



Cybersecurity for everyone.

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





INTRODUCTION	2-3
Welcome to this book, from Fidelity International Information Security.	
USING SOCIAL MEDIA	4-7
Think about what information you put on social media and who can see it.	
MOBILE DATA SECURITY	8-11
How to keep your mobile device safe and your data secure on the move.	
KEEPING KIDS SAFE	12-13
Protect and support children as they discover the online world.	
PASSWORD SECURITY	14-19
Some tools and ideas for creating and managing good, secure passwords.	
CYBER CRIME	20-29
New forms of communication mean new types of crime, be aware.	
WORKING TOGETHER	30-33
What to expect from Information Security at work and why it matters.	
STAYING SAFE	30-31
A round up of our top digital security tips and techniques.	



Cybersecurity for everyone

At Fidelity International, we believe cybersecurity is a crucial part of how we operate our business. With our customers at the heart of everything we do, it's vitally important that we ensure our cyber defences are as good as they can be to protect the information entrusted with us.¹ This is just as important in our personal lives as it is at work.

This guide contains key information on the importance of cybersecurity awareness along with simple and effective tips to help keep you safe in an increasingly digital and online world. With many of us continuing to adapt the ways we work, from home as well as in the office, we need to be vigilant and aware of existing and new threats not only for ourselves, but for our colleagues, friends and family too.

and friends, providing help and advice for staying cyber safe at home, online and on the move.

Thanks for reading - stay safe and stay secure.

Stuart Warner
HEAD OF TECHNOLOGY
Fidelity International

With this in mind, we have produced this guide for you to share with your family



¹www.fidelity.co.uk: How Fidelity protects you and how you can protect yourself.

Take care what you share

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

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.

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'², 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.

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.



²Mashable.com: 10 People who have lost their jobs over social media mistakes.

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

³identity.utexas.edu: How to manage your social media privacy settings.

⁴pleaserobme.com: Raising awareness about over-sharing.

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.³

Try not to let the world know exactly where you are every minute of the day

Telling everyone where you are at all times also lets 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 is to turn up to your home uninvited and steal your stuff.⁴

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 year's time (or even in the morning...).

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'.



“
What happens on social media stays on Google, forever.
”

YourSocial.com

Know who your friends are

It can be exciting to build up a big list of 'friends' but how well do you know them? If you trust them like your family then by all means share everything. Would you, for instance, let them into your house? 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.

Digital security to go

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

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.

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.⁵

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.⁶ When you are done browsing make sure you log-off any services you were signed into. Then, tell your device to forget the network.

⁵Lifehacker.com: How to encrypt and hide your entire operating system from prying eyes.

⁶Lifehacker.com: The best browser extensions that protect your privacy.





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.



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

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...⁷

Get a mobile Firewall

Use a 'travel router' that plugs into the ethernet jack of 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.⁸

Most important of all

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

⁷tabtimes.com: Security firm reveals the damage of lost & stolen mobile devices.

⁸consumerreports.org: Smart phone thefts rose to 3.1 million in 2013.

Safer surfing for children

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

Source:
nspcc.org.uk

Children love computers and the internet, it's really that simple.⁹ 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.

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 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.¹⁰

Train a mini 'security agent'

Next time you have to update your system software or install a security patch, get your kids to do it and tell them *why* it's necessary. Show them how to create strong passwords and do some security investigating online together. You may even learn something yourself.



Better locks and smarter keys

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

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.

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, alongside the requirement for increasingly complex passwords has led to what is commonly called 'Password Overload'.

The demand on most users is, quite frankly, unrealistic¹¹ 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 guess¹² (see below).

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

¹¹teamsid.com: Announcing Our Worst Passwords of 2015.

¹²passwordmeter.com password.kaspersky.com: Secure password checking sites.



“ Treat your password like your toothbrush. Don't let anybody else use it, and get a new one every six months... ”

Clifford Stoll, Astronomer, author and pioneer of digital forensics



How do passwords get hacked?

There are a number of common techniques hackers use to crack your passwords,¹³ 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 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:¹⁴

With a dictionary attack: A dictionary attack uses a programme that runs a database of millions of standard words, phrases, number strings, well-known 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, e.g. first 1-2-3, then 1-2-4 etc. It takes longer than a dictionary attack but it's very effective.

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

Source: theguardian.com

¹³security.blogoverflow.com: Why passwords should be hashed.

¹⁴security.stackexchange.com: What are the differences between dictionary attack and brute force attack?

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...

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

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

without any combination of upper case letters, special symbols (like *&^%\$£@) or numbers is putting your security at risk.

Reusing passwords: It's hard making and remembering a different password for your email, banking, social media and 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:¹⁷

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.
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.

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.¹⁵ See the section: 'Using social media' in this booklet for detailed information of how this is done and what you can do to stop it.¹⁶

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,



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

¹⁷passwordday.org Password creation advice and information.

¹⁸usa.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.

5. Equally, never enter your password if you are using an unsecured, public Wi-Fi connection.¹⁸
6. Change your passwords regularly and don't reuse a password.
7. Don't tell anyone your password. Ever.
8. Use at least ten characters of mixed lower

- case, upper case, numbers and special characters. Use a password with the maximum number of characters allowed.
9. Never leave your device unattended and logged-in.
10. Make sure no one watches when you enter your passwords.

Be aware, stay secure

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

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.

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;¹⁹ 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 cybercrime, you probably know some already.

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.

Cyber crime jargon explained

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.



¹⁹getsafeonline.org: Protecting yourself and your computer.



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.



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.

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 companies and other security conscious organisations will often include partial account

“ Hackers have breached internet connected camera systems, smart TVs, and even baby monitors. ”

Molly Wood, New York Times



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

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

Ransomware²⁰ 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.

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

²⁰blog.trendmicro.com: Ransomware one of the biggest threats in 2016.

How to tell if your computer is infected

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.

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

Source: securelist.com

²¹welivesecurity.com: Top 5 scariest zombie botnets.

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?

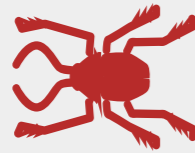
A group of internet capable computers that have been infected by remote controlled robot programs called Bots to create a *Botnet*.²¹

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

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



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 disable 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 is established it can delete or copy your files, observe you through your webcam or keep a record of your keystrokes (like credit card details you enter online).



Worm

Unlike a virus 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 exponential replication rate can be a threat not just to individuals but to the internet itself.

similarly infected computers to make an army under the control of a single master. You may be a zombie and not even know it.

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.²²

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.

Use email filters

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

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.

²²uk.norton.com/botnet: Bots and Botnets—A growing threat.



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

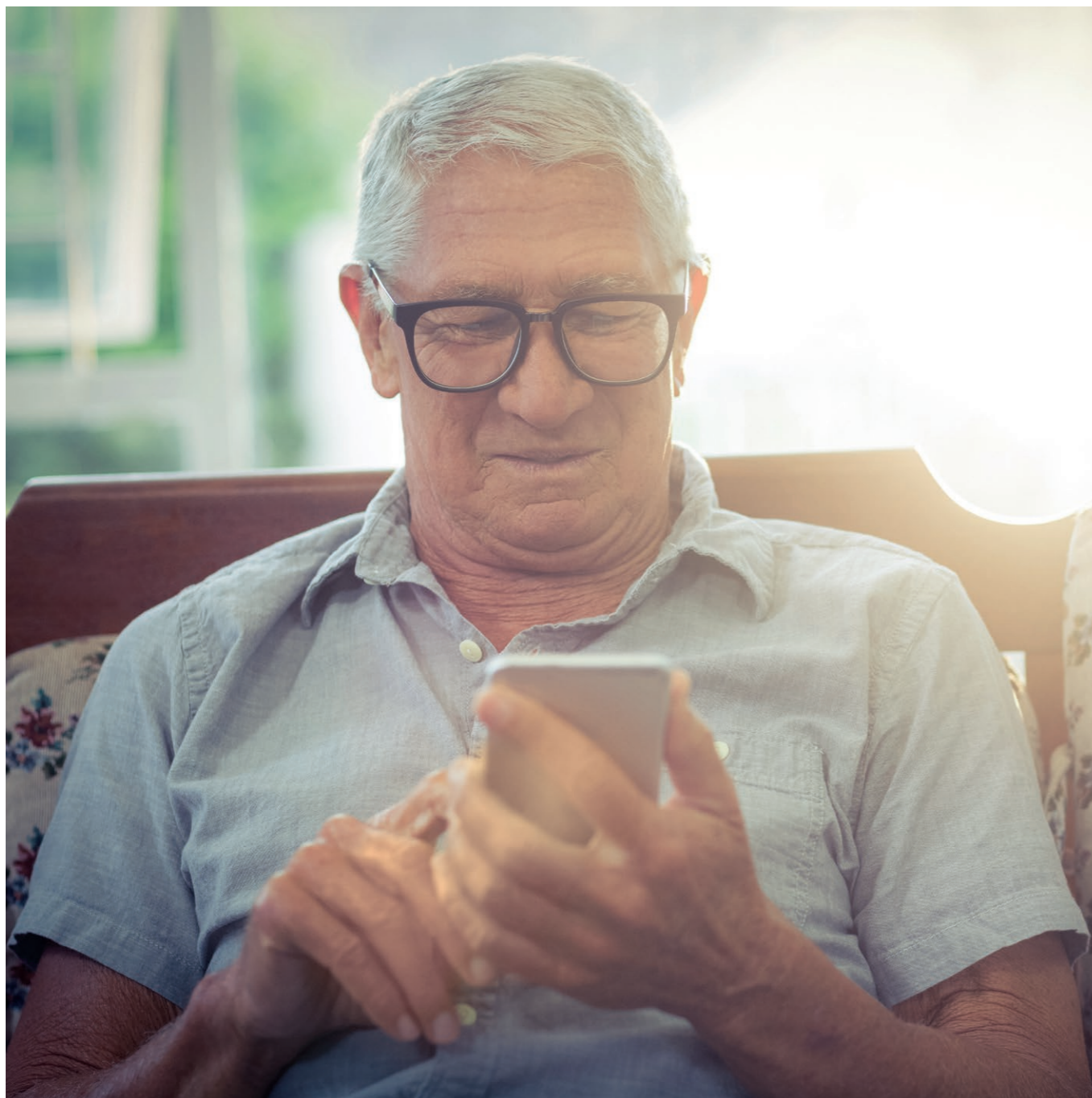
If it seems very high and you are not downloading or uploading anything, that might well indicate you are part of a Botnet.²³

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.

²³f-secure.com: A quick guide to botnets - what they are, how they work and the harm they can causes.



How the scam works

When you are online 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 a legitimate technical support worker 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.²⁴

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.²⁵

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.

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

²⁴*moneysavingexpert:*
30 ways to stop scams.

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

Working together

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

With the increase in financial crime it's just as important to be vigilant in the workplace. Employers are increasingly dependent on information systems; gathering, storing and using ever growing amounts of data. They have a responsibility to be open and honest about what kind of material is being collected, and how it's being stored, but everyone needs to ask - how can I help to keep that data secure?

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.²⁶ 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 you can help protect your data as well as your company, customers and colleagues.

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 (pg14).

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 'Cybercrime' pg20).

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 taped to the underside of your keyboard of course).



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.

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 nasty virus waiting to infect your business’ whole system.

Real World Security

The practice of 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.²⁶



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...

Source: pwc.com

²⁶getsafeonline.org: Physical security is just as important as online security



“ Patient information is like radioactive material it must be protected. It must be contained. Take it seriously. ”

Arthur R. Derse, MD, Bioethics Centre, USA

²⁷cio.com: We All Work In Information Security Now

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 protect the company. And find out who you need to contact if anything goes wrong so you are ready.

This is the digital age,²⁷ 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 its data can lose its customers, its reputation, everything. It’s a 21st century workplace, engage with it.

A little effort goes a long way

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 percentage point since quarter 1 (Jan to Mar) 2014

Source: ons.gov.uk

²⁶staysafeonline.org: National cyber security alliance share their tips and tricks for staying safe.

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.

Following a few sensible procedures will greatly reduce your chances of ever being the victim of cyber crime or identity theft.²⁶ 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

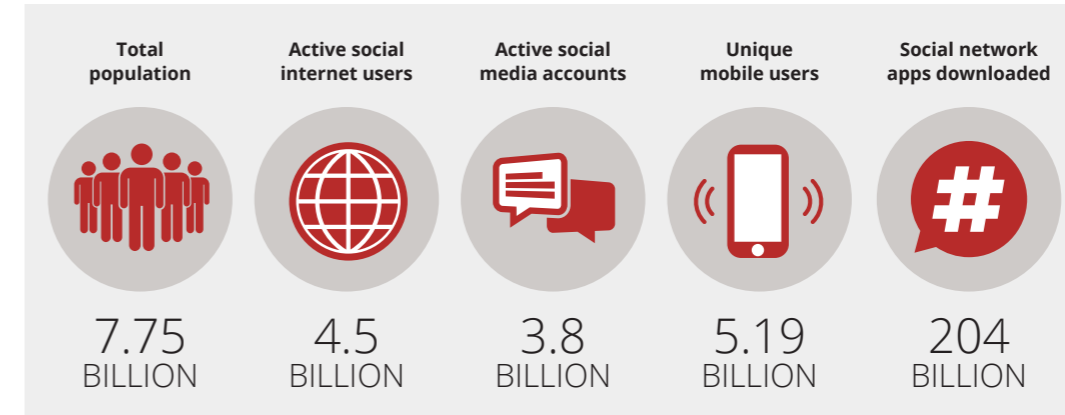
Think about how you use social media; set privacy and security settings and consider what a criminal could do with the information you post. See the 'Using Social Media' pages.

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.

Digital, Social and Mobile in 2015

Almost 42% of the world's population has access to the internet in January 2020, wearesocial.com crunches the numbers to produce a snapshot of digital usage for the World's population at the start of 2020.



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.

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.²⁷ It can be easy to get swept along with the crowd but what happens there matters and can have a lasting effect. Always treat others as you would like to be treated. Be kind, be aware, stay secure.

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

Unknown, Facebook.com

²⁷youtube.com: How does the internet work?



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.

© FIL Limited 2020.

