

Security Advice

Here are some tips to keep your account safe and secure.

Pick a strong and unique password

A strong password has symbols and numbers and confuses logic. Often easier said than done, right?

Let us help you. An easy way to come up with strong passwords are to think of a sentence that includes numbers. Then take the first letter of each word and alternate capital letters. Adding symbol is easy when you replace a matching letter or number.

Example:

Think of an easy to remember personal sentence such as
'My oldest child is born in 2004 at Modern Hospital'

The first letters of each word now form MOCIBI2004AMH
Makes sense, right?

Alternate capital letters and replace the 'A' from 'at' with the symbol @

Now you get MoCiBi2004@Mh

This is a strong password with no real logic to it, yet it is easy to remember for you. It's nice and long too. Spying on you typing this is very difficult and cracking it will be quite a challenge. But remembering it is a breeze.

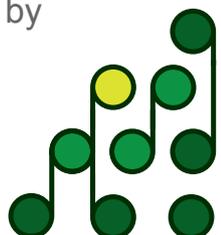
You can use different symbols or create different patterns with the capital letters.

Go nuts 3 instead of E, a ! instead of i, a 4 instead of A or a \$ instead of S. Whatever is easy for you to remember.

In this example we'll swap the i with a 1 and the end result is
MoC1B12004@Mh

Use a unique password for PONSIST, don't use the same password on every site.

Don't share your password with anyone. We will never ask for your password by email, instant message or phone, ever.





Be careful where you log in

Only enter your password on the official [PONSIST](https://www.ponsist.com) website

Check your address bar and pay attention to spelling variations.

If ever you're not sure whether to log in, go to <https://www.ponsist.com> to be safe.

Be cautious when you're online, don't complete suspicious requests for personal information, including any offer that seems too good to be true.

Protect your devices

Make sure your computer and browsers are up-to-date with the most recent updates and anti-virus software.

Only install browser add-ins or plug-ins from publishers that you trust.

Don't open attachments or install software from an email that looks like it's from PONSIST, we will never ask you to download or open files from an email.

Know the risks of using unsecured Wi-Fi

PONSIST uses extra security precautions (HTTPS: Hypertext Transfer Protocol Secure). This encrypts the anything you send within the Society and is designed to keep others from stealing your login credentials, even on an unsecured network.

However, when you use an unsecured Wi-Fi network (one that doesn't require a password) like you find at coffee shops or airports, it can still be possible for someone to see most of the internet traffic sent to and from your device.

If you see strange activity on your account that you don't recognise it is possible that someone got into your account.

You should immediately change your password to secure your account.

If you received an email about a change you didn't make it is possible that someone got into your account.

We'll send you an email when you change your email, username or password.

You should lock your account to protect your profile and then reset your password:

1. In the email we sent you, click **Log Out**
2. [Reset your password](#)

