Ransomware

Selma turned on her computer, waited while it booted up, and then saw this. It was a ransomware message.

Cybercriminals had got access to her computer and infected it with malware which effectively locked her files and meant that she couldn't use them.

The message said that if she wanted to unlock the files, she'd have to pay a fee, in other words a ransom, and then she'd be sent a 'key' to unlock them.

Compared to the disruption that the loss would cause, the amount of money being demanded wasn't that much and she wasn't sure what to do.

Most agencies, including the National Crime Agency, encourage businesses and individuals not to pay the ransom for two main reasons.

Firstly, it makes cybercrime more profitable and sustainable and secondly, there's no guarantee that the files will be released.

Some attacks are aimed at large businesses, others are random attacks which are spread like viruses and look for weaknesses in operating systems and software, then use these as a way in, to infect the device.

So what can you do to protect yourself at home and at work?

Perhaps the first thing is to do everything you can to prevent a device from becoming infected. This is more than just using good antivirus software, it also means keeping things up-to-date.

Software manufacturers regularly issue updates, or patches, to shore up any vulnerabilities they discover in their software. So make sure all your programmes, your operating system, browser and anti-virus software are kept up-to-date and that you know how to keep them updated.

In most cases, it's best to set the software to do this automatically when an update is released.

Next, regularly back up your data to an external drive or to a cloud based system. Do this, so that you have an alternative way to access your files if they were locked. The more valuable your data is to you, the more frequently you should back it up.

Be cautious. Many ransomware attacks start with phishing emails and as these are getting more and more sophisticated, be careful before clicking on any links, or opening any attachments, in the emails you receive.

Criminals also create web ads that are designed to make us curious, or feel that we're missing out on something, and they also play on our emotions in order to get us to click, or tap, on malicious links. So if you see signs of this, or something doesn't feel right, be especially cautious.

We used to think of cybercrimes as only being carried out by highly skilled hackers, but things have moved on.

Hackers can get ransomware kits which require little expertise and provide everything that's needed - including training and support - for as little as $60 a month.

Many of the attacks they carry out are opportunistic and untargeted, so they affect individuals and businesses alike.

Shoring up any vulnerabilities you may have, making regular backups, and being cautious, especially of links and attachments in emails, could save you, or someone around you, from becoming the victim of a ransomware attack.