GETTING STARTED

We recommend starting with AUTO-CRYPT which creates self-decrypting files. This is the easiest way to use PTP. Its the A button in the PTP toolbar. You can also RIGHT-CLICK on any file in Windows File Explorer and choose PTP/Auto-Crypt. The receiver does NOT need PTP to be installed.

Autocrypt creates files with the extension .PTX so they don't get snagged in firewalls. We install a little program (PTX Launcher) with PTP which allows you to run PTX files like EXE files. At the other end, if they don't install PTX Launcher they have to rename the file to .EXE and then run it.

The next most easy to use is SIGN & ENCRYPT. You can put a default password for this in SETTINGS so that it always encrypts with the same password. The receiver must have a copy of PTP installed (which can be the FREE edition).

Finally the full Public/Private key RSA encryption which is the real 'Person To Person' uncrackable security which does not require exchanging passwords and does not require purchasing DIGITAL CERTIFICATES (which all other RSA systems do, including Microsoft). The receiver needs PTP but it can be the FREE edition. With the FREE edition they can receive files and decrypt them but they cannot SEND encrypted files.

To use RSA Public Private Key encryption sender and receiver have to exchange digital public key files by email. PTP provides an easy single click button for this.Once that is done each of you is in the others secure contact list in PTP. This is a bit more work than the first two solutions but the security doesn't rely on exchanging passwords which could be intercepted.

Its all a trade off between security and convenience ie more security=less convenience.

PS - where you have to do it, the best way to exchange passwords is over the phone.