

I.T. can be easy – December 2018 by Steven Dunwell

Phishing emails and the “sextortion” scam

I've had a lot of enquirers about this subject this month, so I thought my article would be dedicated to this troubling form of trying to scam innocent computer users.

In the last few months, a new scam email has been hitting millions of inboxes around the world. In the message the scammer claims to have taken over your computer and recorded you (via your webcam) with plans to release any video footage or photographs that you may have taken innocently, and in private to your friends, family and colleagues unless you pay a ransom.

If you have received such an email, please don't worry, know that it's totally fictitious and merely a method of extorting money from you.

They may also include an old password that you may of have previously used, if you recognise this password and you still use it to access any current websites or emails, you should change it immediately.

The crooks don't actually have access to your computer, nor do they have access to your passwords, pictures, videos or webcams. These unscrupulous people are simply trying to scare you into giving into their demands.

Here are a few suggestions on what to do if you receive one of these messages:

1. Do not pay the ransom!
2. Do not reply to the email, mark the email as junk/spam if possible
3. If you are able to, change your email password as soon as you can
4. Update your anti-virus software regularly
5. Cover your webcam when not being used