Cablers

Case Study: Ransomware

In the winter of 2020, when the world was on lockdown, cybercrime was on the increase. With more and more people having to work from home, using the internet to do so much more than ever before – shopping; meetings; work; communicate; bank; listen to music, opportunities for the malignant side of humankind opened up.

Working with schools within Essex we were seeing more and more cases of cybercrime. An increase in phishing emails, more links to bogus companies purporting to sell items at a 'good price'; people gate crashing on-line meetings; we also saw an increase in ransomware – where a hacker gets into a computer system and locks the whole system up, demanding payment for release.

We want less opportunities for this kind of attack to occur, so please read on...

One of the schools we manage IT for was hit by a ransomware attack but had no idea that someone had infiltrated their system.

Background:

Having moved from Essex Broadband services to RM Education Broadband when Essex closed their provision, we started supporting the schools' broadband services as part of our IT package. Part of that solution included a robust anti-virus package, including anti-ransomware software.

What happened?

A phishing email had been sent to a teacher working from home. Not realising it was bogus, they clicked on the link within the email, which enabled the ransomware software to download in the background. Upon returning to school, the teacher connected their laptop to the network - the malware kicked in and started to encrypt files on the main server.

Peace of mind.

Our anti-ransomware software on the server immediately detected the program and blocked the laptop from the network. Due to this, only three files were infected, our software managed to recover these files and return them to their pre-existing state.

Whilst the software was doing the recovery, notification was sent to the school IT administrator and our team in the office. The software identified the infected laptop to the team, so that it could be re-built and back in working order within an hour.

By averting this attack our client had great peace of mind, as by ensuring they had sufficient protection, the school wasn't technologically crippled by these hackers, and it was business as usual.

Whilst it is invaluable to have anti-virus/anti-ransomware software on your school computer network, it is also imperative for training of all staff that use the computers, educating then on how phishing attacks happen and what to do if they think they have been compromised.

Fast reaction to any intrusion helps save down time and will save your school money in the long term.

Cablers
School IT Services
01787 22 11 66
hello@cablers.co.uk
www.cablers.co.uk