



DON'T LET CYBERCRIMINALS COST YOU.



Cybercrime has become such a high-value industry that most of the scams we hear about today are run by syndicates or gangs. It has gotten so lucrative that some gangs have evolved into cartels by teaming together to expand their reach and revenue.

Ransomware feels like something you'd only see in a movie, but it is very real! It is easy to deploy and brings in **big money** for the cybercriminals.



HOW DOES RANSOMWARE WORK?

1. Cybercriminals send a phishing email, which often looks like it comes from someone within the organisation.
2. The correspondence includes a link or a file that needs downloading.
3. If a user clicks on the link or downloads the file, it installs malicious software on the user's device, encrypting their files.
4. To decrypt the files, the individual or organisation must pay a ransom.
5. If the ransom is refused, they steal the files and threaten to publish the data as additional leverage.
6. Cybercriminals rely on the fact that organisations would rather protect their reputations than risk exposure in the media.

PROTECT YOURSELF AND YOUR ORGANISATION

- **Beware** of phishing emails and look for any red flags.
- **Verify** links or downloads with the sender.
- **Keep** all software up to date.
- **Back up** your files to a secure system.
- **Report** any suspicious activity immediately.

WHO DO
THEY
TARGET?



EVERYONE!

CYBERCRIME IS A REALITY, DON'T LET IT BYTE YOU!