Ransomware & Cybercrime

Cybercrime is a broad term used to describe any illegal activity committed over the internet.

It's a fast-growing area of crime. More and more criminals are abusing the speed, convenience and anonymity that they can achieve by hiding behind a computer screen. This type of crime has far less borders, so more seasoned criminals can find it quite easy to exploit people.

Common types of Cybercrime

- HATE CRIMES
- TELEMARKETING
- INTERNET FRAUD
- IDENTITY THEFT
- CREDIT CARD ACCOUNT THEFT

The WannaCry Attack...

... happened in May 2017, and was the largest global ransomware attack of its kind.

Around **230,000**

machines in 150 different countries were affected

The malware encrypted people's files, and hackers demanded around $300-$600 in bitcoin to regain them back

Users were given 3 days to pay the ransom, and then the fee would double. After 7 days, their files would be lost forever

The NHS in the UK got hit the worst, with a total of 16 organisations affected. Some were driven to cancel outpatient appointments, having to turn sick people away

HOLLYWOOD

In the states, Hollywood Presbyterian hospital were forced to pay $17,000 to re-gain all of their systems

And the worst part of it all is that it could have been avoided if the users had updated their security software. The hackers had used a vulnerability in some Windows systems to get in – which had actually been fixed by security updates. Unfortunately, plenty of people hadn't updated...

Here's our preventative tips:

- Avoid suspicious emails & never download or run anything from them. These can be a death sentence.
- Run your security updates. Trust us.
- Keep all software up to date.
- Back up your data. Do it offline, in several places.
- Consider some cybersecurity programs, such as protective anti-malware software.