

Password Theft: Avoiding the Risk

Practical Suggestions to Help You Keep Your Passwords Safe from Hackers

This article shows you how to:

- Understand the risks arising from password theft
- Create strong passwords (and not forget them!)
- Change your passwords at popular websites

It seems that every time we open a newspaper these days, we're confronted with the news of a hacking attack on an Internet-based company with millions of users' passwords stolen. These stories become almost tedious to read about, but what if your password were among the haul? Would that give hackers access to your email, financial and online shopping accounts?

The threats of password theft are very real, and yet few Internet users take them seriously – until they start receiving receipts for payments they didn't make, and find themselves locked out of their own accounts! Know the risks of password theft, and make sure you're doing all you can to stay safe.



Contents:

The Consequences of Password Theft	P 034/2
Are Your Online Accounts Easy to Hack.....	P 034/4
Choose and Manage Your Passwords Safely.....	P 034/6
Switch to Stronger Passwords at Sensitive Websites.....	P 034/13

The Consequences of Password Theft

Phishing messages are one way to steal your password

We've all received so-called 'phishing' email messages – messages that purport to come from your bank, or PayPal, or a popular online store, telling you that your account has been disabled and you must 'click here' and enter your username and password to 'verify your identity'.

These small-scale attempts at password theft can be lucrative for the criminals who send the messages (and set up the fake websites where they hope you'll type your login details), but nowadays we're all well used to receiving these things. We just cast a weary eye over them, recognise them for what they are and delete them.

Larger-scale theft is more common now

These days, criminal gangs set their sights on bigger targets. They go after major websites, aiming to hack into them and steal their databases of customers' usernames and passwords. As we know from reading the newspapers, too often they're successful, and a single attack can yield the login details of many millions of users.

Example: the hacking of Adobe

What can the hackers do with the data they've collected? Well, let's take an example. A few years ago, an attack on the website of the famous software company Adobe netted the login details of around 150 million Adobe customers. As you'd expect, Adobe quickly reset the passwords of all those customers. So does that mean the hackers had wasted their efforts?

Not at all: the hackers didn't particularly want access to millions of Adobe accounts anyway.

Many passwords are reused at other websites

Hackers know that many of Adobe's customers would have used exactly the same combinations of username and password at other websites. The 'username' is often your email address, and most of us have only one email address, so that will be the same at every site we use. Where we have flexibility is in our choice of password, but many users pick the same password everywhere they go.

So, although those millions of login details stolen from Adobe were no use to the hackers at Adobe's website, they might be very useful indeed at countless other websites. Websites which, of course, hadn't been hacked themselves and therefore had no need to warn their customers!

No warning that those sites are vulnerable!

What could the hackers do? Here are just a few examples:

What a hacker could do with your passwords

- Purchase things in your name and have them delivered elsewhere, leaving you to pick up the bill.
- Transfer money from your account to their own without your knowing about it.
- Send messages to your friends and family from your email account, perhaps asking them for personal details they wouldn't give to someone they didn't know (but might happily give to you) or recommending they visit a particular website (which would foist malicious software on them).
- Change the passwords on your accounts to lock you out of them and then try to force you to pay in order to regain access.
- Find personal details you might have added to your profiles at these accounts, such as your date of birth and address, giving them the ability to wreak even more havoc on your life.

Exactly what a hacker can do depends on which of your accounts he can get into, of course. If he gets into your email account, he could cause problems for you and your contacts, but they're unlikely to lead to anyone losing any money. On the other hand, if he gets into your accounts at PayPal or Amazon, which probably have details of credit cards or bank accounts, it could be a very different story.



For online criminals, all this is child's play, and they can do it with the distance and anonymity of the Internet.

Can you prove it really wasn't you?

If any of this does happen, not only can it leave you with a hole in your wallet, but you're in the position of having to prove it wasn't you who ordered the goods, transferred the money, sent the email messages, and so on.

Quick response needed

If you ever suspect that someone is accessing one of your online accounts, the first thing to do is to change the password on that account to lock them out. However, you may be too late – the hacker may have done that himself, locking you out of your own account!

But prevention is better!

You have to make sure you get there first, and that means prevention – making sure that no-one is ever going to get into your accounts.

Are Your Online Accounts Easy to Hack?

Password databases should be encrypted

There's not much we can do about those industrial-scale password thefts: we have to hope that the websites at which we've created accounts are keeping those login details secure. Too often, sadly, we've learned that they're not.

Nevertheless, the millions of passwords they manage to steal should be encrypted, so the hackers don't end up with an easily-readable list. Although they can try a variety of tricks to decrypt the list and make it readable it could take a very long time and might be ultimately fruitless.

Hackers can often still decipher them

But there's another method they can use: statistics. They know that roughly 3% of users choose the password '123456', so if the same six-character sequence makes up 3% of this encrypted list, it's a safe bet that those users had chosen the password '123456'. They can employ the same method for other popular choices,

such as the list below which contains the most widely-used passwords in 2021:

123456	1234567	123321	555555
123456789	password	666666	3rjs1la7qe
qwerty	123123	18atcskd2w	google
12345678	987654321	7777777	1q2w3e4r5t
111111	qwertyuiop	1q2w3e	123qwe
1234567890	mynoob	654321	zxcvbnm

The knowledge of these popular passwords (which itself comes from past security breaches of websites) leads the hackers to decrypt vast swathes of their list, and perhaps even the entire list.

Short passwords are quickly cracked

This leads to two important points:

- If you tend to choose a short, simple password – similar to one of those listed above – for any of your accounts, those accounts will be easy to hack.
- Even if you’ve chosen a much longer, more-complicated password, it may not give you much protection if you use it at several websites.

That second point needs a little explanation, and for this I’ll return to the Adobe incident I mentioned earlier. If you were an Adobe customer and you’d chosen a long, complex password for your Adobe account, the theft of all those passwords wouldn’t generally affect you because Adobe immediately reset everyone’s passwords – your Adobe account is safe. But if you used the same complex password elsewhere as well, it’s quite likely in the hands of the hacking fraternity and just as vulnerable as if you’d chosen ‘123456’.

The risk of using the same password elsewhere

The five golden rules for passwords

The golden rules of password management are quite well known, but it’s worth quickly running through them

again – even though, in a moment, I’m going to suggest some techniques which break a couple of them.

- Password length* • **Rule 1 – make it long:** a short password is easy to remember and quick to type, but it can be hacked in seconds. Regard 10 characters as a minimum length for a password that provides any form of security.
- No dictionary words* • **Rules 2 – no real words or names:** the word ‘ambidextrous’ is 12 characters, so it might seem like an ideal choice of password based on Rule 1, but it’s still easily cracked: hackers use software that quickly works its way through dictionary words and names (including words spelt backwards).
- Complexity* • **Rule 3 – a variety of characters:** use a mixture of upper- and lowercase characters, peppered with numbers and symbols.
- A unique password for every website* • **Rule 4 – don’t reuse passwords:** if a hacker manages to get hold of your login details for one website, he’ll try using the same details at others. (That, as I mentioned, is precisely the point of those large-scale password thefts you read about.) Make sure he’s destined to fail: don’t use the same password anywhere else!
- Don’t store them on your computer* • **Rule 5 – don’t keep a list of passwords on your PC:** if your PC were infected with spyware, your entire list could be handed over to the criminals behind it in seconds.

Choose and Manage Your Passwords Safely

- The rules are not easy to follow!* Whether or not you’ve read those rules before, you’re probably sighing and thinking ‘Easier said than done’. These days, there are so many websites that require us to set up an account that these rules are almost

impossible to observe. Remembering just one 10-character sequence of letters, numbers and symbols is a tall order; remembering a different sequence for each of your online accounts would leave you little time to think about anything else!

I'm going to suggest some helpful compromises, and we'll start by considering what really matters:

Which accounts need a secure password?

Some websites insist you set up an account and choose a password simply to identify yourself. For example, perhaps you want to read a particular article or download a free program, but you can't until you've jumped this hurdle. Or perhaps the site has a message forum and you'd like to join in the discussions.

The question is: would it matter if this password fell into the wrong hands? For this type of website, probably not. Would a hacker want to pretend to be you while downloading a program or posting messages on your favourite gardening forum? It's rather unlikely, but if he did, you probably wouldn't care!

For this type of account, I'm going to suggest you break a couple of the 'golden rules' above and use the same fairly-simple password each time. After all, that password isn't really protecting anything of value, so why make it hard to remember and difficult to type?

Nothing sensitive to protect?

Use a single easy password

If your gardening forum website did ever happen to be hacked and have its member database stolen, what happens? The hackers potentially have your password, and it's a password you use on several other websites (perhaps many others), but they're all websites that are just as innocuous as this one. Hackers aren't going to bother finding out whether your password works at any of these sites because



there's nothing they can gain by doing so. But if they did, there's also nothing you can lose (provided, as I'll explain in a moment, that you haven't filled in a 'profile' providing any extra information about yourself).

Use strong passwords where they're really needed

When a good password is really necessary

Some online accounts really do need strong passwords because they're protecting something of value. For the same reason, they all need different passwords, because if one were somehow hacked you might lose an awful lot of valuable information from others before you discovered what had happened and changed their passwords.

Sites related to financial transactions

By 'value', I mean anything that could be of use to criminals. That obviously includes websites you might use to manage banking and investments; payment processing sites like PayPal which have your bank information and/or credit card details and can be used to buy goods or transfer money; online shops like Amazon which can store your credit card details to enable one-click purchases.

Accounts at those types of websites clearly must be protected by strong passwords, but there are others you might not immediately think of:

Sites with your personal profile information

- Any website at which you've set up a 'profile' containing personal information, such as Facebook and other social networking sites. Details like your address, phone number, date of birth, and names of family members and friends are all valuable to criminals.

Email accounts

- Email accounts such as Gmail, Yahoo! Mail and Outlook.com, since access to your email account and contacts is an open door to identity theft.

Messaging services

- Messaging and chat services such as Skype, for the same reason as above: using these services, a hacker

has access to your contacts and might convincingly pretend to be you.

- Cloud storage services such as Dropbox, OneDrive and Google Drive where a hacker could gain access to files you've stored online (although you should never store files containing private information at one of these services!).

Online file storage accounts

To recap, then, you have some accounts which aren't in the least sensitive, and those can all use the same simple password. And you have others like those above which all need their own strong passwords.

If you make a list of the websites at which you've created accounts and consider which of these two categories they fall into, you might find you still have quite a few that need long, complex passwords...

How can I remember all these complicated passwords?

My advice is not to try! If you do, you'll soon find yourself tempted to choose much simpler passwords again, or to reuse the same password a second and third time.

Too many to remember?

Instead, keep a note of your passwords on paper:

Keep them on paper

- Buy a cheap notebook and write down the name and/or web address of the site along with the username and password you use for it.
- If you can't trust your handwriting to be readable, do the following each time you set up a new account: start the Notepad accessory (or any other word processor you prefer), type the details into it carefully as in the example pictured below, and then print the result on paper. Having done that, close the program without saving the document on your PC. You can then file these sheets in a cardboard folder or ring binder.



This obviously flies in the faces of rules about not writing down passwords, but something's got to give! While keeping lists of passwords on your PC is definitely unwise, keeping them on paper in your home should be safe enough: if you're unfortunate enough to be burgled, a thief isn't likely to be interested in rummaging through your paperwork.

How can I generate good, strong passwords?

Various ways of creating passwords

You'll read a lot of suggestions about creating passwords, such as thinking of a well-known phrase and removing the spaces between words or taking the initial letters of each word. These are designed to make a password more memorable, but since you should have capital and small letters, numbers, and ideally the odd symbol, that memorable phrase will still become a distinctly unmemorable password!

Use an online password generator

But, in the light of my suggestion to keep your passwords on paper, they don't have to be memorable, so you could try that type of approach. However, there's really no need to tax your imagination to come up with long phrases; just try one of these websites instead:

www.strongpasswordgenerator.com

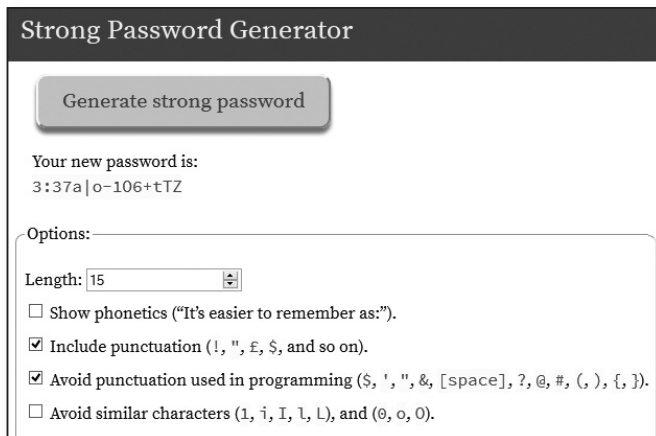
www.safepasswd.com

www.passwordsgenerator.net

Just choose the options you want

These three websites all work in much the same way, although you might prefer one to the others. You

choose how long your password should be, select options about the types of characters it should contain, and then click a button to generate it. If you don't like the result, just click the button again to generate another (changing the options again first if you wish).



Strong Password Generator

Generate strong password

Your new password is:
3:37a|o-106+tTZ

Options:

Length:

☐ Show phonetics ("It's easier to remember as:").

☒ Include punctuation (!, ", £, \$, and so on).

☒ Avoid punctuation used in programming (\$, ', ", &, [space], ?, @, #, (,), {, }).

☐ Avoid similar characters (1, i, l, L), and (0, o, O).

You can then simply use the mouse to highlight the password that's been generated, copy it to the clipboard by pressing **Ctrl+C** and paste it into Notepad for printing by pressing **Ctrl+V** (or, if you're keeping all your login details in a notebook, copy it on to the paper, making sure you write it carefully and clearly).

Copy the password created for you

Let's assume you're currently in the process of setting up an account somewhere and it needs a strong password. After visiting one of these websites and generating a password you're happy with, I recommend getting it on to your paper first. Then, as you set up the account, read that password from your paper copy – not from the password generator's web page. That way, you can be sure that you really can read what you've put on paper.



Change passwords every few months?

Should I change my passwords regularly?

Along with the five 'golden rules' given on page 6, there's another that sometimes gets bandied about: that you should change passwords regularly – perhaps every few months. That's not a practice I subscribe to.

The reasoning is that a hacker might be silently snooping on your email or Facebook account, or watching your transactions at PayPal, for example, waiting for a good moment to pounce, and if you change your password you'll thwart him.

The thing is, hackers are looking for a quick profit. If a hacker has access to one of your potentially-lucrative accounts, why would he hang around for weeks? Regularly changing your passwords is largely pointless, and makes your password management much more time-consuming.

Just change a password when necessary

Once you've set strong passwords on those accounts that need them, there are really only two reasons to change one:

- If you know (or have any suspicion) that someone has been accessing the account or knows its login details.
- If the website itself tells you to change your password, perhaps because it's been the victim of a hacking attack.



On that second point, if a website has been hacked, it would usually send an email message to all its users telling them to change their passwords. However, the criminal fraternity also tends to send out fake 'phishing' messages hoping you'll follow their link and type your personal details into a website set up by the criminals themselves.

If you ever receive an email telling you to change your password at a particular website, ignore any

links in the message and use your usual method to visit the site instead – typing its address into your browser's address box or picking it from your Favourites/Bookmarks list – so that you can be sure you really are at the intended website.

Switch to Stronger Passwords at Sensitive Websites

On page 8 we identified the types of accounts that must be protected by strong passwords. My suggestion is to grab a piece of paper and make a list of the websites at which you've set up accounts (in other words, websites at which you have to enter a username and password). Having done that, consider two things about each of the accounts on your list:

- Is it an account that should have a strong password?
- If it is, have you already set a strong enough password for it – a password that you don't reuse at any other website?

If any of the sites on your list need strong, unique passwords and don't have them, work your way down the list visiting each in turn and changing its password.

Over the following pages, I'll give you the required steps for some of the most popular websites which really should be protected by strong passwords.

Amazon – www.amazon.co.uk

If you're an Amazon customer, your account almost certainly contains your full name and address and quite probably your credit/debit card details. Someone accessing this account could easily launch a major shopping spree at your expense, along with picking up

Make a list of your online accounts

Which need strong passwords?

One-click purchasing – for anyone with your password!

some useful personal details about you into the bargain, so a secure password here is vital.

To change your Amazon password, do this:



1. Log in to your account as usual, by moving the mouse over the **Hello. Sign in/Your Account** link and choosing **Sign in** from the menu that appears.
2. After signing in, move your mouse over the same item again and choose **Your account** from the menu.
3. Near the top of the page, click on **Login & security**. On the next page, alongside **Password** (and a row of asterisks which represents your current password), click the **Edit** button.
4. In the three boxes presented, type your current Amazon password ①, then type your new, stronger password twice ②, and finally click **Save changes** ③.

Confirm your old password, and type the new one twice

Change Password

Use the form below to change the password for your Amazon.co.uk account. Use the new password next time you log in or place an order.

What is your current password?

Current password: ①

What is your new password?

New password: ②

Reenter new password:

③

Now you can continue using Amazon, or sign out via the same menu you used in steps 1 and 2. Next time you log into Amazon, you'll use your new password.

PayPal – www.paypal.com

Instant payments by entering your PayPal password

If you use PayPal, your account includes your bank or credit card details so that, when you want to make a purchase online, you can do so simply by typing your

PayPal password. Of course, a criminal who already has your PayPal password could do exactly the same, so make sure you use a strong password here.

If you need to change your PayPal password, here's what to do:

1. Log into the PayPal website by clicking **Log In** at the top of the page and typing your username and current password.
2. Click the cog icon at the top-right of the page.
3. Near the top of the page, click on **SECURITY**.
4. In the 'Password' section at the top of the page, click on **Update**.
5. On the page that opens, begin by typing your current password into the topmost box to confirm your identity. Then, in the two boxes below, type your new password identically into each. Finally, click the **Change Password** button.



Confirm your identity and change the password

You can now log out of PayPal by clicking the **Log Out** link at the top of the page. In future, you'll log into PayPal (and make purchases with PayPal at online stores) by entering your secure new password.

Facebook – www.facebook.com

If you use Facebook, you've quite likely entered profile information about yourself which could be valuable to a would-be identity thief, such as your date of birth. In addition, Facebook login details can be used to log into many other websites at which you may have accounts (for instance, Skype allows you to log in using your Facebook account's details). So, even if your Facebook profile itself holds nothing of interest, Facebook must have a strong password. Here's how to change it:

1. Log into your Facebook account in the usual way, using the boxes at the top of the home page.



Personal details, and the ability to log into other websites

2. In the top-right corner of the page, click the downward-pointing arrow and choose **Settings**.
3. At the left of the page, click on **Security and login**. On the right, in the 'Change password' section, click the **Edit** button.
4. Type your current password, then type your new password twice and click **Save Changes**.
5. You can then click the downward-pointing arrow again and choose **Log out**. In future you'll log into Facebook (and any other sites which accept Facebook login details) using your new password.

Microsoft Account – login.live.com

Access to a variety of accounts and services

This used to be known as a 'Windows Live ID' and it consists of an email address and a password. These are commonly used to log into a Windows 10 or 8.1 computer, but they do much more than that: your Microsoft Account gives you access to your Outlook.com email account, your personal files stored on the OneDrive cloud storage service, Office 365 and Skype, among other services. In addition, you may have added payment details to your Microsoft Account to enable you to pay for apps at the Windows Store among other things.

So, if you have a Microsoft Account, it definitely needs a strong password. Here's how to change yours if you need to do so:



1. At login.live.com, log in using your current Microsoft Account details.
2. Near the top-right of the next page, beside your email address, click on **Change password**.
3. You should now see a secondary email address you've previously given to Microsoft, partly obscured by asterisks. Type the full email address in the box below and click **Next**.

Microsoft sends you a code by email

4. This will lead you to another web page prompting you to enter a short numeric code. Microsoft has just sent this code to the email address you confirmed in step 3. Type it into the box and click **Verify**. *Enter the code you received*
5. On the next page, type your current password followed by the choice of new password twice and click **Save**. *Change your password*
6. After doing that, click your name in the top-right corner of the site and choose **Sign out**. From now onwards, wherever you use your Microsoft Account, you'll use this new password when you sign in.

Google Account – www.google.co.uk

A Google Account is another 'one login for everything' account: this combination of email address and password is used to get you into Google sites and services such as Calendar, Maps and YouTube, as well as the Google+ social networking site, Google Docs online file storage and the Gmail email account.

One login for all Google services

If you've set up a Google Account, and particularly if you use Gmail, Docs or Google+, you should make sure this account has a strong password.

Here's how to change it if necessary:

1. Visit www.google.co.uk and click the blue **Sign in** button at the top-right of the page.
2. Enter your current Google Account details to log in, and you'll see a coloured circle in the top-right corner. Click that and then click **My Account**.
3. On the next page, in the 'Sign-in & security' section, click **Signing in to Google** then click **Password**. Type your current Google Account password, then your new, secure password twice, and click **Change Password**.



4. You can now click that coloured circle in the top-right corner again and choose **Sign out**. In future, you'll use your new password when you log into any of Google's services.

Skype – www.skype.co.uk

*Contacts list and
payment details in
your Skype
account*

Skype is a popular way to keep in touch, but your Skype account holds contact details for family and friends and it may well store payment details for Skype Credit. As mentioned above, you might log into Skype using a Microsoft Account; however, if you still log in using an older Skype account, it must have a strong password.

Here's how to change it if you need to do so:



1. Click the **Sign in** link at the top of the Skype home page and log in with your usual Skype name and password.
2. Scroll to the bottom of the next page and click **Change password**.
3. Type your current password into the **Old password** box, then type your chosen new password twice and click **Save**.
4. Finally, click the **Sign out** link at the top of the page. If the Skype software is currently running on your PC, open its window and choose **Skype > Sign Out**, then right-click its icon near the clock on the taskbar and choose **Quit**. Next time you log into Skype itself, or the Skype website, you'll use your new password in combination with your Skype name.

*Change your
password*

*Sign out of the
Skype software*