BEWARE OF FREEWARE

Very rarely in life do you get something for free, there is usually a motive behind it and freeware is a prime example of this.

On the 30 August 2018 NHS Digital issued a Cyber Security Threat Notification after identifying suspicious activity on a computer on our network. The threat, which could easily have been avoided, took the Cyber Security team nearly 12 hours to resolve.

It all started so innocently…

Staff within the practice were downloading health videos from YouTube to display on their patient screens. The videos needed to be converted to MP4 files before they could be added to the screens, as they didn't have the software to do this, they searched the internet for something that could do this for them.

Choose wisely…

Unfortunately, this is where the problem which triggered the security threat notification began.

The internet search found an array of options many of which were free software.

Whilst free software, also known as freeware, can come from reputable sources, some freeware contains malware such as viruses, adware and spyware which can pose a significant security threat.

The freeware which was downloaded and used to convert the YouTube videos contained adware. This started to display pop up adverts which became increasingly offensive and replaced the browser homepage on the computers with another which contained links to high risk websites.

Whilst free software, also known as freeware, can come from reputable sources, some freeware contains malware such as viruses, adware and spyware which can pose a significant security threat.

The clean-up operation…

Once the cyber threat notification was issued the NHIS Cyber Security Team contacted the user to gain a full understanding of the issue, how it arose and if other PCs were also affected. It became clear that a further two PCs had also been used to convert the videos using the same freeware. Luckily this malware hadn't been designed to spread or morph, so it was contained to three PCs which had downloaded the software.

Removing the adware and restoring the web settings was a time-consuming process, which took 12 hours to complete over a two-day period. Several products had to be used to remove the different elements of the adware before a full scan could be done to ensure the three computers were free of the offensive adware.

Once it was confirmed that all three PCs were clean, and their browser settings had been restored a full response was issued to the practice, the CCG and NHS Digital enabling the threat alert to be closed.

Removing Adware...

To clean the computers different products were used to target different elements:

- AdAware was used to remove the pop-up ads,
- Malwarebytes removed the malware,
- HitmanPro was used to remove all the cookies,
- Zemana performed a deep scan of each of the computers,
- Sophos performed a full scan to ensure the computers were clean.

Remember…

- **Beware of Freeware** – it can contain malware. Luckily in this instance the type of malware had not been designed to morph or spread but it displayed offensive adverts and redirected web pages to dangerous sites.
- **Report anything strange** - If settings change on your PC or pop-ups start to appear contact the Service Desk immediately.
- **Ask for advice** - If you need a new piece of software contact the NHIS Cyber Security Team for advice.