Email security:
What you need to know about PGP (Pretty Good Privacy), Protonmail, and other options

PGP is a method for securing electronic communication, like email. It's a tool used to encrypt and decrypt messages using keys. PGP has been, essentially, the standard for encryption and decryption of email for decades.

Encryption? Decryption?

Encryption is a fancy way of saying that you're coding a message so that only someone who has the "key" for it can decrypt it. Let's use a low-tech example. Let's say that we want to use a method of encryption like the very simple one below, where the bottom row is what we'd use in the original message and the top row is the character we'll use in the encrypted message:

0	1	2	3	4	5	6	7	8	9	a	b	c… p
a	b	c	d	e	f	g	h	i	j	k	l	m…z

If you were trying to snoop on messages I'm sending and you intercepted a message that read "74bbe mehb3," you might think that I'm just sending gobbledygook (although with a computer and the right skillset, it would take you seconds to decrypt the message). However, if you had the key above, you'd be able to easily decrypt the message: "hello world." That's encryption in a nutshell, although PGP is much more advanced than that.

How does PGP actually work?

PGP uses keypairs; anyone using PGP has both a public key and a private key. If you wanted to send someone an encrypted message, you would encode that message using a special piece of software (such as software that plugs in with your email client) and the intended recipient's public key (which they have shared with you). The software you're using encrypts the message, which you're then able to email to your recipient. It'll look like a whole bunch of gobbledygook just like the example above, but even more complicated! A message encrypted with a particular public key can only be decrypted by the holder of the private key that's the "pair" of that public key, which means that if all goes right, your intended recipient – and only your intended recipient – will be able to use software and their private key to decrypt your message.

The keys can also work the other way around, too. If you want to "sign" a message so that a recipient who knows your public key can be certain it came from you, you could encode a message with your own private key. Of course, this message, too, would be encrypted, but could be easily decrypted by anyone who knows (or can find) your public key, meaning that you wouldn't send a sensitive message encrypted with your private key, only one that you wanted to make sure a recipient could verify came with from you.

It's really important to note that PGP encryption only encrypts the contents of a message, but does NOT encrypt the metadata associated with the message. Anyone sophisticated enough to intercept a message will be able to view the sender, recipient, subject of the message, and more.

OK, how do I use it?

PGP requires just a little bit of effort to set up. You'll have to access your email through a desktop client like Thunderbird (an open-source client made by Mozilla, the makers of Firefox). Once you have Thunderbird up and running with the email you'd like to encrypt, you can download a plugin (Enigmail) which makes setting up, and subsequently managing, a PGP keypair very easy. Once you create a keypair, you can use a wizard in Enigmail to upload your public key to a set of keyservers to make it easy for anyone wanting to send you an encrypted message to do so.

This sounds great, but it's way too complicated. Isn't there an easier way?

Yes – in fact, there is! Another option is to use a standalone, secure email service like ProtonMail. ProtonMail is an encrypted email service that was developed by CERN scientists in their free time. With ProtonMail, you can sign up for a free email address that can be used to safely send encrypted messages *to other ProtonMail users*, or to receive encrypted email messages from anyone who has your ProtonMail public key. Right now, while PGP can be used to send encrypted messages across may email providers, ProtonMail can only be used to send encrypted messages to other ProtonMail users. However, doing so is a piece of cake – messages are encrypted automatically after pressing a "lock" button. ProtonMail is planning to expand to allow users to use PGP, too, and they may make the implementation for doing so easier than PGP has traditionally been to master. We're waiting in eager anticipation to see what they have planned! Additionally, like CERN, they are hosted in Switzerland, which makes them less likely to be forced to turn over records to intelligence agencies (if that's who you're worried about snooping on your email!).

Want to know more?

PGP: https://emailselfdefense.fsf.org/en/

ProtonMail: https://protonmail.com/