**Abstract**

**Prediction of type-Social-Engineering Attacks**



**Under Guidance**

**Mr.N.Srinivasulu**

Aim:

The aim of the present project is to **predict** the **attacks** in specific domain in the areas of social-engineering using R.

**Purpose: (attacks done previously)**

Attacks\_like MalwareAttack-2011-RSA-SecurID-Phishing Attack,

2013 Department of Labor Watering Hole Attack,

Crypto-jacking Attacks

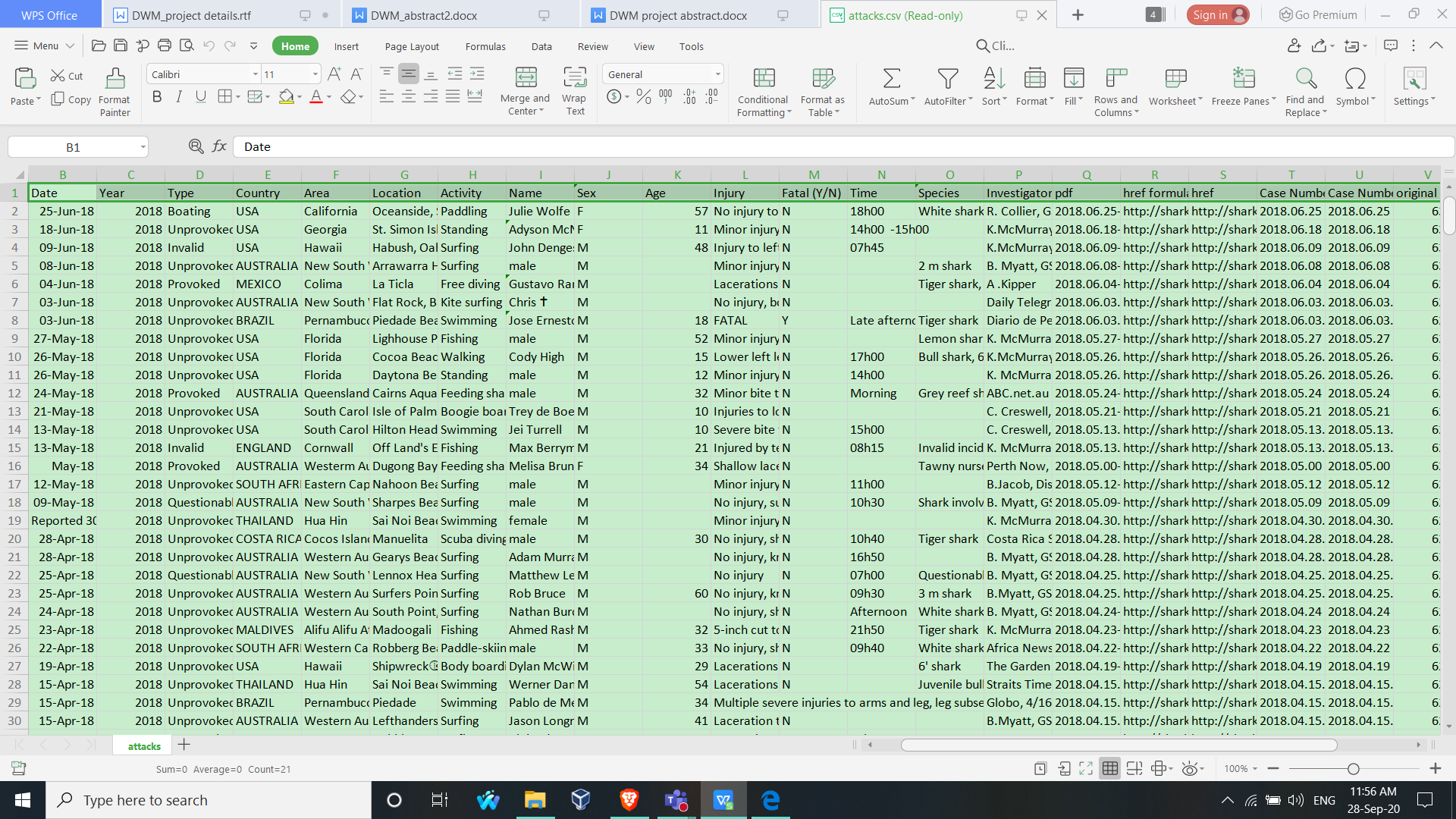
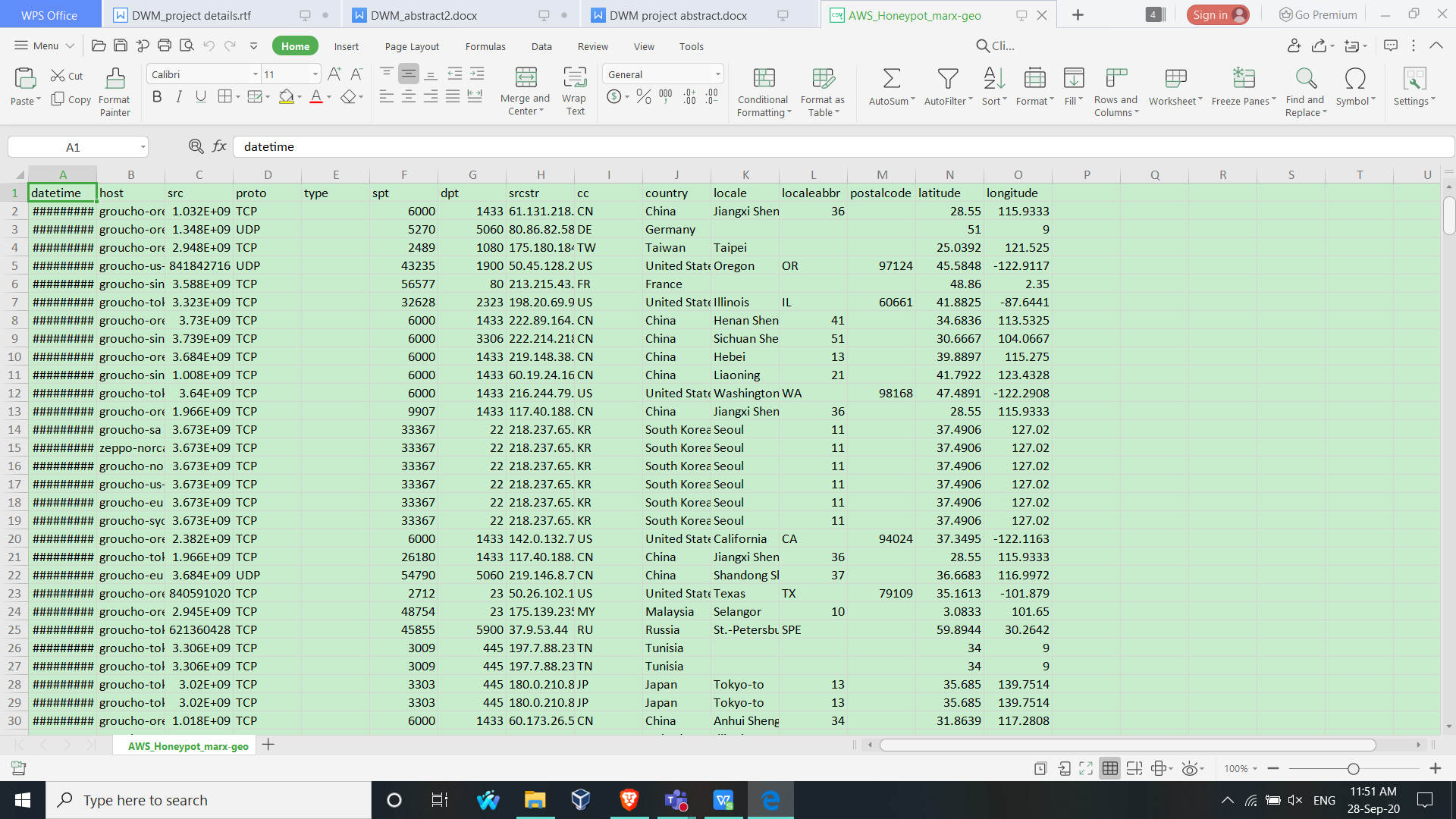
**In-Details** :

In corporations, the main variation of this threat is called spear phishing. This is because cybercriminals collect extremely specific and objective information through social engineering, in addition to targeting precisely certain organizations. In this way, the attacks are smaller, but much more powerful and invasive. Honeypots can be another great source of security information on cyber threats, attackers, their tools, as well as threat actor tactics, techniques, and procedures (TTPs) along with additional valuable information related to the attack.

Our purpose is to classify the attacks and make sure the secure world here after from social engineering-attacks

**References: <https://www.semanticscholar.org/paper/A-Taxonomy-for-Social-Engineering-Attacks-via-Aldawood-Skinner/9860e1b5d4713b2bf5e6ba86846714d758ebd542>**

**DataSets:** Kaggle-data sets (here are the samples)

1. Crypto-jacking attacks - a type of social-engg attack 
2. Aws honeypot attacks:

**Conclusion:**

Finally project suggest the most serious ways to prevent from the companies or the users to safe-guard them by this prediction advice.

An Easy Way to Test Your Cybersecurity Team: In addition to offering precise alerts and requiring low maintenance, honeypots can also be used to test the cybersecurity skills of your organization's employees.

*Prevention is better than cure* (not just for medicine it works in an attack too)

By:

180060010 Kvssk.Pradeep

180050001 K.Gnanedra

180050040 D.Uday Kiran