About GPG Encryption

To understand why encryption is important, you first have to understand how the internet works. The internet is not ‘point to point’. This can be best demonstrated by presenting a scenario:

John works at a web hosting company and manages Company A’s website and email for them.

Bob works for Company A, and so does Dave.

Dave forgets his password and asks Bob to email John to get it changed to ‘lifeisgood1’. Bob sends the email, which John receives and the password gets changed.

Everything may seem to be fine, but it is how that email is sent that is important.

The internet is a very large packet switched network, which means that Bob’s email was split into small chunks and sent to John via a number of other computers, taking the quickest route.

Usually, other people's traffic is unnoticed by our computers, since it's not addressed to us. Unfortunately it is possible to listen to it with the right software. That means that anyone along the path between Bob and John could have picked up what Dave wants his new password to be.

This is exactly the same reason that secure sites encrypt credit card details when you make a purchase online. Email is harder to encrypt, because both people need to be using encryption software, and the same standard of encryption for it to work.

Email encryption never really caught on, but when it comes to password requests, it is highly recommended, even if it is only installed on one computer at your office that is used to contact us.

How does it work?

GPG works by using two types of keys. A public key and a private (or secret) key.

You keep the secret key, and you distribute the public key to people who might need to contact you. When someone wants to send you a secure email, they use your public key to encrypt it. This means that ONLY your private key can be used to read what the text actually says.

Likewise, if you want to send someone a secure email, you use their public key to encrypt it, and they can read it with their private key.

This is one of the most secure forms of encryption available today.