Stroud High School
Headteacher:
Mr Mark McShane BA (Hons)

Registered Office:
Beards Lane
Cainscross Road
Stroud
Gloucestershire
GL5 4HF

Telephone: 01453 764441
Fax: 01453 756304
Email: admin@stroudhigh.gloucs.sch.uk
Website: www.stroudhigh.gloucs.sch.uk
Twitter: @stroudhigh
Facebook: StroudHighSchool

April 2016

Dear Students and Parents

You may, or may not, have heard of 'ransomeware' but it is a type of 'malware' (ie hostile and malicious software) that is a growing threat to personal mobile devices, desktop and laptop computers at home, at work, at school and on the move. Ransomeware could easily affect any devices you use so please take the time to read the following carefully:

What is 'Ransomware':

"Ransomware is malware that prevents you from using your files or your computer, and then extorts money from you in exchange for a promise to unlock them. While forms of ransomware have existed for many years, this category of malware re-emerged in September 2013 in a form that is far more effective and dangerous.

As criminals have learned how to construct and distribute highly effective ransomware, they have built multi-million-dollar enterprises based on victimizing individuals and organizations."

From the Sophos anti-virus website

A common infection scenario may look like this:

- You receive an email that comes from a seemingly plausible sender with an attached document, for instance it could appear to be a parcel service with attached delivery information, or a company appearing to send you an invoice
- The email attachment contains an MS Word or Excel document with an embedded 'macro' (a macro is like a little program that automates a series of actions). If you open the document the macro will attempt to start automatically, executing the following actions:
    1. It downloads the actual ransomware from a series of web addresses that only exist momentarily. If a web address cannot be reached, the next one is accessed until the ransomware has been downloaded successfully
    2. The macro runs the ransomware which contacts the server of the person who sent the e-mail and sends them information about your infected computer
    3. Files of certain types (Office documents, database files, PDFs, CAD documents, HTML, XML etc) are then encrypted on your computer and on all accessible shared drives you may have on your home network. Ecryption means that only people with the secret 'key' or password can then read those files ie the person who sent the e-mail in the first place
    4. Automatic backups of the Windows operating system are often then deleted to prevent you being able to recover either Windows or the files
    5. You are then sent a message demanding money – if you don't pay up all your files will be deleted after a certain period of time … of course, even if you pay up you might not get your files back or they may make further demands

Best Advice:

- Do not open attachments from unknown sources
- Do not click 'enable macros' in document attachments received via email unless you are 100% sure it is something you are expecting
- Do not forward the e-mail to anyone else to check if it is safe – just delete it or put it in your 'junk' folder
- Make sure you use anti-virus software and it is regularly updated

- Make regular backups of your data – you can set your computer to do this automatically
- Make sure you regularly apply all the updates for your operating system (Windows 10 etc) and any software that you use
- Use common sense - if you don't recognise the sender of the email then just delete it … if you are unsure then just delete it

Yours sincerely

Mrs C Pride
Deputy Headteacher