Keep Safe from Identity Theft

Vital Precautions to Keep Your Identity Secure on the Internet

This article shows you:
- How criminals use the Internet to steal your identity
- The steps to take to ensure your information is kept secure
- The dangers of using public computers and Wi-Fi hotspots

Identity theft has been going on for many years, but the Internet has changed it beyond all recognition. A potential thief no longer has to rifle through your dustbin for useful documents, all the while fearing a hand on his shoulder; he can find all he needs to steal your identity from the comfort and security of his computer. Valuable information about millions of people is online, just waiting to be harvested and used. Don’t be among them! Follow the essential precautions in this article to ensure that your identity is safe.

Contents:

What is Identity Theft? .... K 072/2
How the Internet has Changed Identity Theft .... K 072/3
The 5 Common Methods Used by Identity Thieves .... K 072/4
8 Precautions to Protect Your Identity Online .... K 072/6

What is Identity Theft?

Identity theft may not need much information

The term ‘identity theft’ is a straightforward one: it’s the crime of impersonating someone for some kind of gain (usually financial). In order to steal your identity, a criminal has to find information about you. Exactly what type of information is needed depends on what the criminal is hoping to do, but it many cases he can achieve quite a lot with a surprisingly small collection of details.

Easily-available information is sometimes enough for ‘proof of identity’

Let’s take an example. When you telephone your bank to carry out some sort of financial transaction, your bank needs to verify your identity. For starters, they’ll need your name and account number. They’ll then commonly ask you for the answers to some ‘security questions’: your date of birth, your mother’s maiden name, the name of your first school. When you’ve answered these questions correctly, your bank happily accepts that they’re talking to the real you, and you’re free to carry out any transactions you like.

Innocuous details like your date of birth could be valuable!

Admittedly, many banks have tightened up their security procedures, and you may well be asked for details of recent payments you’ve made, or to name some of the direct debits and standard orders you’ve set up. Until recently, however, those little fragments of information were enough to give you quick access to your bank account, and there’s nothing particularly secret about them at all: do you really regard your date of birth or school name as information to be kept strictly private?

Of course, to be successful, an identity thief would need to know who you bank with and your account number, along with these not-very-personal details, but that’s not an insurmountable obstacle. For instance, both are plainly shown on every cheque you write and every bank statement you receive. This small collection of information would – until recently, at least – enable an identity thief to make the same phone call you did, and be just as convincing about it.

Small amounts of information can lead to more

If an identity thief could convince your bank, he could convince others too, and gain ever-more information about you in the process. Identity thieves commonly apply for credit cards, store cards, loans, driving licences and other documents in your name, and each document they obtain makes it that much easier to get the next. In addition, these 'proofs of identity' allow a criminal to apply for changes of contact address, allowing them to run up huge bills (or commit other crimes) in your name without your becoming aware of what's happening until it's too late.

How the Internet has Changed Identity Theft

Identity theft used to be unsophisticated and risky

Before the explosion of the Internet, the most reliable way to steal someone's identity was to go through his dustbins. That's a risky and time-consuming (not to say messy!) business, and a criminal wouldn't be likely to wander the streets searching every dustbin he found. You'd more likely be specifically targeted because you were known to be well-off, or chosen as a target by virtue of living in an affluent neighbourhood with smart cars parked outside your house.

The 'dustbin method' could obviously yield a lot of valuable information in a short time. A name and address would be quickly found, and bank statements, receipts, personal letters, and other paperwork could all help the criminal build up a useful profile of his target. However, that's a profile of just one person, and the rewards (if any) often wouldn't justify the risks.

Now criminals can work anonymously

The Internet makes the harvesting of personal information risk-free: a criminal can anonymously gather whatever he can find just by sitting at his computer. Exactly what he can find, and the methods he uses, can vary enormously, but there are a lot of options open to him; the Internet is very helpful in this department, and it's becoming more so all the time. He may find just tiny snippets of information – a date of birth here, a town name or postcode there – by following a kind of 'trail of breadcrumbs', or he may adopt a more hands-on approach of tricking you into revealing the information he wants.

Identity theft on the Internet is also far less personal. Whereas you'd probably have been singled-out for the 'dustbin method', on the Internet you would be one anonymous target amongst millions, or you'd be picked (along with many others) because a criminal found some useful information about you and felt it worth trying to fill in the gaps.

The 5 Common Methods Used by Identity Thieves

While it's obviously vital that you know how to protect yourself against identity theft, it's useful to know the main methods used by criminals to gather information about you. Although some of these methods are aimed directly at getting hold of your financial details, others are more insidious – they find information via a more circuitous route that could eventually lead to something valuable:

Details we share with friends online

- **Social networking websites:** this is one of the more circuitous methods, but increasingly likely to pay dividends, as I'll explain in more detail later. Millions of people share a great deal of personal information on social networking websites like Facebook, making these sites a popular hunting ground for criminals.

- **Account hacking:** accounts at online shops, and personal or financial details stored at a number of websites. These accounts are usually protected by passwords, but criminals know that many of us choose easily-guessed passwords and then use the same password everywhere we go. They use automated software that tries different passwords to hack its way into an account.

Automated password attacks

- **Spyware:** this is malicious software that usually arrives unnoticed on your PC, often as a 'hidden extra' bundled into another seemingly-useful program. As the name suggests, spyware monitors the websites you visit and the keys you press on your keyboard, sending this information back to the thief via the Internet and allowing him to harvest usernames and passwords, payment and contact details, and perhaps a lot more.

Spying and keyboard logging

- **Phishing websites:** this is a well-known, but still highly-successful, scam in which people are tricked into entering personal information at a website they believe belongs to their bank (or some other trusted company or organisation), but which is actually a copy of the web page set up to fool the unwary.

Cloned websites of banks

- **Wi-Fi hotspot traps:** at many airports, hotels, coffee shops and other public places, you can use the Internet from your portable computer by connecting to a wireless network provided by the establishment for its customers. Criminals can lurk in these areas with their own laptops, and set up their own competing wireless hotspot, apparently giving you a choice of two networks to connect to. If you connect to the criminal's network, he can monitor what you do online or – more simply – present you with a web page that tries to charge you for Internet access and stores the payment details you supply.

Publically-accessible wireless networks

✋ Along with these obviously-criminal techniques, there's also pure chance: someone could stumble upon useful information by seeing you type it, finding it on a public computer you've just used, or discovering it on a computer you've sold or discarded. Whether they'd be tempted to make use of their discovery is a matter of luck, but it pays not to present anyone with the opportunity in the first place!

8 Precautions to Protect Your Identity Online

Over the following pages I'll explain the eight most important things you should do (or, more often, avoid doing) to ensure that online criminals won't be able to find lucrative information about you. Some of these should be well-known already, and others only apply in particular situations, but they're all part of maintaining a healthy attention to your personal security.

1. Don't include personal information on public websites

The extraordinary popularity of social networking websites has caused millions of people to offer up a mine of information about themselves. Facebook is probably the best-known and most widely-used of these sites, but there are many others, and an important part of the 'social' aspect of these sites is that you complete a profile to share information about yourself with your friends, family and – perhaps – anyone else who arrives at your page.

All these small details can add up!

Much of this information can seem quite innocuous when you type it, but as I mentioned at the beginning of this article, small details such as your date of birth, the names of your children, the town you live in, your hobbies, or the names of your pets could all prove useful to an identity thief.

Taken alone, perhaps none of these little snippets of information is particularly helpful, but together they start to form a profile, and perhaps a sufficiently-detailed one to make a thief decide to delve further.

Details you've included in different places could be found

It's also often the case that someone who uses one social networking site has tried others. For example, a Facebook user may have tried Twitter or Instagram, uploaded videos to YouTube or TikTok, set up a blog at Blogger, or tried to develop professional contacts at LinkedIn. Whether they've actively continued to use those sites or not, they almost certainly filled in some profile information when joining, and those profiles are probably still there to be read. However, they may well contain details that the others don't: again, nothing very useful by itself, but perhaps one website provides a full name where the others only give initials, one profile includes an email address, another lists schools they've attended or places they've worked.

Sometimes, one tiny morsel of information could be very useful indeed. Many people use the name of a child or a pet as their password at various websites, for example, or as their answer to personal 'security questions'. Similarly, knowing you have a particular hobby might lead an identity thief to visit websites and forums covering that hobby to see if you have a presence (and yet more information) there.

Many users of social networking websites do indeed use several of them, and they helpfully provide links on each to their pages on all the others. For an identity thief, it's a quick job to move from one to the next, harvesting any new details he didn't already have.

Keep personal details to the bare minimum

The clear precaution to take when filling in personal profiles on websites is to provide only the bare minimum of information. Many of these websites have a few ‘required’ fields to be filled in, and many more ‘optional’ fields, and it’s best to take the view that any optional fields should be left blank. Indeed, you may feel that some of the ‘required’ fields are going a step too far: why should it be necessary to disclose your real date of birth, for example? Unless it’s really going to have an impact on the way you use the site, it’s wiser just to invent a date of birth!

> ✋ Even if the profile information you’re filling in isn’t supposed to be public, it’s sensible to treat it as if it were and only provide the sort of detail you’d be happy to see published in your local newspaper. This is the Internet, after all, and once you’ve provided the information you have little control over how it’s used. You can’t be sure what the website will do with it, now or in the future, or whether the website’s security is robust enough to keep hackers at bay.

2. Install – and use! – good security software

If a website or an individual hacker can install spyware on your PC, you can be as careful as you like in all other departments and your personal information could still be gathered without your suspecting. If every website you visit and every key you press on your keyboard is being logged by this spyware and transmitted back to the program’s maker, your usernames, passwords, credit card details and other information are all there for the taking.

To avoid this, you need two items of software:

Anti-virus software provides constant protection

- An anti-virus program that runs constantly from the moment you start your PC. Both Windows 10 and Windows 8.1 come with Windows Defender built in, and that does a perfectly adequate job. For Windows 7 users, a good choice is Avira Free Security from www.avira.com/en/free-security.

- At least one good spyware scanner, such as Malwarebytes from www.malwarebytes.com. With Malwarebytes, you'll initially be on a trial of the Premium edition, but there's no need to pay when the trial comes to an end: just keep the free edition you're left with. Use this to scan your PC regularly, about once a week, and any time you suspect that something may have sneaked past the defences of your main anti-virus software.

Run a spyware scanner regularly

3. Use an up-to-date web browser

Modern web browsers can do a great deal to protect you. Behind the scenes they use some clever technology to ensure that information you enter at a website can't be intercepted by anyone on its travels. More noticeably, they'll warn you if you try to visit a website that's been reported as malicious in some way – one that's known to foist spyware on its visitors, or one that's a known 'phishing' site.

Maximise your security by using the latest browser

The security features built into web browsers are improving all the time, but – of course – you only get the benefit if you keep your browser up-to-date! The two most popular browsers, Google Chrome and Mozilla Firefox, both update themselves more-or-less automatically, and it's important to allow them to do this. Microsoft Edge in Windows 10 is likewise kept updated automatically. Of the well-known browsers, it's only Internet Explorer that no longer receives updates, so if you're still using that, it's time to stop!

4. Who's watching you type?

If you pay attention to Precaution 5 below, this one shouldn't be necessary, but it's worth pointing out. If you do ever use a computer outside your home to enter usernames, passwords, credit card details and any other sensitive information, check whether anyone's peering over your shoulder first!

Look behind you!

5. Be wary of public computers and Wi-Fi hotspots!

Hotels, libraries, Internet cafes and many other places provide public computers you can use, either free or for a small charge. Handy as they are, the trouble with these computers is that you don't know anything about them. In particular, you don't know whether they've been compromised by the type of spyware I mentioned earlier, either by accident or design.

Avoid sensitive websites when using a public computer

When you're using a computer that's shared with others, it's best to avoid visiting any websites at which you have to type anything that should remain private. Certainly that means not using online banking, and not entering credit/debit card details, but it's wise to skip any site that requires you to log in with a username and password if you can, unless the password isn't protecting anything particularly sensitive.

> You may well have a web-based email ('webmail') account which you have to log in to, and one of the main reasons for having that type of account is to keep in touch with people by email while you're travelling. Therefore, logging into that account from an unknown computer is often unavoidable, but there are a few things you can do to minimise the risks. Make sure no-one is watching you enter your login details; don't leave the computer unattended until you've logged out again; and (as I'll explain in Precaution 6 below) make sure you really do log out when you've finished.

Check the network name and payment method

I briefly mentioned the risks of public Wi-Fi hotspots earlier, and the obvious advice is to avoid them if you can. When you can't, make sure you know the exact name of the wireless network you should connect to (and don't try to connect to any other!), and find out how payment is made if the access isn't free.

In many cases, you'll pay a cashier and receive a password on a piece of paper, and you simply type this into a web page that appears once you've connected. Sometimes, however, a payment page will appear once you've logged on, and you'll have to enter your payment details. It's with this type of system that you must be absolutely sure you've connected to the right network before following the instructions, or you may be sending your card details to a chap sitting a couple of tables away who set up an on-the-fly network with a confusingly-similar name to catch the unwary!

Treat Wi-Fi hotspots with the same healthy suspicion as public computers: besides having to pay for access, which may be unavoidable, don't type payment details or private login information at websites unless you really have no choice.

6. Always log out of private sites after using them

A secure website may not know you've left!

When you log into a password-protected website, such as your online banking, a webmail account, an online shop, and so on, the site starts a 'session' for you. It knows you're logged in, and it allows you to move freely between pages without asking you to enter your password again at every step. This session remains active until one of two things happens:

- A period of time has passed (commonly 15 minutes) during which you haven't moved to a different page on the site. This period of inactivity ends the session and the site assumes you've gone away.
- You log out of the site, usually by clicking a 'Sign Out' or 'Log Off' button, which tells the site to end your session immediately. (Note that simply closing your web browser or shutting down the computer doesn't end your session as far as the website is concerned: it simply begins this period of inactivity!)

When the session has ended, the only way to continue using the site is to log in again. (If you'd simply paused on a particular page for a long time, for example, you might find yourself whisked back to its home page to log in again when you try to view a different page.)

Someone else may be able to continue your session

Until the session ends, the site believes you're still there, and will let you move around without further prompting. Therefore, if you're not actually there, but didn't bother to log out before going away, someone else may be able to pick up your session on this site where you left off, without being prompted to enter your private login details!

Fortunately, this risk isn't quite as great as it seems at first sight. Unless you left the web page open on the screen when you wandered away – which I'm sure you wouldn't! – this 'someone else' would have to know that you'd just been using a potentially-lucrative website and hadn't logged out, and would have to find their way back to one of the protected pages on that site fairly quickly. One thing that does add to the risk, however, is that the History list of the browser you were using might reveal the pages you'd recently visited, which would make them easy to return to.

Always log out when you've finished

Whenever you finish using a site you had to log in to, always look around for a button or link that logs you out again. Of course, this is far more important on public and shared computers than on your own PC, but it's a worthwhile habit to get into.

7. Check which website you're really at!

Phising attempts should be easy to avoid

We've mentioned the dangers of phishing scams many times, and although they're probably the most-used method of identity theft, they're also the most easily-avoided.

To recap, a phishing scam involves directing you to a website which – you're led to believe – belongs to your bank or some other site at which you have an account. Although it probably looks exactly like the site you're expecting to see, it's a clone created by the identity thief: the expectation is that you'll enter your private login details, which the thief will store and use.

Make sure the site address is what you'd expect

Although the design of the page may look exactly like your bank's site, its address will be different, and that's the main giveaway. After arriving at the site, look at your browser's address bar to check its address. It should begin with https:// (the 's' indicating that it's a secure page); immediately following that double-slash, and before the next '/' sign, is the part of the address containing your bank's name, such as:

www.hsbc.com

www.barclays.co.uk

www.natwest.com

If this part of the address contains anything different, don't go any further! Ignore the fact that your bank's name may appear later in the address, since that's been designed to fool you: only the part following '//' tells you which site you're actually visiting.

Check for the padlock symbol

Crucially, too, there should be a padlock symbol to the left of the address: if that's missing or crossed out, the page you're at is not secure. That means you shouldn't type any sensitive details into it (such as a password), and it may well mean that you're not at the website you thought you were, since the vast majority of reputable websites these days (and certainly all finance-related websites) are secure.

Ignore threatening email messages from your bank!

However, you should really never get far enough for any of this to become an issue. Most phishing attempts arrive as an email message purporting to be from your bank, trying to fool you into clicking a link they contain. Since banks never operate in this way, you should simply delete the message. At the very least, you should ignore the link it offers and visit your bank's website using the method you always use – the method you know can be trusted to take you to the right place – either typing its address into your browser yourself, or selecting it from your browser's Favourites or Bookmarks if you've saved a link to it there.

8. Change your password at the first sign of attack

Webmail accounts are a popular target for thieves

An increasingly-popular tactic of identity thieves is to hack into webmail accounts. Since they're usually free, there are many millions of these accounts in existence, and many are protected by fairly weak passwords.

It isn't particularly your email messages themselves the thief is after, although they obviously may yield some useful details. The ability to use your email account means that they can contact the people in your address book – and anyone else they like – posing as you. In effect, they've stolen a small part of your identity already in this way, and this access to your email account and contacts may allow them to steal a little more – or perhaps a lot more.

As well as ensuring you've protected these accounts with a strong password, keep an eye out for unusual activity: messages vanishing that you don't remember deleting yourself; unusual messages arriving from your contacts that appear to be replying to something you didn't write; or any reports from your contacts that they've received unusual messages from you.

Change your password if you notice anything unusual!

At the first sign of unusual activity, find the option in your account details to change your password and make use of it! It should be a quick and easy job involving typing your current password, and then typing a new password twice.