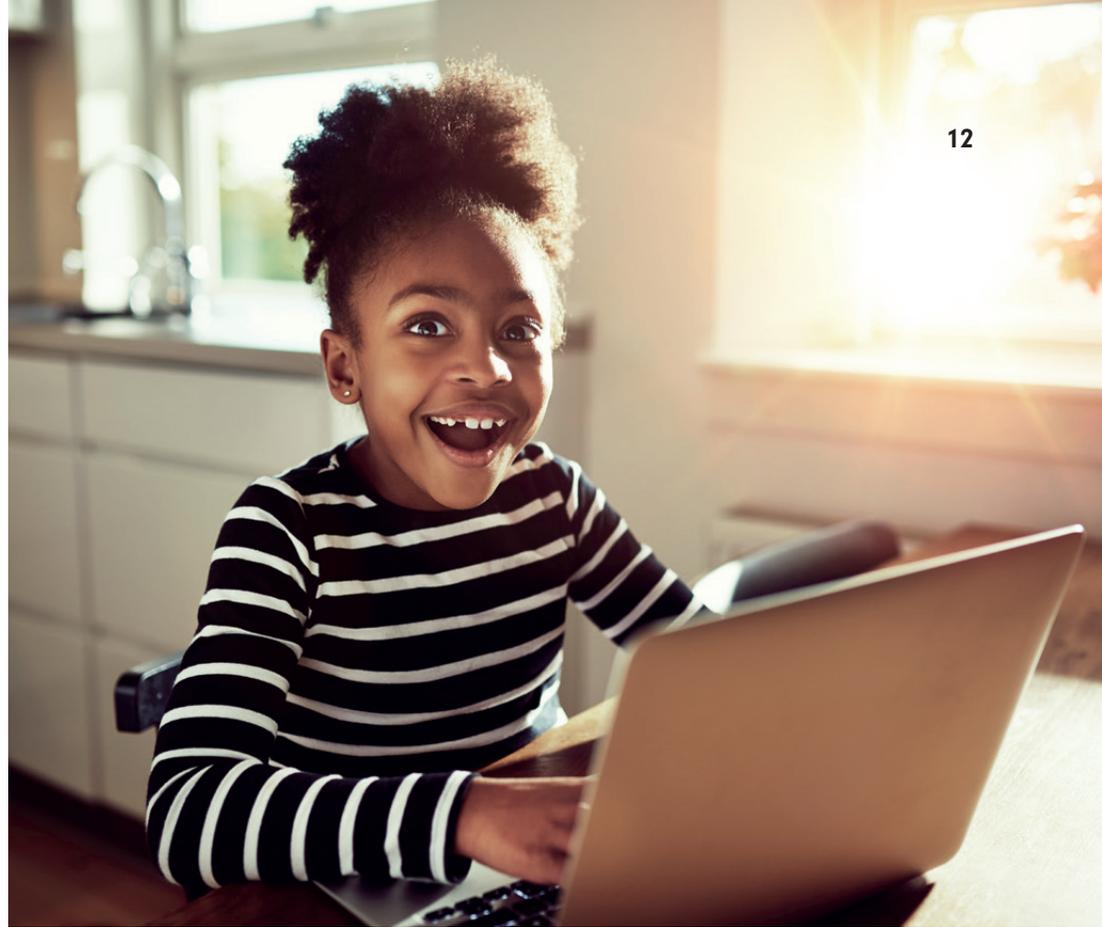
But like so many things in life it's what they don't know that is the danger. They have no idea about password security, trolling and 'netiquette', phishing, cybercrime, hacking and the myriad of other security and safety issues most adults take for granted.

The internet can be a wild and unregulated place, an environment totally at odds with the desire we all have to protect our kids, but one they can't wait to dive into, so where do you begin?

### **Control the environment**

All surfing applications come with safety settings, get to know them. There are also some powerful, dedicated software programmes available that can allow you to filter access to specific sites and programs, receive email alerts if restricted sites are viewed and even record keystrokes.

Many children probably don't need that level of surveillance but do some research to see what's available and use what's appropriate. But remember, no system can deliver 100% safety.



### **Stay together**

If your children are young never, ever, let them surf the net alone. You wouldn't take them to a new city and let them run free, in and out of strangers houses all day long would you? So don't leave them alone online, no matter how strong your security settings.

### **Have an honest conversation**

Most parents want to retain their children's innocence while still letting them have some freedom. It's a delicate balance but you can start to achieve it by having a genuine and open discussion about the dangers they could run into.



How direct you want to be is up to you, and depends, of course, on the child, but it's important to at least start to talk about the idea of inappropriate content and the existence of bad people.<sup>10</sup> You don't have to scare them, just try to prepare them with the basics before one of their friends or an older brother or sister tells them to do something silly.

#### **Train a mini 'security agent'**

Children are so often interested in the things their parents and older siblings are enthusiastic about so try to show them that being switched-on about digital security is for the smart kids.

Next time you have to update your system software or install a security patch, get your kids to do it with you and tell them *why* it's necessary and how it could help. Then when they have done it, congratulate them on being the families first ever digital security agent (you could even give them a codename).

Do some security investigating online together, show them how to create strong passwords, make a game out of it and tell them how much more grown-up and better prepared they are than other kids their age... and while you're doing it, you may even learn something yourself. 🕒

<sup>10</sup> *Thinkuknow.co.uk: Test your own and your children's knowledge of internet safety.*



## Better locks & smarter keys

Passwords are the keys to your digital world, we need them to access everything from bank accounts to email. They can be inconvenient, but they're vitally important if we want to keep our information safe. Here we discuss some ways you can secure your accounts by choosing better, stronger passwords.

**70%** of people do not use a unique password for each Web site. The **10,000 most common passwords** would have accessed **98% of all accounts**.

Source:  
[passwordresearch.com](http://passwordresearch.com)

## CYBERSECURITY FOR EVERYONE

### PASSWORD SECURITY

In **2015** the IRS got in big trouble for still using the password: **'password'** for many of their secure systems.

Source: [theguardian.com](http://theguardian.com)

Passwords are an easy to understand, simple to use and low cost security measure. They have become the standard way we manage our security online and the way we prove our identity, not only to the corporations we do business with every day but also to our friends and family when we communicate with them through email and social media.

In the days of, for instance, face-to-face banking, we would have relied on a combination of our signature, photo I.D., account number and, often, a personal familiarity with the member of staff behind the counter to validate who we are, in the internet age we are exclusively known by just two things; a user name and password.

And it's the success of this two factor procedure, user name and password, which has made the system so vulnerable. The fact that we need a password for every single account, profile, app and log-in, along side the requirement for increasingly complex passwords has led to what is commonly called 'Password Overload'.

The demand on most users is, quite frankly, unrealistic<sup>11</sup> and many users will cope by breaking the cardinal rules of password management; re-using passwords across multiple sites, using the simplest, shortest passwords they can and making their passwords childish and easy to guess<sup>12</sup> (see below).



#### How do passwords get hacked?

There are a number of common techniques hackers use to crack your passwords,<sup>13</sup> many of them rely on simple, easily available, pre-written software which you don't need any special skill to use. Having said that, there are also many ways we make ourselves vulnerable with poor password 'hygiene'.

#### Cracking your password:

Let's say you have a password for your favourite online shopping site; 'MySecurePassword'. When you enter it into

<sup>11</sup> [teamsid.com](http://teamsid.com): *Announcing Our Worst Passwords of 2015.*

<sup>12</sup> [passwordmeter.com](http://passwordmeter.com)  
[password.kaspersky.com](http://password.kaspersky.com):  
*Secure password checking sites.*

<sup>13</sup> [security.blogoverflow.com](http://security.blogoverflow.com): *Why passwords should be hashed.*

### 10 most common passwords of 2015

SplashData's fifth annual "Worst Passwords List" shows people continue putting themselves at risk.

RANK	PASSWORD	PREVIOUS RANK
1	123456	Unchanged
2	password	Unchanged
3	12345678	Up 1
4	qwerty	Up 1
5	12345	Down 2
6	123456789	Unchanged
7	football	Up 3
8	1234	Down 1
9	1234567	Up 2
10	baseball	Down 2

your account login page it isn't saved on the store database as 'MySecurePassword' it gets 'hashed'.

Hashing is a way of changing a password made up of standard words and numbers (called plaintext) into a random, seemingly meaningless string of jumbled text called a *hash*. The hash for 'MySecurePassword' is (let's say) Vxc5\$MnfsQ4iN\$ZMTppKN16y/tlsUYs/obHlhdP.Os80yXhTurpBMUba.

As you can see the hash doesn't look anything like the password, so if you could get hold of the hash for your account (which is surprisingly easy to do) your details would still be safe right? Wrong! All a hacker needs is that hash code string and some free software and they can reverse engineer your

password hash until they get 'MySecurePassword' back out. You don't have to be an international criminal gang member or a secret agent to do it... this is something that's done every day by 12 year old kids. Here's how:<sup>14</sup>

**With a dictionary attack:** A dictionary attack uses a programme that runs a database of millions of standard words, phrases, number strings, well-know sayings and combinations through the hashing software until it finds a match to the hash for your password, it does this over and over again, thousands of times a minute until the term 'MySecurePassword' produces the string 'Vxc5\$MnfsQ4iN\$ZMTppKN16y/tlsUYs/obHlhdP.Os80yXhTurpBMUba'. The use of a dictionary database speeds this process up considerably as most people use names, places, verbs, adjectives and nouns to create their passwords.

**With a brute force attack:** Similar to a dictionary attack but rather than trying known words and phrases to match the password hash the brute force attack will try *any and all* letters, numbers and special characters to try to break the code. Imagine a combination lock with a three number code, a brute force attack would try every possible combination in sequence, i.e: first 1-2-3, then 1-2-4 etc. It takes longer than a dictionary attack but it's very effective.

In **January 2010** Twitter banned **370 users passwords** for being too obvious. They included such terms as: '000000' 'letmein' 'aaaaaaaa' 'whatever' and 'stupid'

Source: trendhunter.com

<sup>14</sup> security.stackexchange.com: What are the differences between dictionary attack and brute force attack?meet five criteria.



**Cracking your security questions:** Many people use the names of family, pets, age, birth date, favourite colour/song/sport stars and celebrities as a basis for their passwords. If you have posted information about any of these on social media you are at risk of having your accounts hacked.<sup>15</sup> See the section: 'Using social media' in this file for detailed information of how this is done and what you can do to stop it.<sup>16</sup>

**Using simple passwords:** The worst thing you can do is to be among the users of the 10 most commonly used passwords (see page 1 of this article). Using passwords under 10

characters, without any combination of upper case letters, special symbols (like \*&^%\$£@) or numbers is putting your security at risk. One of the main reasons that we don't change our passwords to something much more complex and challenging is that nothing bad has happened to us... yet. Even if we get our email hacked mostly we just change *that* password and go on as before. Don't wait until real damage has been done to take action.

**Reusing passwords:** It's hard making and remembering a different password for your email, banking, social media and

<sup>15</sup> *slate.com*: In What City Did You Honeymoon? And other monstrously stupid bank security questions.

<sup>16</sup> *goodsecurityquestions.com*: Good security questions

### Know your hacker

You may have heard the terms black hat and white hat hackers but do you know the difference? It's all about ethics...

 <p><b>WHITE HAT HACKER</b> An ethical computer hacker who specializes in testing an organization's security systems.</p>	 <p><b>BLACK HAT HACKER</b> An individual with extensive knowledge whose purpose is to breach internet security.</p>
 <p><b>GREY HAT HACKER</b> Someone with an ambiguous ethical code and good hacking skills who is not malicious.</p>	 <p><b>HACKTIVIST</b> Hacks for political or moral reasons, often related to free speech and human rights.</p>

shopping but remember, if you use the same password for all of them then if one of these gets hacked they all do. Using one password for everything means you could lose it all.

### What can you do about it?

Nothing is impossible to hack but you can make cracking your security as hard as possible by following these 10 points:<sup>17</sup>

1. Make sure you use different passwords for each of your online accounts.

2. Consider using a password manager. They can generate, record, encrypt and store password information for all the websites you use and help you log into them automatically. Accessed with a master password it means you only have to remember one, secure password and the manager will do the rest.
3. Check the strength of your chosen code by using a reputable password strength analyser website.
4. Never enter your passwords into public or shared computers like Internet cafés or at the library.
5. Equally, never enter your password if you are using an unsecured, public Wi-Fi connection.<sup>18</sup>
6. Change your passwords regularly and don't ever reuse a password or base a new password closely on an old one (i.e. *SecurePasswordApril* becomes *SecurePasswordMay*).
7. Don't tell anyone your password. Ever.
8. Use at least ten characters of mixed lower case, upper case, numbers and special characters. Mix the numbers up with the other characters, don't string them all out together at the beginning or end of you password. Try to create your password with the maximum number of characters allowed by each site, the longer the better.
9. Never leave your device unattended and logged-in.
10. Make sure you are never watched when you enter any of your passwords. ●

It takes only **10 minutes** to crack a lowercase password that is **6 characters long**. Add two extra letters and a few uppercase letters and that number jumps to **3 years**. Add just one more character and some numbers and symbols and it will take **44,530 years** to crack.

Source:  
Stopthehacker.com

<sup>17</sup> [passwordday.org](http://passwordday.org) Password creation advice and information.

<sup>18</sup> [usa.kaspersky.com](http://usa.kaspersky.com): Public WiFi networks pose many security risks to users, but fortunately there are many tips to employ to stay safe and secure online.



## Be aware, stay secure

From organized criminal gangs to covert surveillance and even hacks by foreign nations criminal elements seem ever-present and ready to exploit any weakness in the new and emerging areas of communication and data storage. Most of us use the internet without any problems, but anyone can fall prey to cybercrime if they fail to take basic security precautions.

About **31.8 million** U.S. consumers had their credit cards breached in 2014, more than three times the number affected in 2013. UK identity fraud rose to **27 percent** in the first quarter of 2015 compared to a year earlier and now makes up **nearly half** of all reported fraud crimes.

Source: nasdaq.com

#### Do you know your Botnet from your Spywear?

Below is a list of some of the most frequently perpetrated types of illegal computer infiltration and missuse.

#### CYBERCRIME JARGON

##### Botnets

Infecting your computer and turning it into a remotely controlled 'slave' (known as a 'zombie') which can be used by a criminal gang to commit crimes on their behalf.

##### Pharming

Pointing you to a fake website by redirecting a legitimate URL.

##### Phishing

Fake emails, text messages and websites that appear to be from authentic companies but exist only to gather personal information (like passwords) from you or to get you to open links that will infect your system.

##### Ransomware

Ransomware is malware that encrypts (scrambles) all the data on your computer and displays a message that demands payment in order for your files to be restored to normal.

##### Spyware

Collects your personal information (passwords, browsing history etc) without you knowing. Often installed without your consent or knowledge when you download a file from the internet.

##### Trojan horse

Malicious software that is disguised as, or concealed within, a legitimate (or seemingly legitimate) program.

Activities that at first glance seem completely harmless – such as using email applications, searching the internet, downloading files, playing games and signing-up to new websites and services can all leave your computer or mobile device vulnerable to infection from viruses or spyware leading to data loss, identity theft and even serious fraud.

The best line of defence against becoming a victim of this kind of attack is to be as aware as possible of the tricks and techniques cybercriminals use to try and get access to your computer,<sup>19</sup> because the only way they can get in is if you let them.

Take a look at the box opposite to see some of the terms used to describe common types of cyber crime, you probably know some.

On the following pages we can examine some in detail so you can see how they work and what you need to do to avoid falling victim to them.

#### Gone phishing

*Phishing* is an attempt, usually through email, to gather personal information or to compromise technology for the purpose of financial gain or malicious activities. Phishing emails typically include a link to a fraudulent site or an attachment containing malware, clicking on the link or downloading the file will activate the program.

In 2015, there were **1,966,324** registered notifications about attempted malware infections that aimed to steal money via online access to bank accounts.

*Source:* securelist.com

<sup>19</sup> *getsafeonline.org: Protecting yourself and your computer.*



Every day millions of phishing emails are sent out to unsuspecting victims all over the world. Some are easy to detect as frauds but others are very convincing. How can you tell a real email from a scam? Below we have collected six ways you can spot a potential phishing email:

**1 The message has a suspicious or mismatched URL**

If you are at all suspicious check the integrity of any embedded URLs. The URL in a phishing message may seem to be perfectly valid but if you hover your mouse over the top of it you will see the actual hyperlinked address appear. If the hyperlinked address

is different from the address that is displayed, the message is probably fraudulent.

**2 The message has poor spelling or grammar**

When a major organisation sends out a message it's usually checked for spelling, grammar, and legality, if a message is filled with spelling mistakes it probably didn't come through a major corporation's legal department.

**3 It asks for personal information, especially passwords**

No reputable company will ever ask you to send or confirm

passwords or log-on details via email. Either the company already knows this Information or it's a scam, there are plenty of other ways they can confirm your identity.

#### **4 It lacks a personal greeting or any customised information**

Legitimate emails from banks, credit card company's and other security conscious organisations will often include partial account numbers or user names as forms of address. Greetings like 'Dear User' should ring alarm bells.

#### **5 It's an emergency**

Messages that say you must act now to avoid losing money or having your access cut off are usually trying to get you to act without thinking. Take your time and investigate, double check the hyper-link and use an alternative way (call a known number, pay a visit, go to the web page by typing it in manually etc) to contact the sender.

#### **6 Something just seems 'wrong'**

Maybe it's the slightly off logo or the odd way the message is worded but sometimes things just don't quite seem right, learn to trust that feeling. The truth is, the best defence we have against fraud is our common sense.

#### **If in doubt, throw it out**

The best thing to do, if you have any doubt at all about the legitimacy of an email, link or attachment is simply to delete it. Don't open it, forward it or save it to show someone later, it's much, much better to be safe than sorry.

So, phishing is the most common way a criminal can get you to infect your own computer or steal your private data. Once they have done that what else can they do? One thing might be to launch a ransomware attack:

#### **Digital hijacking**

*Ransomware*<sup>20</sup> is an increasingly popular method hackers are using to make money out of you. It's a kind of digital blackmail and it comes in two types:

#### **Lockscreen ransomware**

Locks your screen with an image demanding payment and displaying payment details.

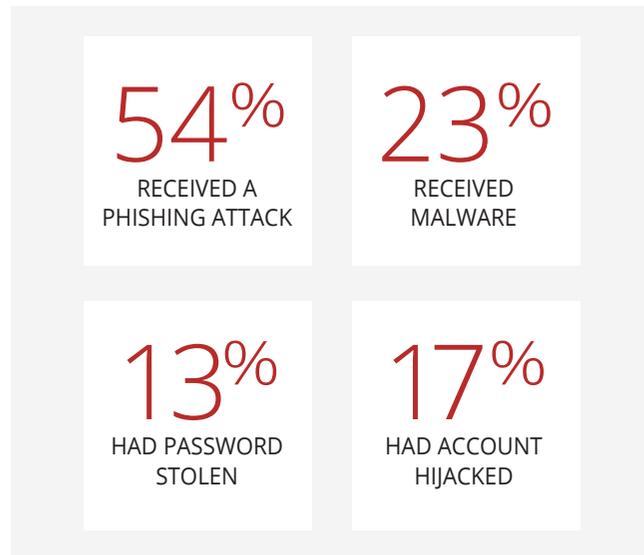
#### **Encryption ransomware**

Encrypts *all* the files on your system's hard drive (also on network drives, external hard drives, USBs, and even cloud storage), preventing you from opening them and demanding payment to regain access.

<sup>20</sup> *blog.trendmicro.com:*  
*Ransomware one of the biggest threats in 2016.*

#### Phishing on social media

Barracuda Networks surveyed users from 20 countries who revealed their experiences of security breaches and privacy issues while using social media.



Occasionally the ransomware virus will also send the user a message purporting to be from a law enforcement agency stating that illegal online activity has been detected and the payment is a fine to avoid arrest.

#### What you can do

There is no guarantee even if you do pay the ransom that you will ever get your files back. It's not like you can complain to anyone if the criminal doesn't keep their end of the bargain. It's also increasingly likely these days that the person contacting

you has simply bought a ransomware virus from a professional criminal programmer and doesn't even know how to restore your data to you, even if you did pay.

Legal threats are meant to scare and intimidate you, they don't come from law enforcement agency and have no legal authority. No police department would ever contact you like this.

You should face the fact that your data might be irretrievable although it's always worth seeking professional advice from a reputable computer specialist to see if your computer can be repaired and your data retrieved.

Keeping your most important and personal files backed up on a removable external storage drive is the only way you can be sure your data is safe.

#### Are you part of a zombie army?

A group of internet capable computers that have been infected by remote controlled robot programs called Bots to create a *Botnet*.<sup>21</sup>

Botnets are the silent hunters of the hacking world, each affected PC is known as a 'zombie' and is coordinated to act in concert with similarly infected computers to make an army under the control of a single master. You may be a zombie and not even know it.

Ransomware programs were detected on **753,684** computers of unique users; **179,209** computers were targeted by encryption ransomware.

Source: securelist.com

<sup>21</sup> *welivesecurity.com: Top 5 scariest zombie botnets.*

### How to tell if your computer is compromised

Just like people, when computers get sick they can start to behave strangely, use this list to see if your PC's health needs some serious investigation.

#### AN INFECTION CHECKLIST

The following checklist can help identify if you have a problem. You may have one, some or even all of the following:

- ✓ Unexpected pop-ups, which appear randomly, can be a sign of a spyware infection
- ✓ Programs seem to start running by themselves
- ✓ Your security software has stopped running
- ✓ It takes much longer than usual for your computer to start up, it sometimes restarts on its own or it doesn't start up at all
- ✓ Your computer display looks distorted
- ✓ It takes a long time to launch a program
- ✓ Files and data have disappeared or moved
- ✓ The system software is constantly crashing
- ✓ Your homepage has mysteriously changed
- ✓ You have unexpectedly run out of memory
- ✓ Files and data have been renamed
- ✓ Internet surfing and loading web pages is slow

If you think your PC is infected update your security software and run a full check. If you don't find anything or you're not sure what to do seek trustworthy, professional help.

Once the hacker has their Botnet in place they can use it to flood a Web site with requests for information, sending the same request over and over again from the army of computers, overloading the site and causing it to shut down (called a distributed denial-of-service - DDoS -attack). This kind of attack can be used to blackmail corporations by demanding money to cease the assault.

The other option for the commander of a zombie army is to use the infected network to send millions of spam emails and spread viruses and malware. All using your computer.<sup>22</sup>

#### What you can do

There are things you can do to reduce the likelihood of an attacker being able to hijack your system:

#### Wall of fire

Install a firewall and configure it to monitor and control traffic coming into and leaving your computer. You can set it up to alert you automatically if it senses an attack may be taking place.

#### Use email filters

Applying intelligent filtering criteria can restrict the amount and type of unwanted emails coming in to your mail application.

#### The 5 Worst Botnet Countries

As of Sept 2016

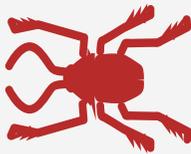
- 1 India: 2326660
- 2 Vietnam: 1009151
- 3 China: 796087
- 4 Iran: 651753
- 5 Pakistan: 458816

Source: spamhaus.org

<sup>22</sup> [uk.norton.com/botnet](http://uk.norton.com/botnet): Bots and Botnets—A growing threat.

**The big three nasties**

Viruses, worms, horses? By naming these things after real creatures we try to emphasise; look, they act like they are alive, don't ignore them, they're dangerous...



**Computer Virus**

A malicious computer program often sent as an email attachment or a download with the intent of infecting your computer. Often used to provide criminals with access to your computer, scan for personal information like passwords, hijack your web browser and trash your security.



**Trojan Horse**

Disguised as, or hidden within legitimate software a Trojan horse is an executable file that installs itself and runs automatically. Once it's established it can delete or copy your files, watch you through your webcam or keep a record of all your keystrokes.



**Worm**

A worm works on its own without attaching itself to your files or programs. It hides in your computer memory and sends itself to other computers in a network or over the Internet. Their incredible replication rate can be a threat not just to individuals but to the internet itself.

Over **27 million** Americans have fallen victim to identity theft over the past five years. **9 million** of them found their identities stolen in the last year alone.

**Source:**  
stopthehacker.com

**Be watchful**

If you notice that your Internet connection is very slow, use a system tool to check the amount of traffic your modem is handling.

If it seems very high and you are not downloading or uploading anything, that might well indicate you are part of a Botnet.<sup>23</sup>

**Trusting Technical Support**

Some fraudsters will even impersonate your internet service providers' technical support department. They will tell you they need you to give them remote access to your computer so they can remove malicious files or software they have identified.

If you haven't contacted your internet service provider or computer help desk you can be sure that an offer like this is fraudulent.

**How the scam works**

Hackers use your Internet Protocol (IP) address to identify your Internet Service Provider. Once they know who supplies your broadband connection it is a simple matter for them to pretend to be legitimate technical support from that company.

The fraudulent technician convinces you, either by communication windows on your screen or via a phone call, that they need to take control of your machine in order to delete infected files from your system. If you give them access they will instruct you to make a payment to remove the allegedly malicious files.

**What you can do**

Never give remote access to anyone you haven't specifically requested to work on your machine.<sup>24</sup>

<sup>23</sup> *f-secure.com: A quick guide to botnets - what they are, how they work and the harm they can cause.*

<sup>24</sup> *moneysavingexpert: 30 ways to stop scams.*

## CYBERSECURITY FOR EVERYONE

### CYBER CRIME

**Cramming** is the addition of charges to a subscriber's telephone bill for services which were neither ordered nor desired by the client, or for fees for calls or services that were not properly disclosed to the consumer.

Source: en.wikipedia.org

Ignore the technical support window, close it and/or put the phone down. Call your Internet service provider directly using a number you are familiar with or have used before and explain the situation.

If you have allowed remote access your system is probably compromised. If that's the case you should disconnect the device, reinstall your operating system or take it to a reputable computer support service to have the system reinstated. Keeping thorough backups of your data will greatly help here.

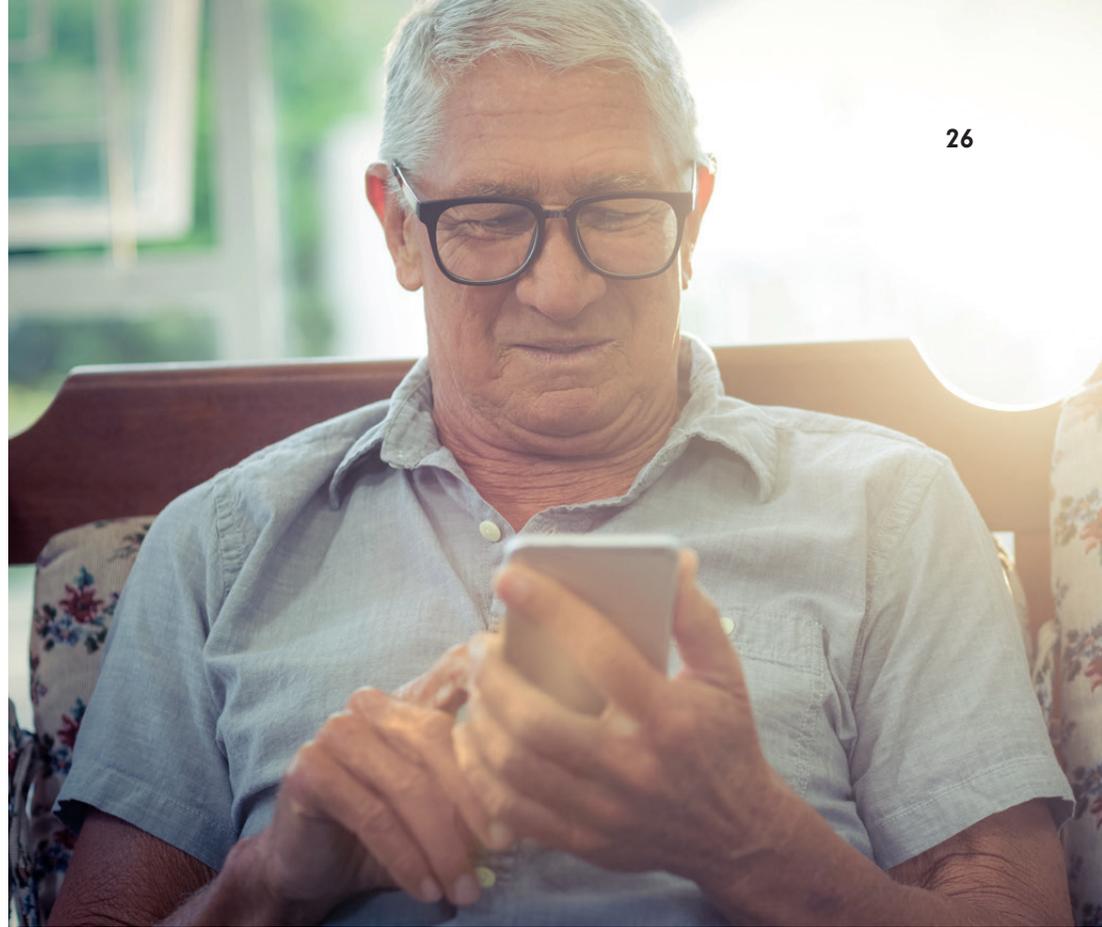
#### Fraudulent phone calls

It's not just 21st century, cutting edge technology that cyber criminals use to get hold of your security information, the telephone is as popular with criminals now as it has ever been.<sup>25</sup>

Known as *vishing* (voice-phishing) fraudsters will call and pretend to be from your bank, to warn you of suspicious activity in your account, your cable company or even from the police force claiming you've been the victim of credit card fraud. All with the aim of relieving you of your account details and passwords.

#### Be particularly vigilant if:

Someone calls to tell you your card has been used fraudulently. A caller suggests you hang up the phone and call them back to



verify they are genuine; criminals can keep your phone line open by not putting down the receiver at their end making it seem you are through to the security number you dialled. Someone asks you to transfer money to a new account, even if they say it will be in your name.

#### What you can do

Never feel pressured into doing something that makes you feel uncomfortable. If something seems wrong stop and take a moment... And never be afraid to just put the phone down, be polite, but be firm. ●

<sup>25</sup> *bbc.co.uk: Caught on tape: How phone scammers tricked a victim out of £12,000.*

CYBERSECURITY FOR EVERYONE  
WORKING TOGETHER



## Working together

Employers these days are more and more dependent on their information systems, gathering, storing and using ever increasing amounts of data. They have a responsibility to their staff to be open and honest about what kind of material is being collected and how it's being stored, while employees have a responsibility to ask; how can we all help to keep our data secure?

According to the Shred-it/ Ipsos Reid Information Security Tracker **47%** of respondents say they have both locked consoles and use a professional shredding service to shred sensitive documents but **46%** do not have anyone directly responsible for secure information destruction

Source: shredit.com



## CYBERSECURITY FOR EVERYONE

### WORKING TOGETHER

In 2015 third parties with trusted access were responsible for **41%** of the detected security incidents at financial services organizations. **62%** of security incidents at industrial product organizations involved a current or former employee.

Source: pwc.com

We all have the right to work in an environment that is safe and secure, both physically and digitally. Creating that kind of culture isn't just down to adhering to local government guidelines or departmental policies, it's a state of mind.

#### Balancing the risk

Wherever there are people there will be risk, that's just how it is but there is, and always must be, a balance between risk and freedom.

If you can't keep your data safe then you're not a fit company to do business with, but you need to make sure that the security processes put in place are there to help, not hinder.<sup>26</sup> Knowledge must be able to flow, you need to be able to respond to situations in a fluid way... It's a balance. Here are some of the ways we can protect our data, our customers and each other.

#### Passwords

Don't tell anyone your work passwords, under any circumstances, ever. And that means not writing it down on a sticky note and attaching it to the front of your PC, OK? For more information see our section on Passwords.

#### Email

We've all done it, it sounds obvious (it *is* obvious) but that doesn't stop thousands of us doing it every day - try *really hard*



to make sure that you are sending your email to the right person.

Sending confidential or sensitive information out to someone we shouldn't is one of the top ways we can embarrass ourselves and put our company at risk. Just take a moment to consider if the email should be encrypted and double check the recipient before hitting 'send'.

Also, don't use your work email for anything other than work; you'll just get your in-box full of spam and increase the likelihood of a phishing attack (see the 'Cybercrime' section of this file).

<sup>26</sup> *inspire-success.com*:  
IT Security in the Workplace  
our TOP Twelve Tips

**Virtual world, physical security**

Keeping your companies data out of criminal hands isn't restricted to smart thinking in the virtual world, there are things you can do in the real world too.<sup>26</sup>

**REAL WORLD SECURITY**



**See something, say something**

If your company has a pass system or issues ID badges then the chances are you have a security department too. If you see someone without a badge or you spot anything unusual try to get in the habit of reporting it. You don't have to confront anyone directly, just let someone know you're concerned. Criminals are counting on us being too shy to say anything, prove them wrong.



**Clean and tidy**

Treat all your printed materials with the same level of security as your digital ones: Keep your desk clear of sensitive papers when you are away from it, lock documents away at the end of the day and make sure you don't leave anything confidential on the photocopier or printer.

When you have finished with a print-out don't throw it away, shred it.



**Keep it to yourself**

Don't give out your personal or confidential details to anyone you don't know, either over the phone or on an email, unless you're sure about the person or company asking and why they want to know. And try not to mention any confidential work details in a public place, or online, you never know for sure who's listening...

**Lock your screen**

Whenever you leave your desk put your computer into sleep mode or activate the screen lock. That way, if someone wants to see what you've been working on they need your password (as long as it's not written on a piece of paper on the underside of your keyboard).

**Taking work home**

Check your organisations' policy on taking business files home. If it's allowed, make sure you encrypt the data before you remove it or put it on a password protected drive so if it gets lost the information is still protected.

**Report Lost or Stolen Devices**

If you do lose anything with work related data on it, make sure you let the relevant department know as soon as possible. As awkward as it may be to admit it will be far, far worse if sensitive information gets into the wrong hands and your company is unprepared.

**Think before you click**

Be very cautious about downloading anything from the internet onto your work computer, especially 'executable' (.exe) files. It's almost impossible for you to tell if a file is what it says it is or if it's really harbouring a virus waiting to infect your business' system.

**Patient information is like radioactive material, it must be protected, It must be contained. Take it seriously.**



Arthur R. Derse, MD,  
Bioethics Centre, USA

**CYBERSECURITY FOR EVERYONE**  
**WORKING TOGETHER**

30



**Engage with InfoSec**

If your company has an IT or Information Security department go and see them. Ask what they are doing to keep your data secure and what you can do to help, find out who you need to contact if anything goes wrong so you're ready. Don't forget, InfoSec are here to help you, one of them even wrote this book.

There is, perhaps, a tendency to think of them as, at worst, an enemy and at best an inconvenience but please try to remember; they are dealing with a brand new threat in a brand new environment.

We are the first society in history who has to deal with the dangers and the possibilities of the internet, it's new for all of us. Some of us are more comfortable with the changes it's bringing, others less so.

But, ultimately, this is the digital age,<sup>27</sup> it used to be enough to make sure the windows were locked and the alarm turned on at night when you left work but it's not just money and equipment that can be stolen now, a business that loses it's data can lose its customers, its reputation, everything. It's a 21st century workplace, let's engage with it together. 🗨️

<sup>27</sup> *cio.com: We All Work In  
Information Security Now*





## A little effort goes a long way

**The internet... it's not the Wild West, it's not the Haunted Forest, there aren't trolls under every bridge and bandits in every canyon. What we've just been talking about are some of the worst case scenarios so please, don't close this book and swear never to go online again, just put some effort into thinking about and updating your security. We promise it's time well spent.**

In quarter 1 (Jan to Mar) 2015, **86% of adults (44.7 million)** in the UK had used the internet in the last 3 months (recent users), an increase of 1% point since the quarter 1 (Jan to Mar) 2014 estimate of 85%. **11% of adults (5.9 million)** had never used the internet, falling by 1% point since quarter 1 (Jan to Mar) 2014

Source: ons.gov.uk

Following a few sensible procedures will greatly reduce your chances of ever being the victim of cyber crime or identity theft.<sup>26</sup> Many criminals are looking to do the least possible work to get the maximum gain. In just the same way a household that leaves its front door and windows open is far more likely to be robbed than one that's sensibly locked, a computer or account protected by a few smart security procedures is a much less attractive target to a hacker than one without. The lesson is: let's not make it easy for them...

#### **Protect your devices**

Keeping your operating system, apps and web browser up to date is one of the easiest and most effective things you can do to keep safe.

Make sure you turn on the *automatic update feature* to get the latest versions of operating systems and security patches.

#### **Protect your data**

Use intelligent passwords and keep different passwords for separate accounts - check the '*Password Security*' section of this book for more.

Only send information over a secure connection, look for the **https://** or **padlock icon** in the address bar when you are

sending any sensitive information like credit card details. If you do access password protected accounts or sites on a public or shared computer remember to sign out and close the browser window when you're done.

Install some protective software, preferably a security suite which includes antivirus/malware and firewall components.

#### **Don't share too much**

Think about how you use social media; set privacy and security settings and consider what a criminal could do with the information you post. See the '*Using Social Media*' pages.

#### **Don't get hooked**

Beware of phishing; links in emails, tweets, bogus websites and too-good online offers are all ways hackers will try to steal your personal information. Learn to be suspicious and don't be afraid to delete something if it feels 'off'. Read more in our '*Cyber Crime*' chapter.

#### **Back it up**

It might sound annoying but regularly backing up all your irreplaceable photos, work files and other digital information onto a removable drive will ensure they are protected, no matter what happens to your hard drive or cloud account.

**Dear internet user,  
someday you  
will really  
regret not  
reading me.  
Sincerely,  
terms &  
conditions..**

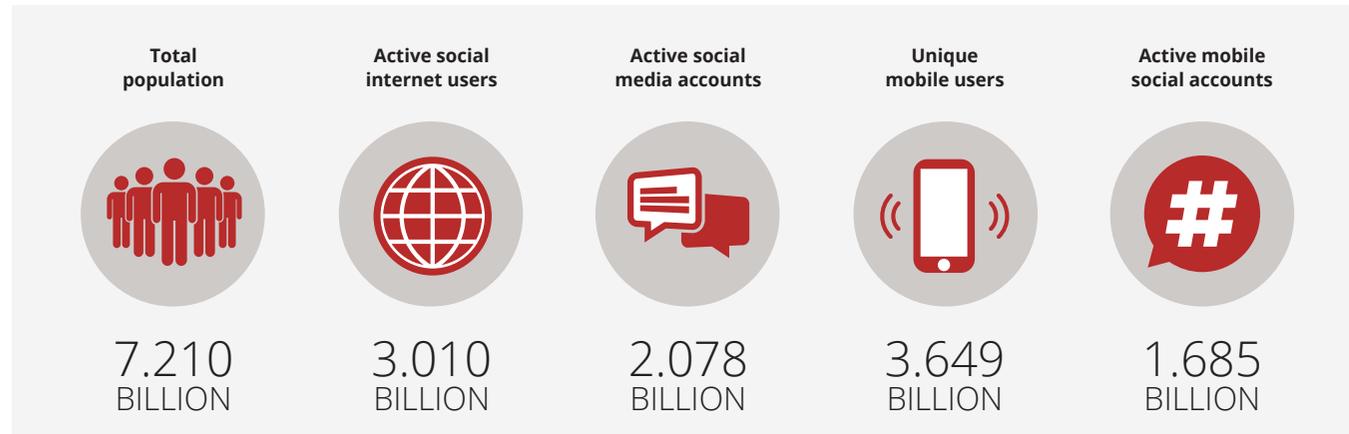
”

Unknown user,  
Facebook.com

<sup>26</sup> *staysafeonline.org*: National cyber security alliance share their tips and tricks for staying safe.

### A virtual world snapshot

Almost 42% of the world's population has access to the internet since January 2015, *Wearesocial.net* produced a snapshot of digital usage for the World in 2015.



### Be prepared

If the worst happens, have a plan. Keep a real, pen and paper copy of the emails, phone numbers and addresses of your friends and contacts in case your identity and accounts are compromised. Make sure you know the correct numbers to cancel credit cards and freeze bank accounts and find out the names and numbers of the relevant fraud or law enforcement departments so you can limit the amount of time a criminal has free access to your finances.

### Think before you act

Many scams rely on us being too eager to take advantage of a super special, one-time-only, limited, low price offer. These too-good-to-be-true frauds often hide a malicious intent. Try to learn

how to see through them. Read about how others have been scammed and what tipped them off, remember, we'd all like a free holiday and an iPad but the chances of getting one by filling in an online form are non-existent. It's a scam.

### Lastly...

Just because the online world is digital doesn't mean it's not real.<sup>27</sup> It's made up of real people with real lives and feelings.

It can be easy and exciting to get swept along with the crowd sometimes but what happens online matters and can have genuine and lasting effects on everyone involved. Always treat others as you would like to be treated. Be kind, be aware and stay secure. Thanks for reading. 

<sup>27</sup> *youtube.com: How does the internet work?*



**THE END.**

© FIL Limited 2017.

Information contained in this booklet has been obtained by Fidelity International from public sources. Care has been taken by the staff of Fidelity International in compilation of the data contained herein and in verification of its accuracy when published, however the content of this booklet could become inaccurate due to factors outside the control of Fidelity International and this booklet should, therefore, be used as a guide only.

This booklet is published and distributed on the basis that Fidelity International is not responsible for the results of any actions taken on the basis of information contained in this booklet nor for any error in or omission from this booklet. Fidelity International expressly disclaims all and any liability and responsibility to any person in respect of claims, losses or damage, either direct or consequential, arising out of or in relation to the use and reliance upon any information contained in this booklet. Fidelity International means FIL Limited and/or its subsidiaries.

