THE ULTIMATE CYBERSECURITY GUIDE

CONQUER

THE WEB

THE ULTIMATE CYBER SECURITY GUIDE

CONQUER
THE
WEB

Legend Business Ltd, 107-111 Fleet Street, London, EC4A 2AB
info@legend-paperbooks.co.uk | www.legendpress.co.uk

British Library Cataloguing in Publication Data available.

Print ISBN 9781787198623
Set in Times. Printing managed by Jellyfish Solutions Ltd
Cover design by Tom Sanderson | www.the-parish.com/

Publishers Note
Every possible effort has been made to ensure that the information contained in this book is accurate at the time of going to press, and the publishers and authors cannot accept responsibility for any errors or omissions, however caused. No responsibility for loss or damage occasioned to any person acting, or refraining from action, as a result of the material in this publication can be accepted by the editor, the publisher or any of the authors.

RISKS OF THE DIGITAL AGE

by

Nick Ioannou

Founder of Boolean Logical Ltd

1

DATA COLLECTION

The incredible growth of the internet

The incredible growth of the internet over the past 20 years has seen a gigantic leap in how we communicate, consume information and interact with each other. Old boundaries of countries are pretty meaningless in our digital lives and the devices we use have shrunk to the point where we can have them with us 24/7. In the 80s you could count the number of TV channels on one hand. You had to buy a newspaper if you wanted to read it and doing any form of research meant visiting the library. Compare that to now, where we all can freely communicate with each other and source our information not just from official media channels and trusted sources, but from social media platforms, companies, pretty much anyone and anywhere. But the truth is, it is not free, we must give the gatekeepers personal information about ourselves to access many of these systems, information that if it falls into the hands of criminals can be used for identity fraud, theft and extortion.

Currently there are over 60 social media / social networking and messaging systems; some are more popular in certain countries like China, while others are actually owned by mainstream social media giants. For instance, Facebook also owns WhatsApp and Instagram, Microsoft owns LinkedIn, and Google owns YouTube. And because of this, data can be shared between the parent company and the social media platform they bought, which in many cases was the whole point of buying them for the data in their customer user profiles.

Personal data

We think nothing of giving up our title, name, address, date of birth, gender, mobile number and email address in order to use an online service, and quickly scroll to the end of the terms and conditions acceptance page, without reading any of it, to click Accept. It's not as if reading it will really make any difference! You cannot say 'I agree to this bit, but not that bit'; it's an all or nothing choice, and you have probably decided to use the service because everyone else you need to communicate with is already using it. Laid out in those long terms and conditions it clearly states what information they will collect, and the fact that they may use it to sell targeted adverts and build a detailed profile of you. In effect you are paying for the 'free' basic service with your personal data.

When George Orwell wrote 1984, he never envisioned us carrying the telescreens in our pockets, complete with location tagging as well. We post pictures of ourselves, our children, our friends and family, especially pets, and even our food, and each picture may include geo tagging location information as well as the date and time the picture was taken. We also give information on our schools and education, our hobbies and pastimes, our cars, where and what we are doing and who with. Every like, every message, every advert clicked, every purchase within the platform, it all goes into building a profile of you. However, that is not all. If I give you half the pieces of a jigsaw puzzle, while you cannot finish it, you can definitely have a good idea of what the image is about after spending a couple of hours trying to solve it. The same applies to your profile, there are enough pieces of the puzzle to allow these companies to fill in a lot of the gaps and make some good guesses about the rest.

Of course, the trick is we don't really realise just how much information we are giving away, because it happens over time in subtle ways, like when we post something innocently like a 'thanks mum you're the best' on social media. Nothing wrong with that is there, except you may have just helped a criminal work out your mother's maiden name. You see, cyber criminals love social media, because it takes all the guesswork out of who to target and gives them hooks to easily create believable emails and messages based on the information we have posted. It's quite easy to fake an email; all you need is a genuine copy of the email from a particular company or service and you have everything you need to replicate it. Even if you don't have a genuine email to start with, there is enough imagery and text on nearly every major company's website to build a convincing fake. However, if that fake email is asking you to update your credit card details or security questions, or open an attachment for a refund, you could unwittingly become a cybercrime statistic.

The thing is that cybercrime is now part of organised crime. It is massively profitable, heavily resourced, with little chance of getting caught as most of the crimes are committed by criminals in other countries. The skill levels required to be involved in cybercrime has also plummeted as criminals sell online services to other criminals. Plus, there are the huge database breaches/ hacks that gave the criminals a massive head start from the Yahoo breach in 2013, Uber in 2016 and Equifax in 2017. Regularly updating your passwords is the best way to reduce the value of these hacks, but this means really changing your passwords, not just adding a 1 at the end. The fact is, it’s not just emails and passwords the criminals have, they may also have your mobile number. If you receive text message updates from your bank, save the number and call it something you recognise. That way if you receive a fake bank message, you’ll be suspicious immediately.

Useful online advice

But not all data hacks are due to criminals. The data analytics firm Cambridge Analytica, which has been accused of harvesting millions of Facebook profiles without permission, did so apparently via a personality app called “thisisyourdigitallife” that utilized a developer feature called Facebook Login, so people wouldn’t have to create a username and password to sign in, but use their Facebook account instead. And when they agreed to use Facebook Login, they also agreed to give access to their Facebook profile and friends list. So not only did the people give extra information about themselves as part of the personality test, they also handed over a lot more information than they expected to. A similar trick is the online survey, often for a voucher or prize draw, and may contain brand logos despite having no connection whatsoever to those brands. Just because it says you’ll receive a £100 worth of Tesco vouchers, it doesn’t mean it’s genuine, or will arrive in the form of a £10 off voucher when you spend £100 and just give you 10 vouchers. So please be wary of online surveys, quizzes and personality tests, firstly for the questions they may ask and also for the additional access to your social media information that may be requested 'for your convenience.'

When you are doing any online shopping, if you get asked to save your payment card details, as convenient as it is, please say no. This way if someone else gets access to your account credentials or computer, you haven't given them everything they need. If you can, either use a credit card or PayPal rather than a debit card, as both give additional protection for goods and services ordered over £100. Online retailers get hacked just like any other company; so if the worst did happen, money isn't being taken straight out of your bank account, unlike a debit card. You can also turn on extra password security on a credit card or two-step verification on PayPal where you get sent a code via a text message to your mobile.

To prevent identify fraud, never enter your passport number or driving licence as part of a security question, the only time you are asked for these is if you are adding advanced passenger information for a flight on an airline's website or hiring a car. If these appear as part of a drop-down list of security or recovery options on any other website, you are probably on a fake website that is phishing you for sensitive personal information. Genuine recovery security questions are things like a memorable place or your favourite actor, nothing that could be used for ID theft.

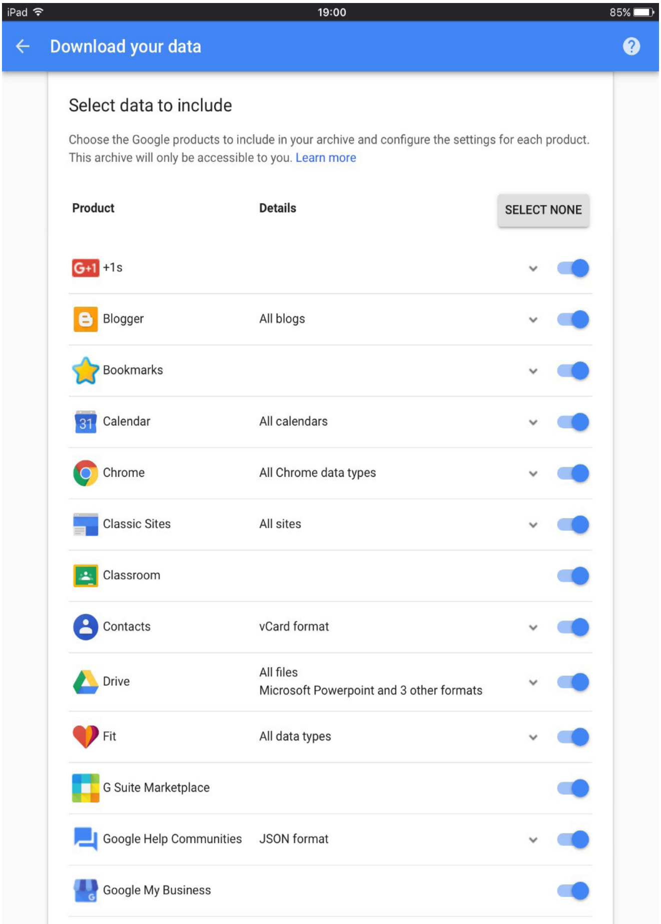
Privacy settings

I live by the maxim that there is no guaranteed privacy with anything you share online. Anything you post into social media may be seen by people you'd rather were not able to and, while you can rely on security settings to dictate with whom you share the information initially, after that it can be shared again, copied, photographed or stolen. If you don't want to risk anything you write or share, don't put it online, it's that simple. Unfortunately, life isn't that simple, and deleting social media accounts is a step too far for most of us. So please ask yourself whether anything you post online could be used against you or would be helpful to a criminal. Updating your social media profile to say to the whole world you are at the airport for a two-week holiday may not be the best idea. So, the first thing to do is see what information the social media companies you use have on you, then limit who has access to your profiles via the privacy options to just your friends and family.

For Facebook this can be found at:
www.facebook.com/privacy
while information on what Facebook collects about you can be found at: www.facebook.com/about/privacy/

For LinkedIn go to: /www.linkedin.com/psettings/
and www.linkedin.com/help/linkedin/answer/50191/accessing-your-account-data

The amount of data Google has on you can be vast, so for ease they split everything into 32 products to make downloading your data more manageable, and created a dedicated website at https://takeout.google.com/



Select data to include

Choose the Google products to include in your archive and configure the settings for each product. This archive will only be accessible to you. Learn more

Product	Details
+1s	
Blogger	All blogs
Bookmarks	
Calendar	All calendars
Chrome	All Chrome data types
Classic Sites	All sites
Classroom	
Contacts	vCard format
Drive	All files Microsoft Powerpoint and 3 other formats
Fit	All data types
G Suite Marketplace	
Google Help Communities	JSON format
Google My Business	

Other social media services will have similar features to let you decide on your privacy settings and how to download your data. The main thing is to be aware of what you have given them and decide if you are happy with that. You actually have a lot more control over your data now then you ever did, backed by new laws that are now in force.

2

DATA PROTECTION AND THE LEGISLATION

GDPR – General Data Protection Regulation

If you live in Europe and are active online, you will probably have received lots of emails mentioning GDPR**,** asking for consent to stay in contact and talking about a new law that is effective from the 25th May 2018. GDPR stands for General Data Protection Regulation, which replaces the older Data Protection Act of 1998 in the UK. As you know, a lot has changed in 20 years; in fact most of the current social media giants haven't been around that long. One of the oldest is LinkedIn, which started in 2002, Facebook didn't start until 2005, with Twitter a year later in 2006. Instagram and Pinterest both started in 2010 and Snapchat and Google+ in 2011. Remember, back in 1998, there was no ADSL broadband; home users generally had dial up internet access only and sharing video or photos taken on a mobile was impossible as no phones had a camera back then. Since then, various companies have been collecting data on us for years, hoping to find a use for it in time and monetise it, often without our knowledge.

It's clear, a revision and rethink when it comes to data protection laws has been long overdue.

So, after years of debate in the EU, the new General Data Protection Regulation (I'll refer to it as GDPR from now on) was agreed to get everyone on the same level across the EU, as different EU countries had quite varied data protection laws. But GDPR is also enforced to protect the personal data of all EU citizens from companies and organisations worldwide, not just in the EU. Now before anyone mentions Brexit, GDPR will become an equivalent UK law, so don't think this is something that is going to change any time soon. Also, and this is a big one, it applies to both 'analog' and 'digital' data, so anything written down, printed, emailed or stored digitally that contains personal data is covered by this law. As to what constitutes personal data, the legislation defines this as pretty much anything that can be used to identify someone, directly or indirectly. In practical terms this becomes an extensive ever-growing list, covering a lot more than what immediately comes to mind like your name, address, email, telephone number, bank account, etc, to include social, economic, cultural, physical, mental and genetic factors. GDPR also talks about 'processing' which is a rather vague term that just about means doing absolutely anything with the data, including but not limited to, storing it, sharing it, altering it, or deleting it.

The six principles of GDPR

Now let's actually look at what GDPR means to you so you don't need to read all the 57,500+ words of the new legislation, starting with the six overall principles of the act which sets out the main responsibilities for organisations.

Firstly, that personal data is processed lawfully, fairly and in a transparent manner in relation to individuals. The important bit here is the transparent manner, so they have to be open and tell you what they are collecting and why, in a way that you can understand, rather than hidden away in small print with lots of legal language.

The second principle is that personal data is collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. So here, the reason why they asked for the personal data, cannot be changed and be used for something else that has nothing to do with the reason you gave them the information in the first place. So, if you were asked for your date of birth in order to be sent birthday discount offers, they couldn't then use it to send you life assurance quotes or medical insurance.

The third principle is that personal data is adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. This principle is to make sure you are only asked to give information that is relevant and in context of the service provided. Too many organisations in the past have asked for things that are not required in order to build a customer profile of you. A date of birth is not required for any online shopping, unless it is for age restricted goods; in the same way it is not generally required if you walk into a shop to buy something. The same applies to your marital status, dependants and household income, you wouldn't tell this to a shop cashier.

Okay, so far nothing to worry about; all good.

The fourth principle is quite a biggie: that personal data is accurate and, where necessary, kept up to date;

every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased or rectified without delay. Here it squarely puts the onus on the organisation to make sure what they have is accurate, and if you tell them to correct something or that they don't need it anymore, it is corrected or erased.

The fifth principle states that personal data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. So basically, once a company has no reason to keep data on you, they need to remove it from their systems.

Lastly, the sixth principle is all about security, that your data is processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage. This ensures that safeguards are in place, which you would expect anyway; though, if the past decade has taught us anything about data security, it is that there is no such thing as 100% security.

So, in order to meet the requirements of the principles, organisations need to know and document the Who, What, Why, Where and When regarding your personal information. There are more, they just don't begin with a W, like How, Access, Security and others. Now you would expect most organisations to know this, but the truth is that your data is probably in more places than they realise; so GDPR makes them evaluate what they have, why they have it, who it is on, when they received the information, where they put it, how they intend to use it and with whom they will be sharing it with. And that is no small task; so don't expect small businesses and organisations to be up to the same speed as major corporations who have been spending over a year preparing.

The Legislation

The legislation says that for organisations to process any personal information they must first have a lawful basis for processing the information. This isn't the same as the first principle to process information lawfully, fairly and in a transparent manner. This is the actual reason and justification for requesting and storing the information in the first place.

GDPR allows for six different reasons:

1. Consent
2. Contract
3. Legal obligation
4. Vital interests
5. Public task
6. Legitimate interests

The one most people will be interested in is *Consent*, where you have agreed to give your personal info, but now the legislation gives you a lot more control than previously. Now consent must be freely given, specific, with an active opt-in (i.e. you had to click yes – it wasn't a pre-ticked or opt-out box in case you missed it) as well as being clear and concise as to what you are agreeing to. There has been a lot of misunderstanding though about consent, with organisations emailing all their customers asking to renew their consent to process their data, otherwise they won't receive any more communication from them, despite those customers having paid annual subscriptions or recently placed orders. One of the main factors of consent is that organisations need to allow you to easily withdraw your consent at any time – it's your data not theirs after all – but there may be contractual considerations to take into account on both sides. Also, there are additional rules around children, who have to be aged 13 or over to be able to give consent for an online service aimed at their age group.

For more sensitive data, which GDPR calls 'special category' data, the six lawful basis reasons are not enough, and one of ten conditions must also be met.

Special category data is basically the following:

1. Race
2. Ethnic origin
3. Health information
4. Biometrics
5. Genetic data
6. Trade union membership
7. Political opinions
8. Religious beliefs
9. Sex life or
10. Sexual orientation

Organisations are expected to implement extra safeguards for special category data, as this can be used for bias and hate crimes as well as extortion or fraud if it falls into the hands of criminals. Further details on this can be found on https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/

Rights

As mentioned previously, to protect and manage your personal data, GDPR has been put into place and the legislation provides the following eight rights for individuals:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling

The right to be informed means a lot more than you think, as organisations must now tell you their reasons for collecting your personal data, how long they will keep it for, who they will share it with, contact information, your rights and more. This needs to be done when they collect your data; so expect to see a web link to a privacy notice, which will then take you to a few paragraphs of text and maybe a tick box to confirm you understand it.

The second right individuals have is the right of access to their personal data. As an EU citizen, you can request what is known as a 'data subject access request' to an organisation either verbally or in writing (emails and social media messages count) which is basically just asking them officially 'please can I have a copy of any personal information you have on me'. This also includes things like attendance to events or courses, rather than just information you gave them. Organisations have the right to ask you to prove who you are, or, if the request is via a third party, evidence that they are entitled to act on your behalf. Typically, they have up to 30 days to respond and in most cases, they are not allowed to charge you anything to reply. Over time, I expect many companies to create self-service web portals, so you can quickly and easily access your data and make any decisions based on your rights: like the third right, the right to rectification, to correct any inaccurate personal data or to complete missing information.

Next, you have the right to erasure, more commonly known as the right to be forgotten. Now there are a lot of scenarios where the right to erasure does not apply, otherwise you could ask to be forgotten after receiving a parking ticket. GDPR does not override other laws, so if you have had any form of contract with an organisation, they are obliged to keep records. If an organisation has shared your data with others or made it publicly accessible, each recipient must also be contacted by the organisation regarding the erasure, unless this proves to be a mammoth undertaking. Slightly less drastic than erasure is the right to temporarily restrict processing, which permits an organisation to store the personal data, but not use it. This right could be used when you are contesting the accuracy of the information or do not want it erased by the organisation because you are in dispute with them or someone else and require the data. This is not the same as the right to object to the processing of your personal data. For direct marketing purposes, the right to object is absolute and cannot be denied. Also, the right to object is not the same as erasure, if you ask an organisation to remove you from a marketing mailing list and not to contact you again, they cannot delete you completely, as they wouldn’t know not to contact you in the future.

The right to data portability is there to basically allow you to obtain and transfer your data from one service to another, without incurring extra charges. This is quite an ambitious requirement as every service is different; so, in order to make it workable, it is limited to the data you have given them yourself, whether typed or uploaded like photos or videos. It does not cover data that was derived or inferred by the organisation about you as a result of being a customer or user. Lastly, there are provisions on automated decision-making and profiling of an individual, where decisions are made without any human involvement; you can request human intervention or challenge a decision. Think of the 'computer says no' sketch from the show Little Britain.

So, what happens if an organisation messes up and loses your personal data, discloses it to unauthorised individuals, accidentally deletes it or it is hacked, commonly known as a data breach? Well, now there is a 72-hour breach notification limit for them to inform the appropriate supervisory authority, but this is based on them having become aware that they have lost personal data in the first place. In many cases months (even years) have gone by before an organisation is aware of what had happened, so the 72-hour limit may not make much of a difference overall, except it stops organisations trying to brush it under the carpet and hide the fact that it happened, once they know about it. Once they have informed the supervisory authority, they are then obliged to inform you of the nature of the breach, contact details of their Data Protection Officer, the likely consequences and mitigation measures they have taken or steps you can take. However, if the personal data they have lost is encrypted, they don't need to inform you, just the supervisory authority, about the incident. Just make sure any breach notifications you receive are genuine, as I expect that criminals will try to capitalise on them whenever there is a major database breach, in order to get you to either click on a malicious link or divulge credentials.

There is a lot more to GDPR, covering international transfers, contracts, penalties and much more, but we have covered the core of the regulation. If you are having trouble sleeping and need something to read, you can find out more about GDPR at the Information Commissioner's Office (ICO) at https://ico.org.uk

3

COUNTER SOCIAL ENGINEERING

For centuries we have been taught to trust and respect our banks, corporations and the authorities, which is required in a fair and just world. Except the world has changed incredibly quickly over the past 20 years. Old tried and tested ways of banking and finance, together with communication in general, have been replaced with digital solutions that require either a mobile phone or internet connection, often both. Many people are overwhelmed by this pace of change, especially if they were born in the last century, and criminals are exploiting this, together with our trusting nature, to bypass the security of these digital solutions through social engineering, getting us to willingly divulge confidential information or carry out actions which compromise us further.

But what is in it for the criminals?

Well it all comes back to fraud, theft, extortion and utilising your computing assets for their own purposes (like cryptocurrency mining). If the criminals can glean the right information from you, they can request a copy of your birth certificate and from that open bank accounts and take out loans, all in your name. Alternatively, your files could be held to ransom, your bank credentials and credit card details used fraudulently; the list goes on. What can I say; the criminals are quite creative in finding ways to monetise our information, but they have to get to it first.

As each digital solution has layers of security built-in, criminals need to find a way to bypass the security in order to succeed, and while they can use technology to hack these systems, it takes resources, time and advanced skills to do so. It is so much simpler and quicker for the criminals to trick us into handing over the keys without us realising. So how do we counter the criminals who are manipulating us for financial gain? In order to do this, we need to take a step back and look at all the ways they can communicate with us. They can email us, phone us or send us a message, either by SMS mobile text or via a social media platform. New words have been created to describe this based around the word ‘fishing’ as in fishing for information. Email based fraud is called ‘phishing’, while telephone-based voice scams are called ‘vishing’ and message-based scams or SMS phishing is called ‘smishing’. The bit to remember though is that the criminals are not restricted to just one method and can use a combination of these to try and convince you of who they say they are.

Fake social media profiles are also a key component utilised by cyber criminals, though the social media companies are fighting back. In one report Facebook purged over 583 million fake accounts in the first three months of 2018. Because you do not need anything other than an email address to set up a social media profile, and you do not need any form of ID to setup an email address, you can see where I am going here.

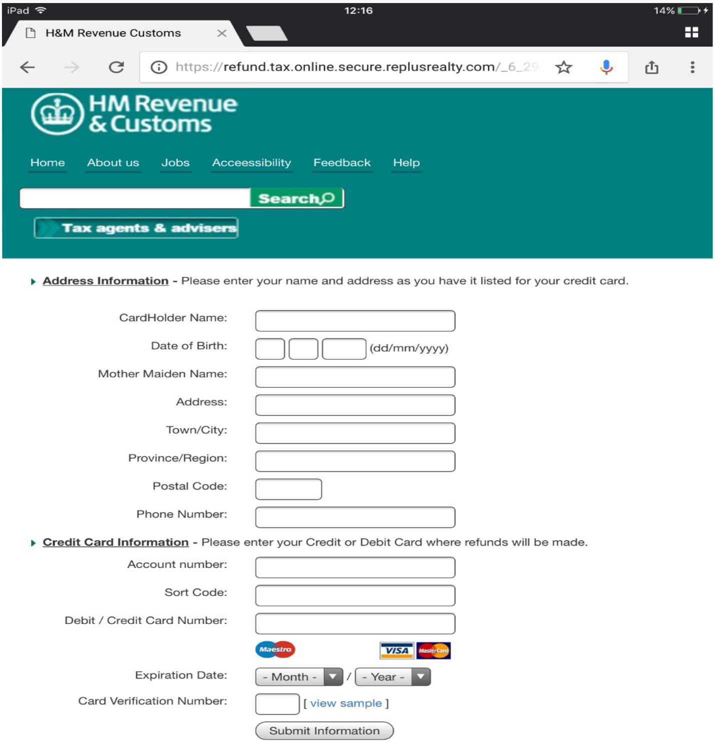
So, the criminals create thousands of fake social media profiles, because it doesn't actually cost them anything; and a lot of people communicate over social media rather than email, so it helps build their illusions as thousands of 'people' cannot be wrong (except those thousands don't actually exist).

So, let's start with phishing.

According to the antivirus firm Sophos, 89% of phishing attacks are by organized crime. Just like fishing, you select a bait and go where you know there are lots of opportunities to catch fish; phishing is no different. The criminals choose services where they know there is a good chance of you being a customer or user, like TV licensing, high street banks, retailers like Amazon, email systems like Hotmail/Outlook.com and Gmail.com, even government departments like HM Revenue & Customs. Next, they offer the bait: 'there is an issue with your account', 'payment has failed', 'we have received a password reset request', 'you are due a refund', 'we have shipped your order'; whatever it is, it's generally a lie. I've even seen fake court summons and land registry charges; do not underestimate the creativeness of the criminals.

There will also be a hook: 'if you do not respond your account will be frozen', 'this is urgent', 'there is a very short time limit'. You get the idea, and the criminals are hoping you don't spot that the email address is not quite right, or the website address they are sending you to is slightly different to the real one. If you click on what they want you to click on, you are then taken to a login page or some type of security challenge for you to verify yourself. It is these credentials they are after and more, like your credit card and bank details.

You may then be taken to a ‘thank you’ page, because the criminals want you to be unaware of what has happened. That is, of course, if the criminal’s intention wasn’t just to get you to visit the website to try and infect your machine using automated scripts looking for vulnerabilities.



Address Information - Please enter your name and address as you have it listed for your credit card.

CardHolder Name:

Date of Birth: (dd/mm/yyyy)

Mother Maiden Name:

Address:

Town/City:

Province/Region:

Postal Code:

Phone Number:

Credit Card Information - Please enter your Credit or Debit Card where refunds will be made.

Account number:

Sort Code:

Debit / Credit Card Number:

Expiration Date: - Month - / - Year -

Card Verification Number: [view sample]

Submit Information

Sometimes the phishing attack is timed to coincide with an actual event like a major data breach or system upgrade; it’s just sent out before the real one. These can be really hard to spot, because they are not unexpected. Not clicking on any links is still the best advice; always go manually to the website of the service or organisation via your web browser. The same applies to attachments, especially PDF attachments which may just contain a glorified link to take you to a fake landing page.

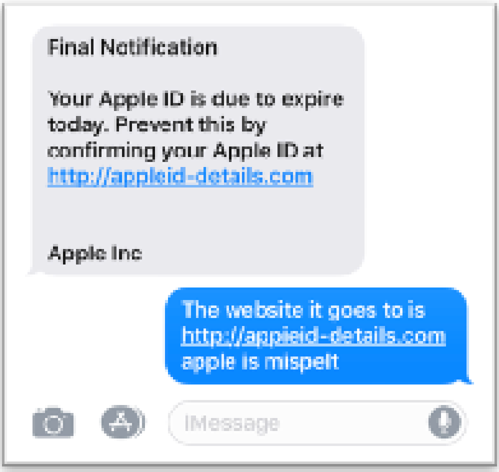
Telephone based voice scams or 'vishing'

Is particularly nasty as many of the victims are elderly. The fraudster calls out of the blue and claims to be from anywhere ranging from the police, the telecoms company, a marketing company doing a survey, even Microsoft (that one has been going on for over a decade) advising you that they have detected a virus on your computer. The lies being told will lead up to you telling the fraudster your credit card or bank details for a refund or a payment, as well as giving up other 'useful' information that could be used later on. Technology allows the fraudsters to use "call spoofing" to falsify the telephone number displayed and even ask you to call them back, but keep the line open, tricking you into thinking you've made a call.

If you do receive a call from anyone claiming to be your bank, a utility or service provider, you can challenge them to verify themselves, or better still ask them for their name and department only and hang up. Call someone you know or even a local taxi service; it doesn't matter, it's just to make sure the line is clear in case it is a fraudster and they are still on the line. Then look up the customer services number online of whoever called you and call them back. If the person is genuine, you will be able to get through to either them or someone in their team. Never give your PIN number for any bank or credit cards if asked, or any form of two factor information like a code from a PINsentry or banking app.

Message based scams or SMS phishing known as 'smishing'

Can be very effective as the smaller screen of a smartphone makes it harder to spot that the message itself is fake as well as the website the link takes you to. Smishing messages tend to be short and contain a look-a-like domain or a shortened hyperlink via services like Bit.ly in order to disguise the link. Bit.ly itself isn't malicious, it's just also being used by criminals. Legitimate messages from a bank, service provider or company wouldn't generally contain a Bit.ly shortened link. Phishing attacks can also be carried out over social media messaging systems like WhatsApp or Facebook Messenger, it just needs to be able to contain a hyperlink to a website to be effective.



Final Notification

Your Apple ID is due to expire today. Prevent this by confirming your Apple ID at http://appleid-details.com

Apple Inc

The website it goes to is http://appieid-details.com apple is mispelt

Fake social media accounts

Criminals may convince you of a whole variety of things, ranging from fake surveys, bogus competitions, even fake jobs. In general, beware of jobs that claim you are a financial adviser and require you to deposit money into your bank account, only for you to transfer it into another account minus a 10% fee. This is just money laundering disguised as a job. Online dating is also a good target for the criminals, with romance scams costing some people thousands. You can do what is known as a reverse image search of any profile pictures, which checks where else the image appears on the web. If it is fake it tends to appear in lots of places and you can see if it has been used in other social media profiles. Online dating fraudsters normally use an excuse as to why you cannot meet up or make video calls, like a military service tour due to finish, or they're spending three months helping rebuild a village in a third world country, so internet access is limited.

Helpdesk scam

The bogus helpdesk scam is another nasty fraud, where either they call you or you call them. Yes, I did say you could call them, because they pay to be high up in online search engine listings for the helpdesks of certain companies; so instead of calling the genuine company you end calling a scammer. Typically, the scenario they run you through is the same, where they ask you for your credentials and then to visit a website to establish remote access to your computer. They then show you something to prove there is a problem, but it's all fake. Next, they request payment to fix the problem or sell you a bogus subscription. Either way, it's bad news, because they have installed something on your computer, they have your credentials and your credit card details. If anyone calls you and tells you they have detected a problem or wants you to verify yourself in any way, ask them to put their request in writing (don't give an email address or postal address) and hang up the call.

Impersonation

Impersonating the boss is also a good way for fraudsters to make a lot of money by asking for funds to be urgently paid to a new supplier to close a deal, timed when the real boss is hard to contact because they are about to get on a long-haul flight or attending a golfing charity day. Of course, the new supplier isn't real, though the bank account is. This is known as CEO fraud and in order for it to work the fraudsters do their research, unlike the scams sent out to thousands of people at the same time. They know the names of key people, maybe upcoming projects and have even already phished the email credentials of the boss. Failing that, they can create a fake personal email address because most employees wouldn't know their bosses personal email address.

The way to avoid falling for most social engineering scams is first not to panic; anything to do with money and a sense of urgency needs to set off alarm bells. Trust your instincts, if something feels even slightly wrong, start to look for clues that will show you it is fake. Look at the email address, the tone, is it too impersonal or too formal. Ask yourself if you would expect to be contacted this way rather than a formal old-fashioned letter in the post. If there is a file attachment, question why, especially if it is a zip file, which can be used to hide the file from security systems. If there is a company mentioned that needs paying or to claim a refund, do not follow any links, instead manually visit their website. Hover over any links and see where it wants to take you, but if you accidently click on a link and it takes you to a website asking you to login, please, please do not login.

The rule is, if you cannot verify something or someone, assume it is fake or a lie until you can establish the truth, and then double check by contacting the relevant customer services department. Remember we are up against organized crime, it is big business, global and very profitable.

4

BANKING, APPS AND PASSWORDS

Our lives have become digital whether we like it or not, with everyday services from banking, to accessing local government services, having moved to a partial or completely digital online platform. We don't need to walk into a travel agent to book a flight or reserve a hotel room or visit the ticket desk to buy a train ticket. We can purchase a vast range of goods and services, including our groceries from our smartphones due to the ease of apps. But despite the ubiquitous nature of apps today with over 2 million different apps available, they have been around for less than 10 years. The first Apple iPhone only came out in 2007 and both the Apple App Store and Google Android Market (now called Google Play) didn't arrive until 2008. Apps were an instant success, small easy to use intuitive smartphone programs that did exactly what they said and little else. This was a world apart from traditional software and websites accessed via a desktop computer or laptop.

Banking was already ahead of the game, as we have had telephone banking since the 1980's and online banking via a website since 1999, so the addition of banking apps was a logical step. Not everything is done with an app though, and ecommerce allowed websites to be much more than information portals. Nearly every major high street retailer has an online presence and the utility companies have added online self-service account management for their customers. Each of the websites or apps, require an account to identify you and normally a password to protect unauthorised access; and in a short space of time we have gone from having to remember a few phone numbers, to having to remember dozens of passwords.

Every year we add more and more passwords as our digital lives expand into new areas of our lives, as well the constant pressure to update our passwords for various security reasons. The resulting effect is that most of us cannot cope with the sheer number of passwords we have, so reuse what we consider to be a good password in multiple places.

What is in a password?

Take a step back and ask yourself how many different online logins and passwords do you think you have? Here are 33 entries just off the top of my head, the true list is closer to 100 for myself.

Finance & Utilities	Online Shopping	Social Media	Online services	Travel
online banking	Amazon	LinkedIn	email	Congestion Charge
PayPal	Tesco	Facebook	Apple ID	Trainline
mobile network	John Lewis	Twitter	Microsoft ID	British Airways
electricity utility	Costco	Pinterest	Dropbox	Hotels.com
gas utility	Debenhams	Meetup		Marriott Hotels
water utility	Pizza company	Instagram		
council tax	Tastecard	Slack		
telephone network		Eventbrite		
Sky TV				

So, let's say for argument's sake, most people have around 50 online accounts that need a password. Unless you write them down somewhere and refer to it every time you need to login, you will stick to a limited number of passwords that you can remember. But what we consider to be a good strong password that is hard for someone else to guess, is not that strong for a computer to guess by literally trying every possible combination. You can test this out at https://howsecureismypassword.net/ which will quickly show you if a password can be broken instantly, as it is on a common passwords list. Just take the length of time estimates with a pinch of salt, as computing power is increasing at such a rapid exponential rate that what took years to compute a year ago, could soon take days. Adding numbers, capital letters and non-standard characters like a question mark or @ sign can help stop other people guessing your password if it is based on guessable things about you, but only makes it slightly harder for a computer to guess.

Also, the password for any given service may have to be changed. They may ask you to update it and change your password as a security precaution if they have noticed any unusual activity on their systems, or they have actually been compromised. Cyber criminals also know this; so send out their own bogus password update requests to trick you into handing over your login credentials and password. Best to ignore any password update requests by email or text message and just manually visit the website of the service concerned (never click on a link in a password update request) when you go to login, if the request is genuine you will normally be prompted to update your password.

So how do you choose a strong password that you can remember?

Firstly, let’s change the word ‘password’ into ‘passphrase’ and string three or four words together. These can be a phrase like ‘TooManyCooks’ or a jumble of random words ‘SteelJellyBrush’ but to meet a lot of the password rules you need to add a number or two and possibly non-standard characters. Try to avoid though, numbers like your year of birth or anything that can be found in any of your social media profiles. So now you have a strong password for one service, only 49 more to go! The advice to not reuse passwords for different services and not write them down, while good advice, is somewhat unrealistic for most people. So, a compromise is needed, actually writing down your passwords (or hints to your passwords) on paper can still be more secure than having a folder in your email system called Passwords.

Just remember though…

If you keep everything in a small notebook or wallet, think about what happens if you lose it. If you can, just list the passwords and very limited login info or website details. Another compromise is to have a set or group of passwords for different things like money, shopping, email, utilities. Again though, remember that using the same password again and again is a really bad idea because if one of those systems is compromised and your credentials are leaked online, criminals now have automated software checking common online services to see if you have used the same email address and password.

A subscription to a password manager service can really make life a lot easier as they remember the individual passwords and all you have to remember is the one really strong password. Some like Dashlane, Lastpass and F-Secure KEY even have a free option, though if you want to use the service across multiple devices you'll need to upgrade. But the best password is one that is also protected with what is known as two factor authentication (2FA) or two step verification. After you enter your password you are then asked to enter a code which is typically sent to you in a text message to your mobile phone or from an app you have linked to your account. So, anyone trying to access your account, not only needs your password, but also access to your mobile phone. So even if your credentials are leaked online, you are still protected. The best part is that a lot of online services like email, Apple ID, Microsoft ID, social media, PayPal and Amazon, it is free to turn on this extra layer of security.

Two factor authentication

This is not a new process; the banks have been using it for years for online banking. You may have a device like a Barclays PINsentry card reader or a HSBC Secure Key at home, these are the second factor used when you need to authenticate yourself to the bank. These days though, the majority of online banking can now be done via the bank's own mobile app and digital versions of the two factor devices are now included in these apps, so you don't need to worry about carrying another device. Security is built into the banks smartphone apps from the start and they are linked to your device handset or mobile number, making it more secure than computer browser based online banking. Just make sure you only download them from an official app store or follow the link from the bank's website. Some of the banking apps also have a feature called 'personal greeting' which you can set to display something only you will expect to see, so that when you login you know are logging to the correct app. If the greeting is missing, you'll know that it is not the genuine login screen and being faked. Also, beware of third party banking apps and websites that claim to manage your bank accounts as these can be fake or potential routes to compromise you if they get hacked. Best to stick to your banks own apps and never follow a link from a text message or email, even if it is claiming to be from your own bank.

Lastly with regards to the two factor authentication via your banking apps or devices, if anyone calls you and claims to be from your bank and then asks you to verify yourself by giving them your two factor authentication code, hang up immediately The same goes for card details, passwords or PIN numbers, the criminals may already have a certain amount of information on you to try and convince you they are genuine; so please don't be fooled by them giving you the last 4 digits of your card number and asking you to verify the rest.

So, smartphone and tablet apps have become the norm for a large percentage of our personal computing activities in the space of a decade, and the cybercriminals know this. They try to get their malicious apps into the mainstream app stores, but this is proving to be much more difficult than the many unofficial ones around the world. That said Google removed over 700,000 Android apps in 2017, and while only a small percentage were outright malicious, that is still a lot of potential victims. If you suspect you may have fallen foul to a malicious smartphone app, please inform your bank immediately so they can monitor your accounts.

In-app purchases

There is also another way apps can drain your bank account, except that this time it is actually legal. I'm referring to 'In-app purchases' where you are charged for additional content, premium features or even virtual currency in a game. Many 'freemium' apps (apps that are initially free but have optional paid premium content) allow you to make multiple in-app purchases, with some popular games allowing you to spend up to £99.99 for in-game virtual currency as many times as you like. Because of the real danger of being able to spend a lot of money unwittingly in a short space of time, I encourage everyone to disable in-app purchases on their devices and require a password on every app purchase (free apps can be excluded).

You can always turn the ability to make in-app purchases back on anytime you like, but this way you cannot accidentally press something and find yourself instantly charged. Apps and passwords are not going to be replaced anytime soon, so we need to find secure solutions to managing our digital identities, because if we do not, the criminals will.

5

MINIMISE YOUR CYBER PROFILE

The sheer number of malicious programs (malware) now in circulation is a mind boggling 700 million according to the March 2018 McAfee Labs Threats Report and growing at rate over 250,000 per day. That is a lot of malicious programs to protect yourself from, but as the saying goes, they only need to be lucky once; you need to be lucky every time.

So how do you stay safe and minimise your cyber profile, or potential attack surface you present to the criminals? Let's break it down into six steps.

1. Reduce the overall number of known vulnerabilities on your computer and smartphone that could be exploited criminals, by regularly updating or patching your system and software. The criminals can move extremely quickly and create malware that exploits vulnerabilities for a fraction of the cost than in previous years, due to cloud computing, crime as a service software (yes criminals sell to other criminals) and automation. So as a result, every week there is a security software patch from a major software publisher trying to fight back and close the gaps

in security. So, while running updates and patching is annoying and time consuming, getting infected is much worse. If you have a computer that you only use occasionally, make a point of turning it on once a week, just to run updates. If you prefer to turn off computers at night, the updates may not happen automatically, so when you are finished and about to power off, check for updates in your system and main software packages that you use first.

2. Next, after making sure everything is up to date, you need good antivirus software. Do not be fooled into thinking you do not need antivirus for a mac, and, yes, modern PCs have antivirus built-in; it's just very basic. It is not just traditional computers that need antivirus as Android mobiles also can benefit; however, you don't need to worry about antivirus on an Apple iPhone as there isn't any available even if you wanted it. Free antivirus will give you a certain amount of protection, but considering what is at stake, it is a small investment to purchase premium antivirus, especially as multiple machine licences or 3-year licences are now available for only slightly more money. So, the question is which one do you choose? Any of the award winning mainstream offerings are good, like Bitdefender, Kaspersky or Malwarebytes, as well as newer offerings like Heimdal PRO. At any given point, one will be rated higher than the others by somebody; so the fact you have premium antivirus protection is the important bit. Just remember to shop around rather than accept the auto-renewal price.
3. How you connect to the internet is the next area to look at. Here two technologies can

keep you safe: a Domain Name Server (DNS) filtering service and a Virtual Private Network (VPN) service. Every website address you type into a web browser needs to be looked up and translated into a numerical internet protocol (IP) address. This is normally provided by your internet service provider, but you can use third party services like Quad9.net or OpenDNS.com which provide additional security by blocking websites that they know to be malicious before you even get there. Both services do not require any software or hardware; just a tweak on your network settings. Quad9 is completely free too for both businesses and individuals, while OpenDNS has a free personal tier and a family tier which is preconfigured to also block adult content. A VPN takes things much further by giving you secure access to the internet via an encrypted link, hiding your address in the process and protecting you from being tracked. This also protects you when you are using public Wi-Fi hotspots as anyone snooping cannot see what you are doing. One of the antivirus companies F-Secure has a very good VPN subscription service called FREEDOME which adds additional security features and works on PCs, Macs, Apple iOS and Android devices. If you can, it's best to avoid free public Wi-Fi and make a hotspot with your mobile data instead, especially if you do not have a VPN.

4. Making sure no one else can pretend to be you is the next step, which means turning on two factor authentication (2FA) for web services you wish to protect. To get started you will need a mobile phone for basic SMS verification texts and, for more security, a smartphone using apps like

Google Authenticator. Obviously, the smartphone can handle SMS texts too. Many mainstream web services offer 2FA as a free option, you just need to turn it on and configure it. So far, I have turned on 2FA as a free option for Amazon, Apple ID, Facebook, Gmail, LinkedIn, Microsoft Outlook.com, PayPal, Twitter and Yahoo. Though, if you are prone to losing your mobile, you might want to avoid TFA. Something to be aware of if you use two factor authentication SMS texts is: if your mobile suddenly stops working and connecting to the mobile phone network displaying “emergency calls only”, you may be a victim of a fraudulent SIM swap. If no one else on the same network is affected, immediately notify your bank and take your phone to the nearest mobile phone shop for your network with some ID to take back control of your phone.

5. The fifth step is to check whether you need to update any of your passwords by visiting a free website called *haveibeenpwned.com* (that’s not a typo, there really is no ‘a’) which tells you if your email address has been compromised because a particular service has been hacked and the contents dumped online. If you have been caught in a hack or data breach, you can then change the password for the compromised account. Right now, at the time of writing, there are over 5 billion breached accounts and the list is growing. It is important to understand that from a data breach the criminals may have your name, email address, mobile, credit card number and password for that service. If you have used the same password anywhere else, you will also need to change that too. Once again, a password manager can greatly help.

6. Limiting day to day activities on a Windows computer to a user account that does not have administrator rights can stop the criminals from installing their malicious software, if you are about to be infected. Because if you aren't allowed, then chances are, they aren't either. This is known as the principle of least privilege and can help keep your computer secure. In Windows, accounts can either have full administrator rights or be standard accounts. What you want is to do all your day to day activity on a standard account, from which you are not allowed to install software. To do this you first need to create a second administrator account; you can make it the same name as your current one with admin on the end and give the account a strong password you won't forget. Once this is done, you can then remove the admin rights from your own account.

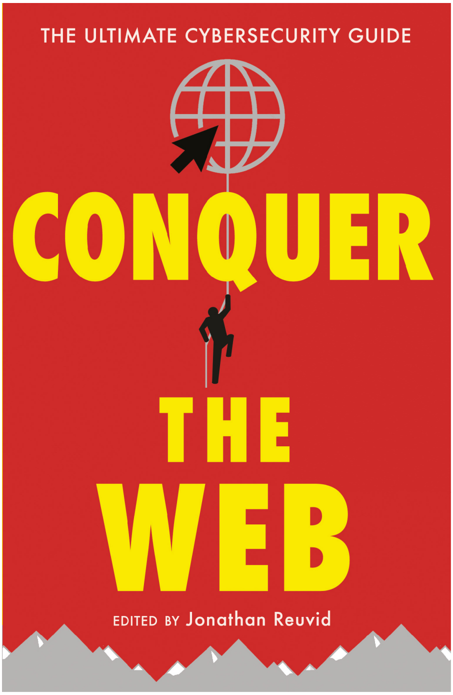
Lastly backups. I know I said six steps, but this one is a bit like insurance if the previous six steps don't work and you end up with an infection like ransomware and cannot access your files. Modern computers have lots of built-in backup features; the main thing is to have the backup somewhere else other than on or near your computer or smartphone. Copying everything onto a USB memory stick or external hard drive is great, and I recommend doing so, but a second copy in the cloud gives you increased protection. Both Apple and Google offer cloud storage for both computers and smartphones, or there are several online backup services like iDrive and Amazon Prime offers unlimited photo backup storage. Either way expect to pay something rather than try and stick to the free tiers and hopefully, like insurance, you never need it, but will be glad you have it.

There is one more thing you can do, and that is to try to do more on devices that are locked down like a Chromebook or an Apple or Android smartphone or a tablet device. If the bulk of your digital life is carried out via a tablet using apps rather than websites, you have significantly less risk than a Windows laptop user. You can still be phished, defrauded and scammed, but you will be immune to millions of malicious programs, at least until the cyber criminals change tactics.

CONTRIBUTORS' DETAILS

Nick Ioannou is an IT professional, blogger and author with over 20 years' corporate experience, including 15 years using cloud/hosted software as a service (SAAS) systems. He started blogging in 2012 on free IT resources (nick-ioannou.com) currently with over 400 + posts. His first book 'Internet Security Fundamentals' available at www.booleanlogical.com, is an easy to understand guide of the most commonly faced security threats and criminal scams aimed at general users. He is also a contributing author of two Managing Cybersecurity Risk books by Legend Business Books.

BOOLEAN LOGICAL LTD
www.booleanlogical.com
Email: info@booleanlogical.com



CONQUER THE WEB

COMPLETE EDITION
£14.99
9781787198623

This book will guide you and provide solutions to avoid common mistakes and combat cyber attacks.

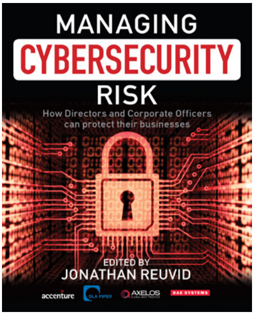
With chapters from
CyberCare UK
Get Safe Online
Boolean Logical

and support material from
Axelos

CYBERAWARE

MORE CYBER BOOKS BY LEGEND BUSINESS

MANAGING CYBERSECURITY RISK
BOOK 1
ISBN: 9781785079153
£39.999



MANAGING CYBERSECURITY RISK
BOOK 2: Case Studies and Solutions
ISBN: 9781787198913
£39£39.99